Privacy Policy

Effective Date: 1 July 2021

1. **PREAMBULA**

THIS HYPELITIX PRIVACY POLICY ("PRIVACY POLICY") IS DESIGNED TO BE "ACCOUNTABLE PURSUANT TO ARTICLE 5(2) GDPR.

BY USING HYPELITIX.COM YOU ACKNOWLEDGE THAT YOU ARE AWARE OF THE PURPOSES AND WAYS IN WHICH YOUR PERSONAL DATA IS COLLECTED AND PROCESSED AND YOU CONSENT TO THE PROCESSING OF YOUR PERSONAL DATA AND ITS SHARING WITH THIRD PARTIES IN ACCORDANCE WITH THE TERMS OF THIS PRIVACY POLICY.

ALL OF THE DATA YOU PROVIDE IS A PREREQUISITE FOR ENTERING INTO AN AGREEMENT TO USE THE SERVICE.

Access to the Service and Services as described in the Terms of Use is provided to you by InMemoryLabOÜ, a limited liability company registered at Harjumaakond, Tallinn, Kesklinnalinnaosa, Vesiväravatn 50-201, 10152, doing business in IT and computer systems sphere ("Data Controller" of your Personal Data).

References to "we," "our," or "us" (or similar words) mean the Hypelitix Service.

References to "you" or "your" (or words similar in meaning) mean our User or Client, as the context of this Privacy Policy requires.

Terms that are not defined in this Privacy Policy are defined in the Terms of USE.

This Privacy Policy describes how We handle certain Personal Information of Clients and Influencers.

We are subject to and fully comply with all rules regarding Personal Information, both European GDPR and U.S. laws related to Personal Information.

All provisions of this Privacy Policy are drafted in accordance with the European Personal Data legislation (Regulation (EU) 2016/679 General Data Protection Regulation ("GDPR")), and are also aligned with, comply with and do not contradict the requirements of U.S. Personal Data protection laws, in particular the California Consumer Privacy Act (CCPA).

2. **PERSONAL DATA AND DATA IS PROCESSED AND THE LEGAL BASIS FOR PROCESSING**

By means of this Privacy Policy We fulfil Our obligation under Articles 13 and 14 GDPR to provide information on data processing to the concerned data subjects.

DISCLAIMER: However, in accordance with Article 62 and Article 14(5)(b) GDPR, in some cases (when we receive Personal Data not from Data Subjects, such as from the social network "Instagram") we are not able to inform each Data Subject (especially Influencers) other than through this Privacy Policy, because due to the large number of Influencers it is impossible or would require disproportionate effort (in particular to process and analyze their content in public domain) to provide such information.

We nevertheless undertake to take appropriate measures to protect the rights and freedoms of the data subject and his or her legitimate interests.

2.1. Client.

We collect various types of information, both directly from you when you register (Article 13 GDPR) and automatically through your device (e.g. personal computer, laptop, cell phone) when you use our Service (Article 13-14 GDPR). In accordance with the principle of "data minimization" (Article 5(1)(c) GDPR), we only collect and process Personal Data that is strictly necessary to provide you with our Services.

Personal data We collect	Legal basis for processing (Art. 13(1)(c) GDPR)	Purposes for processing (Art. 13(1)(c) GDPR):
directly from you:		
1. Full name	Performance of the contract with you (Art. 6(1)(b) GDPR).	We need to know your full name in order to identify you as a party to the Terms of Use in order to fulfill our contractual obligations.
2. Email	1) Performance of the contract with you (Art. 6(1)(b) GDPR).	1) We require your email to log in to your Account and provide you with the Service, Service-related updates, messages, and other important information.

	2) Our legitimate interests, if related to marketing (Art. 6(1)(f) and Recital 47 GDPR).	2) If we use your email to contact you for marketing purposes, it would be in our legitimate interest, but you will always have the option to opt out of such marketing communications about such products and/or services before the first (and any subsequent) communication. You may opt out at any time by sending an email to: legal@hypelitix.com.

The rest is the technical information that must be processed in order to provide you with our services.

Personal Data collected/accessed by Us automatically	Legal basis for processing (Art. 14(1)(c) GDPR)
1. Internet Protocol (IP) address	Performance of the contract (Art. 6(1)(b) GDPR). You need this to connect to the Internet.

2.2 Influencer.

We only process information that you have already publicly shared through public Instagram accounts. We process your Personal Data and ensure its processing in accordance with applicable law, namely the principle of "lawfulness, fairness, transparency" (Art. 5(1)(a) GDPR), and We respect your rights (see section below).

Information about Influencer (categories of personal data):	Legal basis for processing (Art. 14(1)(c) GDPR)	Purposes for processing (Art. 14(1)(c) GDPR): Reason for collection
1. Influencer profile link, full name, avatar, language, bio, country/city/state, brand and general interests, notable engaged users, sponsored posts. 2. Images, graphics, photos, profiles, audio and video clips, sounds, music, works of authorship, apps, links and other content or materials from your Instagram profile.	Influencers make their data available to social media, thereby making it publicly available. We have a legitimate interest in using the data provided by Influencers through the social network Instagram for direct marketing purposes (Recital 47 GDPR) without compromising Influencers' fundamental rights and freedoms.	To allow Clients to choose an Influencer for their business goals and to analyze each Influencer's Instagram posts, stories and IGTV.

3. IDENTITY MANAGEMENT

We do not collect or process Personal Data from Users who do not have an account with the Hypelitix Service.

We process Personal Data in order to provide the Client with analytical data.

Our legitimate interests when dealing with Personal Data are direct marketing purposes as stated in GDPR Regulation 47 (EU GDPR) and statistical purposes as stated in GDPR Regulations 113 and 162.

3.1 Client.

We do not sell, transfer or disclose Client Data except as set forth in this Privacy Policy. We never process your Personal Data without explanation and warning (unless we have informed you and you have given us consent to such use).

We use Client contact information and payment information to establish, maintain and manage the Client relationship necessary to provide the Services. If a Client fails to provide the personal information we require, we may not be able to fulfill our obligations under the terms of the Terms of Service. We only contact Clients for information related to the Services. If marketing is involved, Clients have the option to opt out at any time.

3.2 Influencer.

Notification of Influencers' processing of Personal Information is made through our website and through the provisions of this Policy. We do not have the technical ability to notify each Influencer directly. In addition, under the Terms of Use, the obligation to notify the Influencer of the processing of his or her Personal Data is transferred to the Client.

We provide analytical services, so the above Influencer Data is transmitted to Clients upon payment of the Synchronization fee.

The Influencer Data we process falls into two categories:

1. Raw data	All available information collected from the social network "Instagram". Information is only collected from Influencers' public/open profiles.

2. Processed Data	This category of data is generated from raw data. The processed data are divided into two groups: **1. Collected and saved as is:** - ID; - login / username (unique within Instagram) - full name; - link to profile photo; - bio (status, where the user writes what he or she does, hobbies, etc.); - presence of verification checkbox; - number of posts published; - number of subscriptions; - number of subscribers; - publications, stories, IGTV; 2. **Data processed by the Google Cloud Vision API platform:** media data of publications, IGTV and stories, including the presence or absence of mentions and/or hashtags, text recognition on images and videos of the Instagram Account.

3.3 Data Controller.

The Data Controller may itself use the collected data as a marketing activity. The information collected by the Data Controller will be identical to the information provided to any Client. Such Reports shall be subject to the laws and regulations applicable to all activities of the Data Controller.

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 Client.

We retain your information for as long as your account is active. If you do not perform any activity on the Service for one (1) year, we may remove your Personal Information from our Service.

4.2 Influencer.

As stated above, We process Personal Data obtained from public Instagram Social Network Accounts. It may take up to twenty-four (24) hours to update the data as a result of the synchronization. If Influencer deletes its account, we may also delete such Personal Data from our Service and make it unavailable to the Client. This may take up to one (1) month from the date of Influencer's Instagram deletion.

4.3 Database

All Data is stored in encrypted form. It is impossible to access the Personal Data of any Influencer without an assigned storage ID code.

5. OUR SECURITY MEASURES

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 processors on secure servers (AWS Amazon and Hetzner) in full compliance with international information security requirements. AWS Amazon has ISO 27001 information security management system certifications. We use recommended industry practices to secure access to such data.

We use the appropriate level 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. These include the following measures:

- Protective measures for physical access control:

  We secure access to the premises via ID readers, so that only authorised persons have access. The ID cards can be blocked individually; access is also logged. Furthermore, an alarm system is installed in the premises, preventing infiltration by unauthorised persons. The alarm system is linked to a locking mechanism for the doors.

- 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 have, in addition, a regulation for the creation of passwords. This guarantees 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.

- Protective measures for transfer control:

  The handling of local data storage devices, e.g. USB sticks are regulated via agreements.

  Access to the systems from outside the company network is possible only via secure VPN access.

- Protective measures for input control:

  Our employees do not work directly at 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.

- Protective measures for availability control:

  We ensure the 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 centres 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.

- Protective measures for separation control:

  To separate data, We use logically separate databases so that no accidental reading of data by unauthorised persons can occur.

  Access to the data itself is also restricted by the fact that employees use services (applications) which control access.

- 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 case of data breach (e.g. leakage), We commit to investigate the case, to timely notify the competent data protection authority, to evaluate damages and to communicate the investigation results to all Clients whose personal data were impacted.

We take our responsibility seriously and therefore have implemented a variety of technical and organizational measures ("TOMs") to protect and secure personal data as best as possible. Our measures are aligned with the GDPR regulations (Articles 24, 25 and32).

6. CATEGORIES OF RECIPIENTS OF PERSONAL DATA

We do not rent, sell or transfer Personal Data of Clients to third parties, except as necessary to fulfill our legal obligations.

We provide fee-based analytics services with respect to Influencer data. Recipients of such data are Clients of our Service.

With respect to Client's Data, We review each request to ensure that it satisfies appropriate safeguards, contains a court order or is issued in accordance with legal measures to prevent, investigate, detect or prosecute criminal offenses.

If we hire a processor to act on our behalf, we ensure that adequate contractual arrangements are in place to ensure security and liability at the same level expected of us.

In any case where a third party accesses your data on our behalf or under our instructions (whether inside or outside the EEA), we use the GDPR and CCPA provisions to respect your rights. Where there is no European Commission decision confirming an adequate level of protection (Art. 45(1) GDPR), We use the standard data protection provisions adopted by the European Commission (Art. 46(2)(c) GDPR) to provide appropriate safeguards for your rights and Personal Data in the event of third party access or other data transfer outside of the EEA.

7. YOUR RIGHTS

In compliance 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 range of rights under the GDPR as well as the CCPA, and We are committed to respecting your rights. Among these, you have the right to:

- Require access to your Personal Data (Art. 15 GDPR);

- Require rectification of your Personal Data (Art. 16 GDPR);

- Require deletion of your Personal Data (Art. 17 GDPR; CCPA);

- Require restriction of the processing of your Personal Data (Art. 18 GDPR);

- Require the transfer of your Personal Data (Art. 20 GDPR; CCPA);

- 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, if applicable (Article 7(3) GDPR);

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

- Request to receive certain information about the personal data we have collected about you in the last 12 months. You may make such a request no more than 2 times within a 12-month period (CCPA).

7.2 Your consent and your right to withdraw your consent

If we choose to process your personal data for any purpose you do not agree with, We will provide you with appropriate information at the point where you come across those additional purposes in order to obtain your consent (where required) or are able to perform Our legal obligations, prior to commencing any such additional processing activities. You are not required to give consent just because We ask for it.

If your personal data were processed on the basis of your consent, you may further change your mind and withdraw your consent later by contacting Our Data Protection Officer ("DPO") and requesting to be removed from the mailing list at the following email address legal@hypelitix.com. However, your consent withdrawal will not impact the processing of your personal data which took place before your withdrawal.

7.3 Your right to object to data processing

If your personal data was processed without your given consent (based on the legitimate interest), you may also ask Us to stop processing your personal data and to remove you from the mailing list, by contacting our DPO at legal@hypelitix.com.

However, your request will not impact the processing of your personal data which took place before such request.

If you request Us to rectify, erase your personal data or to restrict processing 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(2)(d), and19 GDPR).

7.4 Your right to lodge a complaint

If your question is not resolved or is not resolved satisfactorily, you have the right to contact your local data protection authority (Art. 13(2)(d), 14(2)(e), 15(1)(f)).

7.5 INFLUENCER: your right to be informed on the Client

You have the right to request information about a Client who has obtained Personal Information from your social media profile, and Hypelitix agrees to provide you with all information about the Client.

If you request information about a Client who has received your Personal Information, Hypelitix will provide you with all of the Client's information within 72 hours of your request.

If Client has shared your social media profile report obtained through use of the Hypelitix service with third parties, you have the right to obtain the entire chain of persons to whom this report has been shared within 72 hours of your request.

7.6 Your right to access to and to erasure of your personal data

You have the right to request the deletion of data/content collected through our Service. In addition, the data/content must be deleted by all persons/companies/auditors to whom this information has been transmitted.

You have the right to log into your Account and change your information to the extent the system allows. You may also submit a request to change your information to the support service.

If you would like to request that your personal information be deleted as required by the CCPA, please send an email to legal@hypelitix.com. If you submit your request by email, you will be asked for information, which will then be verified.

8. COOKIES AND SIMILAR TECHNOLOGIES

We do not use aggregated, non-identifying electronic data collected through the use of our Website and Services.

We cooperate with analytics service providers such as Google Inc., including the Google Cloud Vision API platform, to recognize text in images and videos on the social network "Instagram" .

We inform you that in order to respect our legitimate interests and improve the quality of our services, We may share some of the Personal Data that is publicly available on social media with the following service providers:

- Paypal, Inc.

- Google Inc.

You can find out more about these service providers and the type of data they process by following these links:

https://policies.google.com/privacy;

https://www.paypal.com/ru/webapps/mpp/ua/privacy-full;

https://www.facebook.com/help/instagram/155833707900388/.

9. CHILDREN'S PRIVACY (Article 8 GDPR)

We never knowingly collect, process or solicit any information from anyone of 16 years and younger. The information society services (“Services”) on our sites are neither offered directly nor intend to appeal to such persons. Parents or parental responsibility holders who believe that We directly offer Services to or process personal data of their children aged 16and under may contact Our DPO at legal@hypelitix.com.

DISCLAIMER: When processing public data from the social network "Instagram", if it is not possible to reliably know the real age of users, our verification of the age of users is limited to technically available and reasonable processing of information openly provided by the social network "Instagram". In the event of inaccurate, erroneous or missing age data, the

social network "Instagram" is fully liable for violations of Article 8 GDPR in relation to Personal Data of children.

10. OUR COMMITMENT

- We will only collect and use your data where We have a legal basis to do so;
- We will always be transparent and tell you about how we use your information;
- When We collect your data for a particular purpose, We will not use it for anything else without your consent, unless other legal basis applies;
- We will not ask for more data than needed for the purposes of providing our services;
- We will adhere to the data retention policies and ensure that your information is securely disposed of at the end of such retention period;
- We will observe and respect Your rights by ensuring that queries relating to privacy issues are dealt with promptly and transparently;
- We will keep our staff trained in privacy and security obligations;
- We will ensure to have appropriate technological and organizational measures in place to protect your data regardless of where it is held;
- We will also ensure that all of our data processors have appropriate security measures in place with contractual provisions requiring them to comply with Our commitment;

11. UPDATES IN PRIVACY POLICY

To keep you informed, we will always notify you on our Website if we update this Privacy Policy.