

## **ADHIVE PRIVACY POLICY**

### Contents:

1. Overview
2. Nature of personal data that we process
3. Means of collecting personal data that we employ
4. Purposes of personal data collection
5. Legal basis for use of personal data
6. Disclosure of personal data to third parties. International transfer of personal data
7. Personal data security, accuracy, minimization, confidentiality
8. Personal data retention
9. The rights of individuals
10. Contact details

## 1. Overview

AdHive Platform OÜ (the “**AdHive**”) is a global influencer marketing platform. The privacy of its clients, employees (including ex-employees and job applicants) and users and security of their personal data is of extreme importance for us at AdHive.

This Privacy policy (the “**Policy**”) explains how we at AdHive may collect and use (i.e. process) information related to our clients, employees (including ex-employees and job applicants) and users. This Policy may be amended or updated from time to time, as necessary. This Policy is available on AdHive website (<https://adhiveplatform.com>) and we encourage to regularly review it in order to stay updated with regard to recent changes.

AdHive group consists of several legal entities, and this Policy applies to each entity within AdHive group to the extent that it does not contradict national laws or specific AdHive policies dealing with personal data outside the European Union.

This Policy covers AdHive as a group, so any mentions of “AdHive”, “we”, “our” or similar are related to AdHive or a respective entity with AdHive. For the purposes of complying with EU personal data privacy regulations AdHive shall be the data controller with regard to personal data of its clients, employees (including ex-employees and job applicants) and users and shall have the corresponding responsibilities with regard to such personal data and other personal data which is in lawful possession of AdHive.

## 2. Nature of personal data that we process

AdHive may process the following personal data obtained through the use of means that are covered in this Policy:

Personal details	Name, username; password, date of birth, age, preferred language(s).
Contact details	Address; telephone number (including mobile phone number); e-mail address, any other information provided when filling out a contact form.
Consent records	Records of any consents given, together with any related information.
Online details	Information that is obtained through the use of website, and may or may not constitute personal data, depending on the circumstances and applicable laws: non-precise information about the approximate physical location, Internet Protocol address, information collected through the use of cookies, Javascript, other technologies, log files and similar information.

AdHive will not process following personal data that may be deemed sensitive: race or ethnicity, political views, religious or philosophical beliefs, trade union membership, physical or mental health, sexual life and sexuality, any actual or alleged criminal offences or penalties, or any other information that may be deemed to be sensitive under GDPR in the ordinary course of our business.

AdHive will not process personal data of minors. Our services, website and marketing materials are not intended for use by children, especially those under 13 years old. They may not be used by individuals under 18 years old.

## 3. Means of collecting personal data that we employ

We employ the following means of collecting personal data:

Provided	Personal data provided directly by an individual engaging with us through any means (direct interaction, sign up for emails or newsletters; register for site membership, contact through any means, becoming an employee, provided in the ordinary course of our business relationship, etc.).
Made public	Personal data that was clearly chosen to be made public, including via social media.
Website and other technical means	Personal data of an individual obtained through the use of our website
Advertising and third party	Personal data collected from service providers and third parties that an individual chose to interact with

This Policy does not cover the practices of third parties, including those that may disclose information to us. We are not responsible for the accuracy of any information provided by third parties or third-party policies or practices (including personal data processing practices).

#### 4. Purposes of personal data collection

Purpose/activity	Nature of Personal Data	Lawful basis of processing, including basis of legitimate interest
To manage our relationship with individuals, including our clients, employees (including ex-employees and job applicants) and users	Personal details, Contact details, Consent records	(a) Necessary to comply with legal requirements (legal compliance) (b) Necessary to further our legitimate interests (to keep our records updated and to ensure uninterrupted flow of our business)
To manage and protect our business and ensure security of online services (including website), deliver relevant content and understand the effectiveness of our online offerings (including advertising)	Personal details, Online details, Consent records	(a) Necessary to further our legitimate interests (to ensure uninterrupted availability of our online services, maximize their effectiveness, grow our business and further our marketing strategy) (b) Necessary to comply with legal requirements (legal compliance)
To make suggestions and recommendations to individuals about services that may be of interest to them	Personal details, Contact Details, Online details, Consent records	(a) Necessary to further our legitimate interests (to grow our business and further our marketing strategy)
To be able to manage our finances, including planning and reporting; personnel; sales; accounting; finance; corporate audit; and compliance with legal	Personal details, Contact Details, Online details, Consent records	(a) Necessary to further our legitimate interests (to grow our business and further our marketing strategy) (b) Necessary to comply with legal requirements (legal

requirements		compliance)
To ensure possibility of legal compliance and legal proceedings in case of necessity	Personal details, Contact Details, Online details, Consent records	(a) Necessary to comply with legal requirements (legal compliance)

## 5. Legal basis for use of personal data.

AdHive will only use personal data of an individual when legally allowed to do so. Most commonly, AdHive will use personal data of an individual in the following circumstances:

- To ensure that we are able to perform our obligations under the contract the we entered or are about to enter (including contract with an individual whose personal data we use or other third party, provided that we obtained consent from such individual);
- To ensure that we are able to further our legitimate interests (or legitimate interests of a third party that we have contractual relationship with, provided that we obtained consent from individual whose personal data we use) and the fundamental rights of an individual, whose personal data we use, do not override those interests.
- To ensure that we are compliant with applicable legal and regulatory requirements.

We always consider whether the risk to an individual's personal data protection rights in connection with personal data that we process on the basis of our legitimate interests is not excessive. We also protect individual's rights by ensuring proper retention periods and security controls with regard to personal data of such individual.

We use explicit and unambiguous consent of an individual as a legal basis for processing personal data of such individual, in cases of sending direct marketing communications (including those of third parties). Such consent may be withdrawn at any time by contacting us. In other cases, we use appropriate and reasonable legal basis which may not involve obtaining explicit consent of an individual.

## 6. Disclosure of personal data to third parties. International transfer of personal data

Some areas of business we engage into and services that we provide require the involvement of third parties. We have procedures in place to screen and select these third parties based, among other criteria, on their ability to adequately protect personal data that we process.

From time to time we will transfer personal data to third parties (within or outside of AdHive) outside of the EU. If such third parties are within AdHive group, then their actions are covered by this Policy (to the extent permitted by local laws) and individuals shall have comparable level of protection after transfer of their personal data. If such third parties do not belong to AdHive group, we will only transfer personal data if such third party is contractually obliged by us to provide comparable level of protection to individuals after transfer of their personal data. Specifically:

- We will only transfer personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.
- We may use specific contracts approved by the European Commission which give personal data the same protection it has in the EU.

Details about how we share personal data with third parties are below.

- Sharing personal data within AdHive and to international service providers within AdHive group.

In order to ensure that our business processes run uninterrupted we share personal data with service providers within AdHive group subject to obtaining consent from individuals whose personal data is shared. Such consent may be obtained in an online form (by ticking a box or similar form). We may share personal data without consent of an individual if it is required in order to provide services (or fulfill other obligations) to such individual.

We may use personal data for other purposes subject to informing individuals whose personal data is used first.

We use and share personal data in relation to our website for the purposes of hosting and maintaining it, providing data storage; assisting us with database management, and in order to assist us with related tasks or processes.

All of our service providers are bound by written contract to process personal data provided to them only for the purpose of providing the specific service to us and to maintain appropriate security measures to protect such personal data.

- Sharing with other third parties

We share personal data with our accountants, auditors, lawyers or similar advisers when we ask them to provide us with professional advice.

We share personal data with any other third party if we are under a duty to disclose or share personal data in order to comply with any legal obligation, or to protect our rights, property and/or safety of our personnel or others.

We share personal data with any other third party for the purposes of acting in accordance with the requirements of a court, regulator or government agency.

We share personal data with investors and other relevant third parties in the event of a potential corporate transaction that we may be party to.

All of the third parties that we have a contractual relationship with are under obligation to process personal data provided to them only for the purpose of providing the specific service to us.

## **7. Personal data security, accuracy, minimization, confidentiality**

We have implemented appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorised way. Such measures include two-factor authorization when accessing our data management systems, and market standard encryption algorithms used where our data is stored electronically. Moreover, such measures include means of physical protection and limited access in cases where our data is stored physically.

We limit access to personal data to employees and third parties on a need to know basis. Such employees and contractors are bound by our instructions and respective confidentiality agreements.

We have put in place procedures to deal with any suspected personal data breach and will notify relevant regulator and individuals of a breach where we are legally required to do so. However, we cannot guarantee there will not be a breach, and we are not responsible for any breach of security or for the actions of any third parties. We also cannot guarantee the security of any personal data that is being transmitted to us electronically.

We take reasonable effort to ensure that personal data in our possession is accurate and, where necessary, kept up to date, and any of personal data that we were informed is inaccurate is erased or rectified. However, we cannot guarantee that personal data in our possession is accurate if we were not informed that it is inaccurate and given reasonable time to rectify discrepancies.

We take reasonable effort to ensure that personal data that we process is limited to the information reasonably necessary in connection with the purposes set out in this Policy.

We treat personal data in our possession as confidential. We do not make personal data available to any third party, except our service providers for the purposes and on conditions set out in this Policy or applicable laws. We maintain confidentiality agreements with all our service providers and employees.

## 8. Personal data retention

We take reasonable effort to ensure that personal data is processed for the minimum period necessary for the purposes set out in this Policy. In order to ensure that we consider the following:

- the amount, nature, and sensitivity of the personal data in our possession;
- the potential risk of harm from unlawful breach or disclosure of personal data;
- whether it is possible to fulfill the purposes stated in this Policy without use of personal data in our possession.

Once personal data is no longer able to be used in order to fulfill the purposes stated in this Policy, we immediately delete it.

## 9. The rights of individuals

Individuals shall have the following rights with regard to personal data that we process:

Right	Actual meaning
The right to be informed	Individuals have the right to be informed about the collection and use of their personal data.
The right of access	Individuals have the right to access their personal data.
The right to rectification	An individual can make a request for rectification verbally or in writing.
The right to erasure	Individuals can make a request for erasure verbally or in writing.
The right to restrict processing	Individuals have the right to request the restriction or suppression of their personal data.
The right to data portability	Individuals have the right to obtain and reuse their personal data for their own purposes across different services
The right to object	Individuals have the right to object to the processing of their personal data in certain circumstances.

Each right listed above is not absolute and subject to certain restrictions, exceptions and qualifications. We will be able to grant each such right only to an extent that is determined by us taking into account our prior assessment. We do not grant any rights that go beyond the rights explicitly granted by GDPR.

## 10. Contact details

Individuals may contact us with regard to the above rights. We will be able to respond within one month, provided that all of the necessary information was made available by the individual (including any additional personal data).

For above and any inquiries related to this Policy, our full contact details are:

<b>Full name of legal entity</b>	AdHive Platform OÜ
<b>DPO / Responsible officer</b>	Kristina Kurapova
<b>e-mail address</b>	Kristina@adhive.tv
<b>Postal address</b>	Peterburi tee 47, Tallinn city, Harju county, 11415 Estonia