

Privacy Policy of the Heatmapa Mobile Application

of **heatmapa s.r.o.**, with its registered office at Pod vinohradem 211/7, Braník, 147 00 Prague, Czech Republic, Company ID (IČO): 244 19 010, registered in the Commercial Register kept by the Municipal Court in Prague under file No. C 440662, e-mail: support@heatmapa.com (the "Controller")

This English translation is provided for convenience only. The Czech version of this Privacy Policy is the authoritative and legally binding version (Article 14.2).

I. Introductory Provisions

- 1.1 This privacy policy (the "Policy") contains information on the processing of personal data of users of the Heatmapa mobile application (the "Application" and the "User") provided in accordance with Articles 13 and 14 of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation, "GDPR") and with Act No. 110/2019 Coll., on Personal Data Processing, as amended.
- 1.2 The Policy supplements the Terms of Use of the Heatmapa mobile application and applies to all processing of personal data carried out by the Controller in connection with the operation of the Application. The Policy applies to all Users regardless of the manner in which they use the Application, i.e. both to Users who merely browse the content of the Application and to Users who create content, perform administration of a Venue or Event, or use paid services.
- 1.3 Given the nature of the Application, the essence of which is the display of Users' locations, the Controller pays increased attention to the processing of location data; detailed rules are set out in Article V of the Policy.

II. Identity and Contact Details of the Controller

- 2.1 The controller of personal data is heatmapa s.r.o., identified in the heading of this Policy. The Controller may be contacted in matters of personal data processing at the e-mail address support@heatmapa.com.
- 2.2 The Controller has not appointed a data protection officer, as it is not subject to this obligation under Article 37 GDPR.

III. Categories of Personal Data Processed

- 3.1 The Controller processes personal data provided to it by the User and personal data generated by the use of the Application, to the following extent:
 - a) **identification and registration data:** first name, surname, e-mail address, date of birth (also serving to verify fulfilment of the 18+ age condition by way of the User's declaration), nickname and profile photograph (mandatory components of registration) and password stored exclusively in a secured cryptographic form;
 - b) **profile data:** links to the User's accounts on social networks and other data that the User voluntarily adds to their profile;
 - c) **location data:** the current location of the User's device, if enabled in the device settings, location history to the extent necessary for the functioning of the Application, and Check-ins made by the User (in detail, Article V of the Policy);

- d) **social data:** the list of confirmed friends, sent and received friend requests, invitations to Events, data on participation in Events and on followed Venues;
- e) **content data:** Events created by the User, texts, descriptions, photographs and other content published by the User in the Application;
- f) **contacts:** data from the device's address book, if the User has granted access to them in the device settings; the access serves exclusively to find persons who already use the Application or to send an invitation, and may be revoked at any time;
- g) **data on the use of the Application:** the User's interactions in the Application, in particular displayed Venues and Events, searches, reactions to notifications, settings and preferences;
- h) **technical data:** IP address, device type and model, operating system and its version, language settings, device and Application identifiers, push notification delivery token, operational records (logs) and error records;
- i) **communication data:** the content of the User's communication with the Controller, in particular suggestions, complaints, content reports and feedback;
- j) **billing and transaction data of Business Users:** identification and billing data of persons using paid services under the Terms of Use (name, registered office, Company ID, VAT ID, e-mail) and data on transactions carried out; the Controller does not process complete payment instrument data, the processing of which is ensured by the operator of the App Store / Google Play or the payment gateway provider.

- 3.2 The Controller does not process special categories of personal data within the meaning of Article 9 GDPR. The User acknowledges that location data and Check-ins may indirectly reveal information about their habits and interests; the Controller therefore handles them with an increased level of protection in accordance with this Policy.

IV. Purposes and Legal Bases of Processing

- 4.1 Personal data are processed for the following purposes and on the following legal bases:
- a) **provision of the services of the Application** (maintenance of the user account, display of the map, Venues and Events, connecting with friends, Check-ins, creation of Events, administration of Venues, provision of paid services) – the legal basis is the performance of a contract under Article 6(1)(b) GDPR;
 - b) **sharing the User's location with their friends on the map** – the legal basis is consent under Article 6(1)(a) GDPR, granted by enabling access to location in the device settings and by activating location sharing in the Application; consent may be withdrawn at any time in accordance with Article V of the Policy;
 - c) **access to contacts for the purpose of finding friends** – the legal basis is consent under Article 6(1)(a) GDPR;
 - d) **personalisation of content and recommendations** (adaptation of the map and recommendations of Venues and Events to the User's location, preferences and previous interactions) – the legal basis is the performance of a contract under Article 6(1)(b) GDPR, or the Controller's legitimate interest in increasing the relevance of the service under Article 6(1)(f) GDPR;
 - e) **sending notifications of Venues and Organisers and other marketing communications** – the legal basis is consent granted by enabling the Application's notifications in the settings of the User's device; the sending of notifications may be

switched off at any time in the device settings by switching off the Application's notifications; individual categories of notifications cannot be switched off separately;

f) **ensuring the security of the Application and preventing its misuse** (detection of fake accounts, spoofed location, stalking of other persons, unsolicited communications and other prohibited conduct, content moderation) – the legal basis is the Controller's legitimate interest in protecting Users and the service under Article 6(1)(f) GDPR, or compliance with legal obligations under Regulation (EU) 2022/2065 (DSA);

g) **analytics and improvement of the Application** (aggregate usage statistics, error diagnostics) – the legal basis is the Controller's legitimate interest under Article 6(1)(f) GDPR; where required by legal regulations, the User's consent;

h) **compliance with legal obligations** (in particular bookkeeping, fulfilment of tax obligations, cooperation with public authorities, handling of reports of unlawful content) – the legal basis is Article 6(1)(c) GDPR;

i) **establishment, exercise and defence of legal claims** – the legal basis is the Controller's legitimate interest under Article 6(1)(f) GDPR.

- 4.2 The provision of registration data, including the nickname and profile photograph, is a contractual requirement; without them, the contract on the use of the Application cannot be concluded or performed. The provision of location data and access to contacts is entirely voluntary; failure to provide them only results in the non-functionality of those parts of the Application that depend on them.

V. Location Data

- 5.1 The User grants access to the device's location in the settings of their device, including the choice of accuracy and access mode. The User is entitled to switch off location sharing at any time in the settings of the device or in the settings of the Application, thereby withdrawing the consent under Article 4.1(b) of the Policy; the lawfulness of processing prior to the withdrawal of consent is not affected. Switching off location sharing is the only privacy setting available in the Application.
- 5.2 The User's location and Check-ins are visible exclusively to Users with whom the User has mutually confirmed friendship. The User's precise location is not public and is not made available to Venues or Organisers; only aggregate and anonymised statistics may be made available to them.
- 5.3 The current location is processed on an ongoing basis for the purpose of displaying the map and friend functions. The history of the precise location is retained only for the period necessary for the functioning of the Application and for ensuring its security, for a maximum of 30 days; after this period it is deleted or anonymised. Check-ins are retained for the duration of the user account or until deleted by the User.
- 5.4 The use of the Application for stalking or monitoring other persons is prohibited and constitutes grounds for blocking the account; in serious cases, the Controller will report the matter to law enforcement authorities.

VI. Recipients of Personal Data

- 6.1 The following are made available to other Users: the User's profile (name or nickname, profile photograph, links to social networks), their location and Check-ins (exclusively to Users with whom they have mutually confirmed friendship), data on participation in Events and on followed Venues (likewise exclusively to confirmed friends) and the content published by the User in the Application.
- 6.2 The Controller may make personal data available, to the necessary extent, to the following categories of recipients:
- a) providers of hosting and cloud services;
 - b) providers of map data and geolocation services (in particular Mapbox);
 - c) providers of push notification and e-mail delivery services (including the Apple Push Notification service and Firebase Cloud Messaging);
 - d) providers of analytical and diagnostic tools;
 - e) Apple and Google in connection with the distribution of the Application and in-app purchases; the payment gateway provider for payments made outside the App Store / Google Play;
 - f) providers of accounting, tax, legal and similar professional services;
 - g) public authorities, where so provided by a legal regulation or an enforceable decision.
- 6.3 The Controller shall provide the current list of processors upon request sent to the e-mail address support@heatmapa.com.
- 6.4 The Controller has concluded personal data processing agreements under Article 28 GDPR with all processors. The Controller does not sell personal data or transfer them to third parties for their own marketing purposes.
- 6.5 The Controller is entitled to create from personal data aggregate, statistical and anonymised data, i.e. data that cannot be attributed to a specific User or any other identified or identifiable natural person, even retrospectively with the use of additional information. Data anonymised in this way do not constitute personal data within the meaning of the GDPR (Recital 26 GDPR) and their processing is not governed by the GDPR. The Controller is entitled to use anonymised and aggregated data without restriction, including their use for commercial purposes and their disclosure to third parties, whether for consideration or free of charge, in particular in the form of aggregate statistics on footfall and use of the Application provided to Venues and Organisers. Article 6.4 of the Policy remains unaffected; Users' personal data are not the subject of any trade.

VII. Transfers of Personal Data to Third Countries

- 7.1 Some processors may process personal data outside the European Economic Area, in particular in the United States of America. Such a transfer is based on a European Commission adequacy decision under Article 45 GDPR (the EU-U.S. Data Privacy Framework, where the recipient is certified), or on standard contractual clauses under Article 46(2)(c) GDPR, supplemented where appropriate by additional safeguards.

VIII. Retention Period of Personal Data

- 8.1 Personal data are retained only for the period necessary to fulfil the purpose of the processing, in particular as follows:

- a) registration, profile and social data: for the duration of the user account; after its cancellation, they are deleted or anonymised within 30 days, with the exception of data that the Controller is obliged or entitled to retain for longer;
- b) precise location history: for no longer than the period under Article 5.3 of the Policy;
- c) content published in the Application: for the duration of the account or until deleted by the User; content shared with other Users may remain accessible to those Users even after the cancellation of the account, but without any link to the User's identity;
- d) accounting and tax documents: for the period laid down by legal regulations, as a rule 10 years;
- e) operational and security records (logs): for no longer than 12 months;
- f) data necessary for the establishment, exercise or defence of legal claims: for the duration of the relevant limitation periods, or for the duration of the relevant proceedings.

IX. Automated Processing and Profiling

- 9.1 The Application personalises the displayed content and recommendations based on the User's location, preferences and previous interactions; recommendations may be generated algorithmically, including with the use of artificial intelligence. This does not constitute automated individual decision-making with legal or similarly significant effects within the meaning of Article 22 GDPR.
- 9.2 Paid highlighting of Venues and Events is always clearly recognisable in the Application.

X. Rights of the Data Subject

- 10.1 In connection with the processing of personal data, the User has the following rights:
 - a) the right of access to personal data and to obtain a copy thereof under Article 15 GDPR;
 - b) the right to rectification of inaccurate personal data and completion of incomplete personal data under Article 16 GDPR;
 - c) the right to erasure of personal data under Article 17 GDPR, where the conditions of that provision are met; the user account may be deleted directly in the settings of the Application;
 - d) the right to restriction of processing under Article 18 GDPR;
 - e) the right to portability of data that the User has provided to the Controller and that are processed on the basis of a contract or consent, under Article 20 GDPR;
 - f) the right to object to processing based on the Controller's legitimate interest under Article 21 GDPR;
 - g) the right to withdraw consent to processing at any time, without affecting the lawfulness of processing based on consent before its withdrawal; consent relating to location and contacts may be withdrawn in the settings of the device or the Application, and consent relating to notifications by switching off the Application's notifications in the device settings;
 - h) the right to lodge a complaint with the supervisory authority, which is the Office for Personal Data Protection (Úřad pro ochranu osobních údajů), Pplk. Sochora 27, 170 00 Prague 7, www.uoou.gov.cz.

- 10.2 The rights under Article 10.1 of the Policy may be exercised by e-mail at support@heatmapa.com. The Controller shall handle the request without undue delay, at the latest within one month of its receipt; in justified cases, this period may be extended by a further two months, of which the applicant will be informed. For the purpose of protecting personal data, the Controller is entitled to verify the identity of the applicant before handling the request.

XI. Security of Personal Data

- 11.1 The Controller has adopted appropriate technical and organisational measures to protect personal data against unauthorised access, loss, misuse or destruction within the meaning of Article 32 GDPR, in particular encryption of data transmission, storage of passwords exclusively in cryptographic form, access management based on the principle of least privilege and regular security updates.
- 11.2 The User acknowledges that no data transmission over the internet can be absolutely secured. The User is obliged to protect their login credentials and device and to report any suspected misuse of their account to the Controller without undue delay.

XII. Processing of Data of Persons Under 18 Years of Age

- 12.1 The Application is intended exclusively for persons over 18 years of age; fulfilment of the age condition is based on the date of birth provided upon registration and the User's declaration. The Controller does not knowingly process personal data of persons under 18 years of age. If the Controller discovers that a user account has been created by a person under 18 years of age, it will cancel the account and delete the related personal data, unless prevented from doing so by a legal obligation.

XIII. Cookies and Similar Technologies

- 13.1 The Application may use device identifiers, third-party software development kits (SDKs) and similar technologies necessary for its functioning, security and analytics. Technologies that are not necessary for the provision of the service are used exclusively on the basis of the User's consent, which may be managed in the settings of the Application or the device.

XIV. Final Provisions

- 14.1 The Controller is entitled to update this Policy, in particular in the event of a change in the scope of the services provided, the range of processors or legal regulations. The User will be notified of material changes in the Application or by e-mail before they take effect. The current version of the Policy is available in the Application and at heatmapa.com/privacypolicy and heatmapa.cz/privacypolicy.
- 14.2 This Policy is drawn up in the Czech language. Any translation into another language is for information purposes only; the Czech version is the authoritative version.
- 14.3 This Policy enters into effect on 23 July 2026.