PRIVACY POLICY

I. INTRODUCTION

1. The Controller of personal data collected, in particular, via the platform available at www.seeplaces.com (hereinafter referred to as the 'Service' or 'Platform') and the SeePlaces mobile application (hereinafter referred to as the 'Application') — i.e. the entity that determines how your personal data is used — is Akati Sp. z o.o., with its registered office at ul. Reymonta 39, 45-072 Opole (hereinafter referred to as the 'Controller' or 'Akati'). The Controller can be contacted by email at: info@seeplaces.com.

   The Controller is responsible for ensuring the security of the personal data provided and for processing it in accordance with applicable law.
2. The Controller has appointed a Data Protection Officer (DPO), who can be contacted regarding matters relating to the processing of personal data and the exercise of your rights under data protection legislation. The DPO can be contacted by email at: iod@seeplaces.com.
3. Your personal data is processed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as the 'GDPR'), as well as other applicable data protection laws.
4. The Controller processes the personal data of:
   1) logged-in users who hold a user account in the Application;
   2) non-logged-in users of the Platform and the Application who use services, tools or functionalities that do not require account registration or login.
5. When visiting the Service and the Application, the following data is collected:
   1) personal data provided by you (the user),
   2) data obtained and recorded automatically.
6. The subsequent sections of this 'Privacy Policy' describe the purpose and scope of personal data used by the Controller in detail.

II DATA COLLECTED – BASIC INFORMATION

1. This information applies to all methods by which the Controller processes your personal data, as described in Sections III and IV.
2. The Controller does not use your personal data for automated decision-making, including profiling, as defined in Article 22 of the GDPR.
3. Provided that all data security guarantees are met, personal data processed through the Service may be transferred to other entities, including:
   1) entities authorised to receive such data under applicable law;
   2) entities processing data on behalf of the Controller, e.g. providers of technical and hosting services, analytics providers, marketing agencies and consulting firms;
   3) other data controllers, where necessary to perform a contract or provide services or meet legal obligations, including, in particular, providers of travel services presented on the platform and in the application, as well as notaries, law firms and postal or courier companies;
   4) business partners providing services to the Controller under contract.

4. Where necessary for the proper performance of a contract, the Controller may transfer personal data to recognised subcontractors or business partners of Akati who process personal data in countries outside the European Economic Area (EEA).

   As data protection standards in these countries may differ from those guaranteed under the GDPR in the European Union, any transfer is carried out with appropriate safeguards, primarily through:

   1) cooperation with data processors located in countries outside the EEA that the European Commission has deemed to provide an adequate level of data protection. This includes companies based in the United States that are certified under the approved EU–US Data Privacy Framework, such as Microsoft,

   and in the absence of the aforementioned European Commission decision:

   2) the use of Standard Contractual Clauses in agreements with such entities;
   3) the use of Binding Corporate Rules approved by the competent supervisory authority;
   4) the application of the conditions specified in Article 49 of the GDPR.

   The Controller ensures that any transfer of personal data is based on appropriate agreements and carried out securely and in a controlled manner.

   For each of the options listed in points 2–4 above, you can request more information about the safeguards in place, obtain a copy of these safeguards or find out where they are available.

5. The Controller informs you that, in connection with the processing of personal data collected via the Service and the Application, every data subject has the right to submit a request regarding:
   1) access to data (including information about what personal data is processed by the Controller and the scope of processing, and obtaining a copy of the data – as specified in Article 15 of the GDPR);
   2) the rectification of personal data (i.e. the correction of personal data processed by the Controller if it is inaccurate or incomplete – see Article 16 of the GDPR);
   3) the erasure of data (e.g. where the data is no longer needed for the purposes for which it was collected, or where the Controller has no legal basis for processing it – see Article 17 of the GDPR);
   4) the restriction of data processing (e.g. if you contest the accuracy of the personal data used by the Controller or if the data is no longer needed by the Controller but must be processed for the purpose of pursuing claims, see Article 18 of the GDPR);
   5) the objection to the processing of personal data, including profiling (if data is processed on the basis of the Controller's legitimate interest or for direct marketing purposes – see Article 21 of the GDPR);
   6) data portability to another controller (if processing is automated and based on consent or a contract – see Article 20 of the GDPR);
   7) if processing is based on consent (e.g. for marketing purposes), you have the right to withdraw your consent at any time and in any manner (withdrawal of consent does not affect the lawfulness of processing carried out before consent was withdrawn.)
6. Every person whose data is processed has the right to lodge a complaint with the President of the Personal Data Protection Office (the supervisory authority) if they believe that the processing of their personal data violates legal provisions (more information: https://uodo.gov.pl/pl/83/155).
7. The Controller obtained the data directly from you (users of the Service and the Application). The Controller may also process:

1) data of other individuals provided by users of the Service and Application when using the services described in this 'Privacy Policy';
2) personal data obtained from entities with which the Controller cooperates based on concluded agreements (e.g. the professional details of employees designated as contact persons for the purpose of fulfilling the agreement or the details of individuals participating in events organised by the Controller);
3) personal data obtained from third parties cooperating with the Controller, provided that the data were made available to the Controller on the basis of your consent;
4) data obtained from publicly available sources, such as the National Court Register, the Central Register and Information on Business Activity, or websites.

III. PERSONAL DATA PROVIDED BY THE USER

III. A. CONTACT BY EMAIL OR PHONE

1. The Controller processes personal data — in particular your name, email address, phone number, and other information you provide — to the extent necessary for handling inquiries and fulfilling requests, including communication and responding to questions submitted via the contact phone number and email address provided in the Service (legal basis: Article 6(1)(f) of the GDPR – legitimate interest).
2. The Controller has the right to process personal data for the period necessary to handle the inquiry, including responding to the correspondence sent or the submission/question communicated during the telephone conversation.
3. Providing personal data is voluntary, but necessary in order to respond to the submitted question, handle the submission properly, and address the enquiry. The consequence of failing to provide personal data may be the impossibility to answer or process the enquiry.

III. B. HELPLINE

1. The Controller processes personal data to handle enquiries made via the Helpline service, the number of which is available on the Platform and in the Application. This includes:
    1) responding to questions asked during phone calls (legal basis: Article 6(1)(f) of the GDPR – legitimate interest);
    2) collecting and using personal data obtained through the call recording system to verify the quality of services provided (legal basis: Article 6(1)(f) of the GDPR (legitimate interest);
    3) establishing, pursuing or defending claims for the duration of the proceedings and the period until potential claims become time-barred. The legal basis for this is the Controller's legitimate interest (Article 6(1)(f) of the GDPR – legitimate interest).
2. The Controller is entitled to process personal data for the period necessary to achieve the above purposes. Depending on the legal basis, this shall be:
    1) the period necessary to fulfil the above-mentioned purpose, i.e. until the user's enquiry has been responded to;
    2) until an objection is raised.
3. Recordings from the call recording systems will be stored for no longer than three months from the recording date. If a recording constitutes evidence in proceedings conducted under the law, or if the Controller becomes aware that it may constitute such evidence, this period will be extended until the proceedings have concluded. After these periods expire, recordings containing personal data will be destroyed.

4. Providing personal data is also necessary for the proper handling of the submission. Failure to provide personal data may result in the request being unable to be responded to or processed (including, for example, preparing and presenting an offer).

III. C. FORM (CONTACT / OFFER FORM)

1. The Controller may collect your personal data via the form available in the Service and the Application, in particular:
    1) first and last name;
    2) email address;
    3) IP address
    4) any other information you provide via the selected form (e.g. phone number).
2. The Controller processes personal data solely to the extent necessary:
    1) to receive and handle submissions, including communicating with and responding to users who have sent submissions or questions via the form (legal basis: Article 6(1)(f) of the GDPR – legitimate interest);
    2) to establish contact (via the selected communication channel) and to prepare and present an offer in response to the request submitted by the user of the Service and the Application via the form (legal basis: Article 6(1)(b) GDPR – taking steps at the request of the data subject prior to entering into a contract).
3. The Controller is entitled to process personal data for the period necessary to achieve the above purposes. Depending on the legal basis, this shall be:
    1) the time required to handle the submission and respond to the enquiry sent by the user via the form;
    2) the time required to prepare and deliver a dedicated offer.
4. Providing the personal data specified in the form is voluntary but necessary in order to respond to the submitted enquiry, handle the submission properly, and prepare and present a dedicated offer. Failure to provide personal data may result in the inability to respond, fulfil the inquiry, or present the offer.

III. D. USER ACCOUNT IN THE SEEPLACES APPLICATION

1. The Controller processes your personal data for the following purposes:
    1) concluding an Electronic Services Agreement (in accordance with the Act of 18 July 2002 on the Provision of Services by Electronic Means, hereinafter referred to as the 'ESA'), using the Application, including registering and maintaining a free user account (legal basis: Article 6(1)(b) of the GDPR – performance of a contract);
    2) pursuing claims arising from the contract (legal basis: Article 6(1)(f) of the GDPR (legitimate interest). The time limits for pursuing claims arising from the contract are defined in detail in the Civil Code.
    3) verifying the quality of services provided under the concluded contract (legal basis: Article 6(1)(f) of the GDPR – legitimate interest);
    4) performing agreements and cooperation arrangements with business partners who commission services provided by the Controller on your behalf (legal basis: Article 6(1)(f) of the GDPR – legitimate interest);
    5) direct marketing of the Controller's own products and services, as well as those of its partners, including personalising marketing content (legal basis: Article 6(1)(f) of the GDPR – legitimate interest).

2. The Controller may process personal data of users for whom electronic services are provided via the Application, to the extent necessary to perform the contract, including registration and maintenance of a user account, in particular:
    1) first and last name;
    2) email address;
    3) IP address
    4) and any other data provided by the user while using the service.
3. The Controller is entitled to process personal data for the period necessary to achieve the above purposes. Depending on the legal basis, this shall be:
    1) the time required to perform the contract;
    2) the time required to fulfil legal obligations and the period during which the law requires data retention (e.g. tax regulations);
    3) until claims arising from the agreement become time-barred;
    4) until an objection is raised.
4. Providing personal data is voluntary but necessary in order to conclude an Electronic Services Agreement, including the registration and maintenance of a user account within the Application. Failure to provide personal data may result in an inability to conclude the agreement or register a user account.
5. The Terms and Conditions, which specify the rules and conditions for using the SeePlaces mobile application and the services provided by the Controller, are available at: https://seeplaces.com/static/pdf/pl/Warunki_Uzywania_Platformy_Seeplaces_25.pdf

III. E. PROVISION OF SERVICES

1. The Controller processes your personal data for the following purposes:
    1) providing the service (including services provided electronically) aimed at sharing information about travel services offered by Providers and forwarding enquiries about offers to the Providers, in accordance with the SeePlaces.com Platform Terms of Use (legal basis: Article 6(1)(b) of the GDPR – taking steps at the request of the data subject);
    2) performing legal obligations incumbent on the Administrator, e.g. financial settlements and accounting reporting, including issuing and storing invoices or responding to complaints (legal basis: art. 6.1. lit. c of the DPA - legal obligation),
    3) establishing, pursuing or defending claims arising from the contract (legal basis: Article 6(1)(f) of the GDPR – legitimate interest); the time limits for pursuing such claims are specified in detail in the Civil Code;
    4) verifying the quality of services provided in connection with the concluded contract (legal basis: Article 6(1)(f) of the GDPR (legitimate interest);
    5) for direct marketing (of the Controller's own products and services as well as those of its partners), including the personalisation of marketing content (legal basis: Article 6(1)(f) of the GDPR – legitimate interest),
    6) carrying out marketing communication via electronic means (in particular email, telephone calls and SMS messages), based on separate consent for data processing for this purpose (legal basis: Article 6(1)(a) of the GDPR – consent).
2. The Controller obtains the identification and contact details of all individuals named in an inquiry submitted for a selected travel service offered by its Provider directly from the person who submits the inquiry via the Service and Application.

3. The person submitting the inquiry referred to in para. 2 above does so also on behalf of all individuals listed in the inquiry and thereby assumes responsibility for informing them of the principles for the processing of personal data by the Controller, as set out in this document.
4. The Controller is entitled to process personal data for the period necessary to achieve the above purposes. Depending on the legal basis, this shall be:
    1) the period necessary for the performance of the contract;
    2) the period for fulfilling legal obligations and the period during which legal provisions require data to be retained (e.g. tax regulations);
    3) the period until claims arising from the contract become time-barred;
    4) the period until an objection is raised;
    5) the period until consent for communication via the selected channel (email address or phone number) is withdrawn.
5. Providing personal data for the purpose of entering into and performing the contract is voluntary but necessary in order to conclude the contract, including submitting an enquiry for an offer concerning a selected travel service offered by the Provider.
6. Providing personal data for the purpose of receiving marketing communications via the selected communication channel (i.e. email address or telephone number) is voluntary, but necessary to receive commercial information. Failure to provide personal data will result in an inability to receive marketing content (e.g. promotional offers).
7. Recipients of marketing communications may opt out of receiving them at any time, in particular by contacting the Controller or the Data Protection Officer via the contact details provided above. Withdrawing consent does not affect the lawfulness of data processing carried out before consent was withdrawn.
8. The Terms of Use of the SeePlaces.com Platform are available at: https://seeplaces.com/static/pdf/pl/Warunki_Uzywania_Platformy_Seeplaces_24.pdf

III. F. MARKETING COMMUNICATION

1. The Controller processes your personal data for the following purposes:
    1) carrying out marketing communication via electronic means (in particular email, telephone calls and SMS messages), based on separate consent for the processing of data for this purpose (legal basis: Article 6(1)(a) of the GDPR – consent);
    2) carrying out direct marketing, including sending information about the controller's products and services, and the products and services of third parties cooperating with Akati (e.g. business partners), including personalising marketing content, i.e. preparing and presenting offers tailored to your preferences (legal basis: Article 6(1)(f) of the GDPR – legitimate interest;

    – in accordance with the provisions of the Act of 12 July 2024 – Electronic Communications Law.
2. The Controller is entitled to process personal data for the period necessary to achieve the above purposes. Depending on the legal basis, this shall be:
    1) the period until consent for communication via the selected channel (email address or phone number) is withdrawn;
    2) the period until an objection is raised.
3. Providing personal data for the purpose of receiving marketing communications via the selected communication channel (i.e. email address or telephone number) is voluntary, but necessary to receive commercial information. Failure to provide personal data will result in an inability to receive marketing content.

4. Recipients of marketing communications may opt out of receiving them at any time, in particular by contacting the Controller or the Data Protection Officer via the contact details provided above. Withdrawing consent does not affect the lawfulness of data processing carried out before consent was withdrawn.
5. The Controller may share your personal data with third parties (e.g. business partners) to enable them to carry out their own marketing activities. Such sharing of data will only take place if you give separate consent to the processing of your data for this purpose. The entity indicated in the content of the consent will then become an independent controller of the personal data provided on that basis.

III. G. PARTNER PROGRAMME FOR AFFILIATES

1. The Controller processes your personal data for the following purposes:
    1) carrying out actions at your request prior to entering into an agreement, including handling your application, registering you for the Partner Programme, and establishing cooperation (legal basis: Article 6(1)(b) of the GDPR – taking steps at the request of the data subject);
    2) receiving and handling the application submitted via the registration form, including communicating with you about your participation in the Partner Programme (legal basis: Article 6(1)(f) of the GDPR – legitimate interest);
    3) maintaining and developing business relationships (legal basis: Article 6(1)(f) of the GDPR – legitimate interest).
    4) for direct marketing (of the Controller's own products and services as well as those of its partners), including the personalisation of marketing content (legal basis: Article 6(1)(f) of the GDPR – legitimate interest),
    5) carrying out marketing communication via electronic means (in particular email, telephone calls and SMS messages), based on separate consent for data processing for this purpose (legal basis: Article 6(1)(a) of the GDPR – consent).
2. The Controller may process personal data to the extent necessary to establish cooperation and register with the Partner Programme, including, in particular, the following:
    1) first name,
    2) last name,
    3) email address;
    4) telephone number,
    5) company name
    6) VAT number,
    7) registered office address,
    8) IP address
3. The Controller is entitled to process personal data for the period necessary to achieve the above purposes. Depending on the legal basis, this shall be:
    1) the period necessary for the performance of the contract;
    2) the period for fulfilling legal obligations and the period during which legal provisions require data to be retained (e.g. tax regulations);
    3) until claims arising from the agreement become time-barred;
    4) until an objection is raised.

4. Providing personal data is voluntary but necessary to enter into an agreement, including joining the Partner Programme and establishing cooperation. Failure to provide personal data may result in an affiliate being unable to register for the Partner Programme.

III. H. ADDING RATINGS AND COMMENTS

1. The Controller processes personal data to enable you to add ratings and comments about travel services offered by Providers and presented on the Platform and in the Application. This is done via an online survey shared via email after you have used a selected service (legal basis: Article 6(1)(a) of the GDPR – consent).
2. The Controller has the right to process personal data until your consent is withdrawn.
3. Providing personal data is voluntary, but necessary to use the Controller's option to add a rating or comment. Failure to provide the required personal data will result in an inability to add a rating or comment.

III. I. LINKEDIN

1. Akati is the controller of the personal data of users of the services and products offered by LinkedIn Ireland Unlimited Company (hereinafter: LinkedIn), a company with its registered office at Wilton Place, Dublin 2, Ireland, who visit the Controller's page available at: https://www.linkedin.com/company/seeplaces (hereinafter referred to as the 'Company Page').

   As the Controller, Akati is responsible for the security of the personal data provided, and for processing such data in compliance with applicable laws.
2. The Controller processes the personal data of users who visit the Company Page while using LinkedIn products and services. This data is processed:
   1) in connection with operating the Company Page, including for the purpose of promoting its own brand (legal basis: Article 6(1)(f) of the GDPR – legitimate interest);
   2) for the purpose of responding to questions submitted via services offered by LinkedIn (legal basis: Article 6(1)(f) of the GDPR – legitimate interest); where users provide special categories of personal data (e.g. information about health), they are declaring that they consent to the use of such data for the proper handling of submissions and responses, including communication and providing answers (legal basis: Article 9(2)(a) of the GDPR – consent).
3. The Controller has the right to process:
   1) publicly available personal data (such as username, profile photo, LinkedIn activity status), content of comments and other information made publicly available by the user via LinkedIn services;
   2) personal data provided by users visiting the Company Page, including information shared in the user's profile, as well as other content, comments, messages and communications (e.g. photos, contact details, workplace, place of residence, education, interests or worldview beliefs);
   3) other personal data provided by users in messages sent via LinkedIn services (including contact details and health information), for the purpose of responding to submitted enquiries or requests for contact.
4. The scope of personal data processing, specific purposes and the rights and obligations of users of LinkedIn products and services arise directly from:
   1) the LinkedIn User Agreement (available at: https://pl.linkedin.com/legal/user-agreement), and
   2) the 'LinkedIn Privacy Policy' (available at: https://pl.linkedin.com/legal/privacy-policy);
   3) or applicable legal provisions

– which are further clarified by the actions taken by the user on the LinkedIn social networking platform.

5. The Controller is entitled to process personal data for the period necessary to achieve the above purposes. Depending on the legal basis, this shall be:
    1) the period until an objection is raised (or the LinkedIn user account is deleted);
    2) the period until consent is withdrawn (or the LinkedIn user account is deleted); Withdrawal of consent does not affect the lawfulness of data processing carried out while the consent was in force.
    3) the period necessary to handle the inquiry submitted by the user via LinkedIn services.
6. The catalogue of recipients of personal data processed by the Controller depends primarily on the scope of products and services used by the LinkedIn user, but also on the user's consent or legal provisions. Once all data security safeguards are in place, the Controller may disclose the personal data of a user visiting the Company Page to other data processors acting on the Controller's behalf, such as providers of technical services and advisory service providers (including law firms), as well as business partners performing services for the Controller under executed agreements.
7. The Controller will not transfer the personal data of users of LinkedIn products and services to countries outside the European Economic Area (i.e. countries other than EU Member States, Iceland, Norway and Liechtenstein).
8. The Controller may process the personal data of users of LinkedIn products and services who visit the Company Page in order to analyse how users interact with the Controller's page and related content (for statistical purposes), provided that visiting the Company Page and associated content generates a page insight event involving the processing of personal data (legal basis: Article 6(1)(f) of the GDPR – legitimate interest).
9. In the case of personal data processed for the purpose of compiling statistics on user activity on the Company Page (including following or unfollowing the page, or recommending it in posts or comments), Akati and LinkedIn will act as joint controllers of users' personal data. The types of data, scope of processing, privacy principles and user rights are defined in:
    1) this document;
    2) the 'LinkedIn Privacy Policy' document published on LinkedIn's website at: https://pl.linkedin.com/legal/privacy-policy;
    3) 'Page Insights Joint Controller Addendum', published on LinkedIn's website at: https://legal.linkedin.com/pages-joint-controller-addendum.
10. LinkedIn is responsible for informing users of LinkedIn products and services about the processing of their data for page insight purposes and for enabling them to exercise their rights under the GDPR (information about the data used to generate page insights is available at: https://pl.linkedin.com/legal/privacy-policy).
11. The LinkedIn Data Protection Officer may be contacted via the form available at: https://www.linkedin.com/help/linkedin/ask/TSO-DPO.

III. J. FACEBOOK

1. Akati is the controller of the personal data of users of the products and services offered by Meta Platforms Ireland Limited, a company with its registered office at 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland, who visit the Controller's Company Page, available at: https://www.facebook.com/SeePlacescom/ (hereinafter referred to as the 'Fanpage'). As the Controller, Akati is responsible for the security of the personal data provided and for processing it in accordance with the law.

2. The Controller processes the personal data of users who visit the Fanpage while using Meta's products and services. This data is processed:
    1) in connection with the operation of the Fanpage, including for the purpose of promoting its own brand (legal basis: Article 6(1)(f) of the GDPR – legitimate interest);
    2) for the purpose of responding to questions submitted via Messenger or other services provided by Meta (legal basis: Article 6(1)(f) of the GDPR (legitimate interest); and if users provide special categories of data (e.g. health information), they are declaring their consent to the use of such data for the proper handling of the submission, in order to respond to the enquiry and for communication purposes (legal basis: Article 9(2)(a) of the GDPR – consent).
3. The Controller has the right to process:
    1) publicly available personal data (such as username, profile photo and activity status on Facebook or Messenger); comment content and other information that the user has shared publicly using Meta's products and services.
    2) personal data provided by users visiting the Fanpage, including information shared in their profile, as well as other content, comments, messages and communications (e.g. photos, videos, contact details, information on interests or worldview beliefs, place of residence);
    3) other personal data provided by the user in messages sent via Messenger or other Meta services (including contact details, health information, etc.), in order to respond to submitted enquiries or fulfil requests for contact.
4. The scope of personal data processing, specific purposes and the rights and obligations of users of Meta's products and services arise directly from:
    1) the terms and conditions governing the user's access to and use of Facebook, Messenger and other Meta products, websites, features, applications, services, technologies and software (available at: https://www.facebook.com/legal/terms), and
    2) the 'Privacy Policy' (available at: https://www.facebook.com/policy), or
    3) or applicable legal provisions

    – which are further clarified by the actions taken by the user on the Facebook social networking site.
5. The Controller is entitled to process personal data for the period necessary to achieve the above purposes. Depending on the legal basis, this shall be:
    1) the period until an objection is raised (or the Facebook user account is deleted);
    2) the period until consent is withdrawn (or the Facebook user account is deleted); withdrawal of consent does not affect the lawfulness of data processing carried out before the withdrawal;
    3) the period necessary to handle the inquiry submitted by the user via Messenger or other Meta services.
6. The catalogue of recipients of personal data processed by the Controller depends primarily on the scope of products and services used by the Facebook user, but also on the user's consent or legal provisions. Once all data security safeguards are in place, the Controller may transfer a user's personal data to other entities, including data processors acting on the Controller's behalf, such as technical service providers, entities providing advisory services (including law firms) and business partners providing services to the Controller under concluded agreements.
7. The Controller will not transfer the personal data of users of Meta products and services to countries outside the European Economic Area (i.e. countries other than EU Member States, Iceland, Norway and Liechtenstein).

8. The Controller may process the personal data of users of Meta products and services who visit the Fanpage to analyse how users interact with the controller's page and related content (for statistical purposes), in cases where interaction with the Fanpage and related content triggers a page statistics event involving the processing of personal data (legal basis: Article 6(1)(f) of the GDPR – legitimate interest).
9. In the case of personal data processed for the purpose of compiling statistics on user activity on the Fanpage (including following or unfollowing the Page, recommending the Page in a post or comment, liking or unliking the Page or a post), Akati and Meta act as joint controllers of users' personal data. The types of data, scope of processing, privacy principles and user rights are defined in:
    1) this document;
    2) in the 'Privacy Policy' document published at: https://www.facebook.com/policy;
    3) in the 'Information about Page Insights' document published at:
    https://www.facebook.com/legal/terms/page_controller_addendum.
10. Meta is responsible for informing users of Meta products and services about the processing of their data for page insight purposes and for enabling them to exercise their rights under the GDPR (information about the data used to create Page statistics is available at: https://www.facebook.com/legal/terms/information_about_page_insights_data).
11. Meta's Data Protection Officer can be contacted via the form available at: https://www.facebook.com/help/contact/540977946302970.

III. K. INSTAGRAM

1. Akati is the controller of the personal data of users of the products and services offered by Meta through the Instagram platform, as well as visitors to the controller's business profile, which is available at: https://www.instagram.com/seeplacescom/ (hereinafter referred to as the 'Business Profile'). As the Controller, Akati is responsible for the security of the personal data provided and for processing it in accordance with the law.
2. The Controller processes the personal data of users who visit the Business Profile while using Meta's products and services. This data is processed:
    1) in connection with operating the Business Profile, including for the purpose of promoting its own brand (legal basis: Article 6(1)(f) of the GDPR – legitimate interest);
    2) for the purpose of responding to enquiries submitted via Instagram or other services provided by Meta (legal basis: Article 6(1)(f) of the GDPR (legitimate interest); and where the user provides special categories of data (e.g. health information), they declare their consent to the use of such data for the proper handling and processing of their submission,
    including communication and responses (legal basis: Article 9(2)(a) of the GDPR – consent).
3. The Controller has the right to process:
    1) publicly available personal data (such as username, profile photo, Instagram activity status), content of comments and other information that users share publicly using Meta's products and services on Instagram;
    2) personal data provided by users who visit the Business Profile, including information shared on the user's profile, as well as other content, comments, messages and communications (e.g. photos, videos, contact information, details about interests or worldview beliefs, place of residence).

3) other personal data provided by users in messages sent via Instagram or other Meta services (including contact details, health-related data, etc.), for the purpose of responding to an enquiry or fulfilling a contact request.

4. The scope of personal data processing, specific purposes and the rights and obligations of users of Meta's products and services arise directly from:
    1) Instagram's Terms of Use (the document is available at: https://help.instagram.com/581066165581870) and
    2) 'Privacy Policy' (available at: https://privacycenter.instagram.com) or
    3) or applicable legal provisions

    – which are further clarified by the actions taken by the user on the Instagram social networking site.
5. The Controller is entitled to process personal data for the period necessary to achieve the above purposes. Depending on the legal basis, this shall be:
    1) the period until an objection is raised (or the Instagram user account is deleted);
    2) the period until consent is withdrawn (or the Instagram user account is deleted); withdrawal of consent does not affect the lawfulness of data processing carried out before the withdrawal;
    3) the period necessary to handle the inquiry submitted by the user via Instagram or other Meta services.
6. The catalogue of recipients of personal data processed by the Controller depends primarily on the scope of products and services used by the Instagram user, but also on the user's consent or legal provisions. Once all data security safeguards are in place, the Controller may transfer the personal data of a user visiting the Business Profile to other entities, including data processors acting on behalf of the Controller, such as providers of technical and advisory services (including law firms), as well as business partners performing services for the Controller under concluded agreements.
7. The Controller will not transfer the personal data of users of Meta products and services to countries outside the European Economic Area (i.e. countries other than EU Member States, Iceland, Norway and Liechtenstein).
8. The Controller may process the personal data of users of Meta's products and services who visit the Business Profile for the purpose of analysing how users interact with the Controller's page and related content (for statistical purposes), in cases where interaction with the Fanpage and related content triggers a page statistics event involving the processing of personal data (legal basis: Article 6(1)(f) of the GDPR – legitimate interest).
9. In the case of personal data processed for the purpose of compiling statistics on user activities on the Business Profile (including following or unfollowing the Business Profile, recommending the Business Profile in a post or comment, liking or unliking the Business Profile or a post), Akati and Meta act as joint controllers of the personal data of users. The types of data, scope of processing, privacy principles and user rights are defined in:
    1) this document;
    2) in the 'Privacy Policy' document published at: https://privacycenter.instagram.com/policy,
    3) 'Information about Page Insights', published at: https://www.facebook.com/legal/terms/page_controller_addendum.
10. Meta is responsible for informing users of Meta products and services about the processing of their data for page insight purposes and for enabling them to exercise their rights under the GDPR

(information about the data used to create Page statistics is available at: https://www.facebook.com/legal/terms/information_about_page_insights_data).

11. Meta's Data Protection Officer can be contacted via the form available at: https://www.facebook.com/help/contact/540977946302970.

III. L. YOUTUBE

1. Akati is the controller of the personal data of users of the products and services offered by Google Ireland Limited (hereinafter: Google), a company with its registered office at Gordon House, Barrow Street, Dublin, D04 E5W5, Dublin, Ireland, within the YouTube service and who visit the Controller's company page, which is available at: https://www.youtube.com/channel/UCV-Q_jlzD32ESqnCQsMy5YQ (hereinafter referred to as the 'Brand Account Channel'). As the Controller, Akati is responsible for the security of the personal data provided and for processing it in accordance with the law.
2. The Controller processes the personal data of users who visit the Brand Account Channel when using the products and services provided via YouTube. This data is processed:
    1) in connection with operating the Brand Account Channel, including for the purpose of promoting its own brand (legal basis: Article 6(1)(f) of the GDPR – legitimate interest);
    2) for the purpose of responding to questions asked via YouTube or other services offered by Google (legal basis: Article 6(1)(f) of the GDPR (legitimate interest); and where the user provides special categories of data (e.g. health information), the user declares their consent to the use of such data to handle the submission properly and respond to the enquiry, including for the purpose of communication and providing responses (legal basis: Article 9(2)(a) of the GDPR – consent).
3. The Controller has the right to process:
    1) publicly available personal data (such as username, profile photo, YouTube activity status), content of comments and other information made publicly available by the user while using YouTube products and services;
    2) personal data provided by users visiting the Brand Account Channel, including information shared in user profiles, comments, messages and other content (e.g. photos, videos, contact details, information on interests or worldview beliefs, place of residence);
    3) other personal data provided by users in messages sent via YouTube or other Google services (including contact details, health data, etc.), in order to respond to enquiries or fulfil contact requests.
4. The scope of personal data processing, detailed purposes and the rights and obligations of YouTube service users arise directly from:
    1) the 'Community Guidelines' document (available on the YouTube website at: https://www.youtube.com/intl/ALL_pl/howyoutubeworks/policies/community-guidelines/),
    2) the 'Google Privacy Policy – Privacy & Terms' document (available on Google's website at: https://policies.google.com/privacy) or
    3) or applicable legal provisions

    – which are further clarified by the actions taken by the user on YouTube.
5. The Controller is entitled to process personal data for the period necessary to achieve the above purposes. Depending on the legal basis, this shall be:
    1) the period until an objection is raised (or the YouTube user account is deleted);

2) the period until consent is withdrawn (or the YouTube user account is deleted); Withdrawal of consent does not affect the lawfulness of data processing carried out while the consent was in force.

3) the period necessary to handle an enquiry sent via YouTube or other Google services.

6. The catalogue of recipients of personal data processed by the Controller primarily results from the scope of products and services used by the YouTube user, but also from the user's consent or legal provisions. Once all data security safeguards are in place, the Controller may transfer the personal data of users visiting the Brand Account Channel to other entities, including data processors acting on behalf of the Controller, such as technical and advisory service providers (including law firms), as well as business partners providing services to the Controller under concluded agreements.
7. The Controller will not transfer the personal data of users of YouTube products and services to countries outside the European Economic Area (i.e. countries other than EU Member States, Iceland, Norway and Liechtenstein).
8. The controller may process personal data of users using YouTube products and services who visit the Brand Account Channel to analyse how users interact with the controller's site and related content (for statistical purposes) – in cases where user activity on the Brand Account Channel and related content triggers an event for page statistics that involves the processing of personal data (legal basis: Article 6(1)(f) of the GDPR – legitimate interest).
9. In the case of personal data processed for the purpose of generating statistics on user activity on the Brand Account Channel (including following or unfollowing the Brand Account Channel, recommending the Brand Account Channel in a post or comment, liking a video or removing a like), Akati and Google act as separate controllers of users' personal data. The types of data, scope of processing, privacy principles and user rights are defined in:
    1) this document;
    2) the 'Google Privacy Policy – Privacy & Terms' document, published at Google's website at: https://policies.google.com/privacy);
10. Google is responsible for notifying users of YouTube products and services about the processing of data for the purpose of generating statistics, and for enabling users to exercise their rights under the GDPR (information on data used to generate page statistics is available at: https://policies.google.com/privacy).
11. The Google Data Protection Officer may be contacted at: data-protection-office@google.com.

III. M. TIKTOK

1. Akati is the controller of the personal data of users of the products and services offered by TikTok Technology Limited (TikTok Ireland) and TikTok Information Technologies UK Limited (TikTok UK) within TikTok, as well as users who visit the Controller's TikTok Business Account, which is available at: https://www.tiktok.com/@seeplacescom (hereinafter referred to as the 'Brand Channel'). As the Controller, Akati is responsible for the security of the personal data provided and for processing it in accordance with the law.
2. The Controller processes the personal data of users who visit the TikTok Brand Channel when using the products and services provided via TikTok. This data is processed:
    1) in connection with operating the TikTok Brand Channel, including for the purpose of promoting its own brand (legal basis: Article 6(1)(f) of the GDPR – legitimate interest);
    2) for the purpose of responding to questions submitted via services offered by TikTok (legal basis: Article 6(1)(f) of the GDPR – legitimate interest); where users provide special categories of personal data (e.g. information about health), they are declaring that they consent to the use of such data for the proper handling of submissions and responses,

including communication and providing answers (legal basis: Article 9(2)(a) of the GDPR – consent).

3. The Controller has the right to process:
    1) publicly available personal data (such as username, profile photo), content of comments and other information made publicly available by the user while using TikTok products and services;
    2) personal data provided by users visiting the TikTok Brand Channel, including data shared in their profile, as well as other content, comments, messages and communications (e.g. photos, videos, contact details, etc.);
    3) other personal data provided by users in messages sent via TikTok (including contact details and health data) for the purpose of responding to enquiries or fulfilling contact requests.
4. The scope of personal data processing, detailed purposes and the rights and obligations of users of TikTok products and services arise directly from:
    1) TikTok's Terms and Conditions (available on the TikTok website at: https://www.tiktok.com/legal/terms-of-service-eea?lang=pl) and
    2) privacy policy (available on the TikTok website at: https://www.tiktok.com/legal/privacy-policy-eea?lang=pl) or
    3) or applicable legal provisions

    – which are further clarified by the actions taken by the user on TikTok.
5. The Controller is entitled to process personal data for the period necessary to achieve the above purposes. Depending on the legal basis, this shall be:
    1) the period until an objection is raised (or the TikTok user account is deleted);
    2) the period until consent is withdrawn (or the TikTok user account is deleted). Withdrawal of consent does not affect the lawfulness of data processing carried out while the consent was in force.
    3) the period necessary to handle the inquiry submitted by the user via TikTok services.
6. The catalogue of recipients of personal data processed by the Controller primarily results from the scope of products and services used by the TikTok user, but also from the user's consent or legal provisions. Once all data security safeguards are in place, the Controller may transfer the personal data of users visiting the TikTok Brand Channel to other entities, including data processors acting on behalf of the Controller, e.g. providers of technical services and advisory service providers (including law firms), and contractors providing services to the Controller under concluded agreements.
7. The Controller will not transfer the personal data of users of TikTok products and services to countries outside the European Economic Area (i.e. countries other than EU Member States, Iceland, Norway and Liechtenstein).
8. The Controller may process the personal data of users of TikTok products and services who visit the TikTok Brand Channel, in order to analyse how users interact with the Controller's page and associated content (for statistical purposes), provided that visiting the TikTok Brand Channel and related content triggers a page statistics event involving the processing of personal data (legal basis: Article 6(1)(f) of the GDPR – legitimate interest).
9. In the case of personal data processed for the purpose of compiling statistics on user activity on the TikTok Brand Channel (e.g. following or unfollowing the account, mentioning TikTok in a post or comment, liking or unliking a video), TikTok Ireland and TikTok UK (acting as joint controllers) and Akati are separate controllers of users' personal data. The types of data, scope of processing, privacy principles and user rights are defined in:

1) this document;
2) TikTok's privacy policy, available at: https://www.tiktok.com/legal/page/eea/privacy-policy/en;

10. TikTok is responsible for informing users of TikTok products and services about the processing of personal data for page statistics purposes, and for enabling users to exercise their rights under the GDPR. Information about data used to generate page statistics is available at: https://www.tiktok.com/legal/privacy-policy-eea?lang=en).
11. TikTok's Data Protection Officer can be contacted via the website: https://www.tiktok.com/legal/report/DPO.

IV DATA COLLECTED AUTOMATICALLY

1. The Controller collects information obtained automatically (so-called 'event logs').
2. The event logs record data relating to user sessions when using the services provided via the Website and the Application (in particular: IP address, date and time of visit, information about the web browser and operating system, type and name of the device).
3. Data recorded in the event logs is not linked to specific individuals.
4. Access to the contents of the event logs is restricted to persons authorised by the Controller to administer the Service.
5. The chronological record of event information serves solely as an auxiliary resource for administrative purposes. The analysis of event logs allows, in particular, the detection of threats, the provision of appropriate security for the Service and the Application, and the creation of statistics to provide insight into how users interact with the website and mobile application.
6. The Controller uses data concerning user sessions to diagnose problems relating to the functioning of the Service and the Application, analyse potential security breaches, manage the Service and the Application, and generate statistics (legal basis: Article 6(1)(f) of the GDPR – legitimate interest).
7. We use cookies and similar tracking technologies within the Service and the Application. More information can be found in the 'Cookie Policy'.

V. FINAL PROVISIONS

1. This Privacy Policy is for informational purposes only and applies in particular to the Platform available at https://seeplaces.com and the SeePlaces mobile application.
2. The Service and the Application may contain tools and plug-ins from third parties, such as Google Play and the App Store, as well as links to the websites of other entities, including social media platforms (e.g. Facebook, Instagram and LinkedIn), service providers and Akati's business partners. The Controller recommends that each user read the privacy policies applicable to external websites upon entering them.
3. The Controller reserves the right to make changes to this Privacy Policy, particularly in the event of:
    1) technological developments;
    2) changes to generally applicable laws, including those relating to personal data protection or information security;
    3) development of the Service and the Application, including the implementation of new services and functionalities.
4. The Controller will inform users of any relevant changes to this Privacy Policy by posting a notice on the Service and sending an email to users with active accounts on the Application.
5. This version of the 'Privacy Policy' comes into effect on 23 July 2025.