We Love Budapest Limited Liability Company (Kft.)

Privacy and Data Processing Notice

I. Purpose and Scope of the Notice

1.1 The purpose of this Notice is to record the principles of data protection and data management applied by We Love Budapest Limited Liability Company (Kft.), as well as the company's data protection and management policy, which the company, as the data controller, recognises as binding.

1.2 This Notice contains the principles for the management of personal data provided by users on the Services' websites.

1.3 When formulating the provisions of this Notice, the company paid special attention to the provisions of Regulation 2016/679 of the European Parliament and Council (the "General Data Protection Regulation" or "GDPR"), Act CXII of 2011 on the right to information self-determination and freedom of information ("Infotv."), Act V of 2013 on the Civil Code ("Ptk."), Act XLVIII of 2008 on the basic conditions and certain limitations of economic advertising activity ("Grtv."), Act CVIII of 2001 on electronic commerce services and certain aspects of services related to the information society, and Act C of 2000 on accounting (concerning the issuance and retention of documents).

1.4 Unless otherwise stated, the scope of this Notice does not extend to services and data processing carried out in connection with the promotions, sweepstakes, services, other campaigns, and content published by third parties advertising on or otherwise appearing on the websites referenced below in this Notice. Similarly, unless otherwise stated, the scope of this Notice does not cover the services and data processing of websites and service providers linked from the websites under the scope of this Notice. For such services, the provisions in the privacy notices of the third-party service providers apply, and the Data Controllers accept no responsibility for these data processing activities.

II. Definitions

2.1 Data Processing: Any operation or set of operations performed on Personal Data, regardless of the method used, such as collecting, recording, organising, structuring, storing, transforming, altering, using, retrieving, consulting, using, disclosing, transmitting, distributing or otherwise making available, publishing, coordinating or combining, restricting, deleting, and destroying Personal Data.

2.2 Data Controller: The entity that, alone or jointly with others, determines the purposes and means of Data Processing.
For the Services referenced in this Notice, the following entities qualify as Data Controllers:

- **We Love Budapest Limited Liability Company** (1036 Budapest, Lajos utca 48-66; registered by the Metropolitan Court of Registration, company registration number: 01-09-174253; tax number: 24381383-2-41; hereinafter: "Data Controller1")
- **Indamedia Support Closed Joint-Stock Company** (1036 Budapest, Lajos utca 48-66; registered by the Metropolitan Court of Registration, company registration number: 01-10-045996; tax number: 14307544-2-41; hereinafter: "Data Controller2").

Both Data Controllers are economic entities registered in Hungary.
Data Controller 1 operates the Websites, primarily providing media content services and the Services accessible through the Website related to its main activities.
Data Controller 2 primarily provides IT services related to the provision of Services.

The Data Processing activities described in this Notice constitute joint data processing under the GDPR because the Personal Data provided by the User during registration for a specific Service on the Website and during the use of the given Website is transferred by one Data Controller to the other, who processes it to provide the Service. The tasks and responsibilities regarding joint data processing are defined in an agreement between the Data Controllers. According to this, each Data Controller is responsible for its own Data Processing activities, especially for ensuring that the Personal Data collected is lawfully made available to the other Data Controller. Regardless of the conditions of the agreement referred to here, the User may exercise their rights under the GDPR concerning and against each Data Controller.

The data processing activities conducted by Data Controller 2 are governed by its own privacy notice, which can be found at: http://indamediasupport.hu/adatkezeles.

2.3 Personal Data: Any information concerning an identified or identifiable natural person.

2.4 Data Processor: A service provider that processes Personal Data on behalf of the Data Controller. In the case of the services referenced in this Notice, Data Processors may include:

Name	Address	Service	Link for Privacy and Data Management Notice
Magex Solutions Kft.	1133 Budapest, Váci út 76.	IT, development, operational, and hosting services	https://www.magex.hu/adatvedelmi-nyilatkozat
Wildom Informatikai Kft.	1146 Budapest, Hermina út 17.	IT, development, operational, and hosting services	https://wildom.com/
Indamedia Sales Kft.	1036 Budapest, Lajos utca 48-66. E ép.	media advertising space sales services	https://ajanlat.indamediasales.hu/adatvedelem/Indamedia_Sales_Adatkezelesi_Tajekoztato
Dialogue Creatives Kft.	1036 Budapest, Lajos utca 48-66. E ép.	services related to social media platforms	https://dialoguecreatives.com/privacy-statement/
Hotjar Limited	Level 2 St. Julian's Business Centre, 3 Elia Zammit Street, ST Julian's STJ 1000, Malta	user behavior analysis service	https://www.hotjar.com/legal/support/dpa/
Facebook Ireland Ltd.	4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Írország	in connection with the websites' Facebook pages	https://www.facebook.com/privacy https://www.facebook.com/about/privacy/update
Google LLC.	18 Lower Leeson Street, Dublin 2, DO2 HE97, Írország	providing statistical data related to user activity and serving advertisements	https://policies.google.com/privacy?hl=hu&gl=hu

2.5 Website(s): The websites welovebudapest.com, welovebudapest.com/en, welovebalaton.hu and their subpages, operated by Data Controller 1.

2.6 Service(s): The online publications operated by Data Controller 1, as well as the services provided by the Data Controller, which are available on the Websites, and participation in events organised by the Data Controller.

2.7 User: A natural person who registers for the Services and, in doing so, provides the data listed in Section III below.

2.8 External Service Provider: Third-party service providers, either directly or indirectly, engaged by the Data Controllers in connection with the operation of the individual Websites or the provision of the Services available through the Websites, to whom Personal Data is or may be transferred for the purpose of providing their services, or who may transfer Personal Data to the Data Controllers. External service providers also include those that do not cooperate with any of the Data Controllers but, by accessing the Websites of the Services, collect data about the Users, which, either on their own or in combination with other data, may be used to identify the User.

2.9 Notice: This privacy notice of Data Controller 1.

III. Scope of Processed Personal Data, Purpose, and Legal Basis of Data Processing

3.1 Data Processing Related to Website Visits

3.1.1 When a User visits a page of one of the Websites, the system of Data Controller 2 automatically records the User's IP address. In this case, the purposes of the data processing are to ensure the security and technical development of the IT system, protect the rights of the data subjects, and enforce the legitimate interests of the Data Controller. The data is recorded without the User's explicit consent as it is necessary for the lawful provision of the service (e.g., to filter out illegal use or content).

3.1.2 Data Controller 1 handles the personal data of natural persons involved in content creation, either as sources or by being referenced in edited content. The Personal Data most commonly processed by Data Controller 1 may include the person's name, position, workplace, age, residence information, or other data that indicates how the person is related to the topic of the edited content. The purpose of this data processing is to provide content. The legal basis for this processing may be Data Controller 1's legitimate interest, as well as ensuring the fundamental rights to information and freedom of expression, within the framework defined by laws. Additionally, the Data Controller may request the data subject's consent, in which case data processing will primarily be based on the consent.

3.2 Additional Services Available Through the Website

3.2.1 If the User consumes content available on the Website after registration, Data Controller 2 may process the following Personal Data of the User: name, nickname, profile picture, email address, secondary email address, last login IP address, last login timestamp. In this case, the purposes of the data processing are to identify the User's rights (the Services the User can access), to provide the Services, to protect the rights of the data subjects, to ensure the security and technical development of the IT system, to create statistics, and to enforce the legitimate interests of the Data Controller. The data is recorded and processed for the lawful provision of the service (e.g., to filter out illegal use or content). Personal data is processed based on the User's voluntary, prior, informed declaration, which includes the User's express consent to the use of the personal data provided during the use of the site. The User may withdraw consent at any time; however, this does not affect the lawfulness of the data processing before the withdrawal.

3.2.2 If the User sends an email (e.g., message, reader letter) to any of the Data Controllers, the relevant Data Controller records the User's email address and processes it to the extent and for the duration necessary to provide the service. The purpose of data processing is to fulfil the User's request. Data processing is based on the User's consent.

3.2.3 If the User voluntarily links their Facebook account with their Indapass account, the Data Controllers may process the following additional Personal Data: Facebook profile name, Facebook profile URL, Facebook profile ID, Facebook profile picture, Facebook email address, Facebook-provided address, Facebook-provided gender, birthday, bio, and website URL. In this case, the purposes of data processing are to identify the User's rights (the Services the User can access), to provide the Services, to protect the rights of the data subjects, to ensure the security and technical development of the IT system, to create statistics, and to enforce the legitimate interests of the Data Controller. Personal data is processed based on the User's voluntary consent.

3.2.4 If the User has consented, Data Controller1 will send newsletters to the User. In this case, Data Controller1 processes the User's name and email address and may collect additional data about the User (such as interests, content consumption habits, and demographics) using surveys. In these cases, the purposes of data processing may include contacting the User, preparing statistics, and analyses. Data processing is based on the User's consent.

3.2.5 If the User registers for an event organised by Data Controller 1, Data Controller 1 may process the User's name and email address in connection with the event. In these cases, the purposes of data processing may include identifying the User, contacting the User, handling individual requests, and preparing statistics and analyses. Data processing is based on the User's voluntary consent.

3.2.6 If the User participates in a sweepstake organised by Data Controller 1, Data Controller 1 may process the User's name and email address in connection with the sweepstake. In these cases, the purposes of data processing may include ensuring the User's participation in the sweepstake, drawing the winner, communicating with the winner, and delivering the prize. The legal basis for the data processing is the User's voluntary consent, and for sweepstakes, there may be legal obligations for accounting record retention.

3.3 Regardless of the above, a service provider technically related to the operation of the Services may conduct data processing on one of the Websites without the Data Controller's knowledge. Such activities are not

considered data processing carried out by the Data Controllers. The Data Controllers will make every effort to prevent and filter out such data processing activities.

3.4 The User guarantees that they have legally obtained the consent of the natural persons for any personal data they provide or make accessible about others during the use of the services (e.g., during the publication of User-generated content). The User is solely responsible for any User-generated content uploaded or shared through the services.

3.5 When providing their email address and other registration data (e.g., username, ID, password), the User takes responsibility for ensuring that only they use the services with the provided email address and data. Accordingly, any liability related to any access made with a given email address and/or data falls solely on the User who registered the email address and provided the data.

IV. Additional Data Handled by Data Controllers

4.1 Use of Cookies

The Data Controllers place a small data package, known as a "cookie," on the User's computer for personalised service. The purpose of the cookies is to ensure the high-quality functioning of the site, to provide personalised services, and to enhance the user experience. The User has the right to delete the cookies from their computer and can set their browser to refuse cookies. The User acknowledges that without cookies, the operation of the site may not be fully functional.

4.2 Personal Data Collected via Cookies

When providing personalised services, the Data Controllers handle the following Personal Data through the use of cookies:

- Interest-related information
- Habits
- Preferences (based on browsing history)

4.3 Collection of Reading Habits

From time to time, the Data Controllers collect information about Users' reading habits to optimise the design of the Websites. In this process, the Data Controllers handle Users' IP addresses, which are anonymised at the beginning of the process, thus preventing the identification of individual Users. The data is processed and evaluated in aggregated and averaged form.

4.4 Technical Data Recording

During the operation of systems, data generated by the User's logging-in computer is automatically recorded, which is generated while accessing the Service. The system logs the automatically recorded data without the User's separate statement or action upon logging in and out.

V. Principles and Methods of Data Processing

5.1 Transparency and Legal Compliance

The Data Controllers process Personal Data in accordance with the principles of good faith, fairness, transparency, and the applicable legal regulations and provisions of this Information.

5.2 Purpose-Limited Data Processing

The Data Controllers only use the necessary Personal Data based on the consent of the concerned User and solely for specific purposes.

5.3 Changing Purposes

The Data Controllers only process Personal Data for the purposes defined in this Information and relevant legal regulations. If the Data Controllers wish to use the Personal Data for a purpose other than the original data collection purpose, they will inform the User and obtain prior explicit consent.

5.4 Data Accuracy

The Data Controllers do not verify the accuracy of the provided Personal Data. The person providing the data is solely responsible for its accuracy.

5.5 Data Processing for Minors

Personal data of individuals under the age of 16 can only be processed with the consent of a legal guardian. The Data Controller is not able to verify the legitimacy of the consenting person's rights or the content of their statement; therefore, the User and the legal guardian guarantee that the consent complies with legal requirements. In the absence of a consent statement, the Data Controller does not collect Personal Data related to individuals under the age of 16, except for the IP address used during the Service usage, which is automatically recorded due to the nature of online services.

5.6 Disclosure to Third Parties

The Data Controllers do not disclose the Personal Data they process to third parties, except in cases where the data is used in aggregated statistical form that cannot identify individual Users. In certain cases, such as official court or police requests, legal proceedings regarding copyright, property rights, or other legal violations or the suspicion thereof, the Data Controllers may make the accessible Personal Data of the affected User available to third parties.

5.7 User Activity Data

The Data Controllers may collect data about User activity, which cannot be linked to the other data provided by Users during registration or data generated when using other websites or services.

5.8 Notification Obligation

The Data Controllers will notify the affected User about the correction, restriction, or deletion of the Personal Data they handle, as well as all those who have previously received the Personal Data for processing purposes. Notification may be omitted if it does not violate the affected User's legitimate interests concerning the purpose of processing.

5.9 Data Security

The Data Controllers ensure the security of Personal Data, taking technical and organisational measures to prevent accidental loss, unlawful destruction, unauthorised access, unlawful use, and unauthorised alteration or dissemination of the data. To fulfil this obligation, the Data Controllers will call upon any third parties to whom Personal Data is transmitted.

5.10 Data Protection Officer

In accordance with the relevant provisions of the GDPR, the Data Controllers are not obliged to appoint a Data Protection Officer.

VI. Duration of Data Processing

6.1 The Data Controllers will store the automatically recorded IP addresses for a maximum of 7 days after their recording.

6.2 In the case of emails sent by the User, if the User does not have a registration, the contacted Data Controller will delete the email address 90 days after the closure of the matter referred to in the inquiry, unless the Data Controller has a legitimate interest in further processing the Personal Data in a specific case, which will be valid until the Data Controller’s legitimate interest no longer exists.

6.3 The processing of Personal Data provided by the User will remain valid as long as the User does not unsubscribe from the Service with the given username or otherwise request the deletion of the Personal Data. In this case, the Personal Data will be deleted from the systems of the Data Controllers. The Personal Data provided by the User can be processed by the Data Controllers as long as the User does not explicitly request in writing that the processing of such data be terminated. The User's request for termination of data processing without unsubscribing from the Service does not affect their right to use the Service; however, it may occur that without Personal Data, they will not be able to access certain Services.

6.4 In the case of illegal, misleading use of Personal Data or a crime committed by the User, or in the case of an attack against the system, the Data Controllers are entitled to immediately delete the Personal Data of the User simultaneously with the termination of the User's registration. Additionally, in the case of suspicion of a crime or civil liability, the Data Controllers are entitled to retain the Personal Data for the duration of the proceeding.

6.5 During the operation of the system, data that is automatically and technically recorded will be stored for as long as necessary to ensure the operation of the system. The Data Controller ensures that these automatically recorded data cannot be linked to other Personal Data, except in cases mandated by law. If the User withdraws their consent to the processing of Personal Data or unsubscribes from the Service, their identity will not be identifiable concerning the technical data thereafter – excluding investigative authorities and their experts.

6.6 If a court or authority orders the deletion of Personal Data, the Data Controllers will carry out the deletion. Instead of deletion, the Data Controllers may restrict the use of the Personal Data with the User's notification if the User requests this or if it can be presumed from the available information that the deletion would violate the User's legitimate interest. The Data Controllers will not delete the Personal Data as long as the purpose of data processing, which excludes the deletion of the Personal Data, exists.

VII. Data Security and Knowledge of Personal Data

7.1 The Data Controller ensures the security of the Personal Data it handles and takes the technical and organisational measures necessary to enforce the relevant laws, data protection, and privacy regulations. The Data Controller protects the Personal Data with appropriate measures against unauthorised access, alteration, transmission, disclosure, deletion, or destruction, as well as against accidental loss and damage, including accessibility issues resulting from changes in applied technology.

7.2 The Data Controller maintains the Personal Data it handles in accordance with the relevant laws, ensuring that Personal Data can only be accessed by those employees and other persons acting on behalf of the Data Controller who need to know it for the performance of their job duties. The employees of the Data Controller will only conduct individual searches and specific operations on the data at the User's request or when necessary for the provision of the service.

7.3 When determining and applying measures for the security of Personal Data, the Data Controller considers the current level of technological development. The Data Controller will choose the solution that provides a higher level of protection for Personal Data from among several possible data processing solutions unless it would involve disproportionate difficulty. The Data Controller, in terms of its IT security tasks, ensures, in particular:

- Measures to protect against unauthorised access, including the protection of software and hardware tools, as well as physical protection (access protection, network protection);
- Measures to ensure the possibility of recovering data files, including regular backups and secure handling of copies (backup);
- Protection of data files against viruses (antivirus protection);
- Physical protection of data files and the devices that carry them, including protection against fire damage, water damage, lightning strikes, and other elemental damage, as well as the recoverability of damages caused by such events (archiving, fire protection).

7.4 Employees and other persons acting on behalf of the Data Controller are required to securely store and protect any data carriers containing Personal Data that they use or possess, regardless of how the data is recorded, against unauthorised access, alteration, transmission, disclosure, deletion, or destruction, as well as against accidental loss and damage.

7.5 The Data Controller operates the electronic record-keeping through an IT program that meets data security requirements. The program ensures that data can only be accessed in a controlled manner and for specific purposes by those who need it to perform their duties.

VIII. User Rights and Methods of Enforcement

8.1 Right to Access
The User may request any Data Controller to inform them whether their personal data is being processed, and if so, to provide access to the personal data they process. The personal data provided by the User related to the respective Service can be viewed in the settings of the access system for the Services or on the profile pages associated with each Service. Regardless of this, the User may request information about the processing of their personal data at any time, in writing, by sending a registered letter or a return-receipt letter to any of the Data Controllers, or by emailing adatvedelem@welovebalaton.hu or adatkezeles@indamediasupport.hu. The Data Controller will only consider the request sent by letter as authentic if the User can be clearly identified based on the request. An email request for information will only be considered authentic if it is sent from the User's registered email address; however, this does not exclude the possibility that the Data Controller may identify the User by other means before providing the requested information. The information request may extend to the User’s data processed by the Data Controllers, its source, the purpose of data processing, the legal basis, the duration of processing, the names and addresses of any Data Processors, activities related to data processing, and, in the case of data transfer, who has received or will receive the User's data and for what purpose.

8.2 Right to Rectification
The User may request the correction or modification of their personal data processed by the Data Controllers. Taking into account the purpose of data processing, the User may request the completion of incomplete personal data. The personal data provided by the User related to the respective Service can be modified in the settings of the access system for the Services or on the profile pages associated with each Service. Once the request for modification of personal data is fulfilled, the previous (deleted) data cannot be restored.

8.3 Right to Erasure
The User may request the deletion of their personal data processed by the Data Controllers. Deletion may be refused (i) for the purpose of exercising the freedom of expression and the right to information, or (ii) if the processing of personal data is authorised by law; and (iii) for the establishment, exercise, or defence of legal claims. The Data Controllers will inform the User of the reasons for any refusal of a deletion request. Once a request for the deletion of personal data is fulfilled, the previous (deleted) data cannot be restored. Newsletters sent by Data Controller 1 can be unsubscribed through the unsubscription link found in them. In the event of unsubscription, Data Controller 1 will delete the User's personal data from the newsletter database. In the event of the User's death, a close relative or any person who has received a bequest can request the deletion of the data concerning the User by providing a death certificate or sending a copy of it to the customer service address of the Service, along with proof of their relationship to the User.

8.4 Right to Restrict Processing
The User may request that the Data Controllers restrict the processing of their personal data if they dispute the accuracy of the data being processed. In this case, the restriction applies for the duration that allows the Data Controllers to verify the accuracy of the personal data. The Data Controllers will mark the personal data they process if the User disputes its correctness or accuracy, but the incorrectness or inaccuracy of the disputed personal data cannot be clearly established. The User may also request that the Data Controllers restrict the processing of their personal data if the processing is unlawful, but the User opposes the deletion of the personal data and instead requests the restriction of its use. The User may further request that the Data Controllers restrict the processing of their personal data if the purpose of processing has been achieved, but the User requires its processing by the Data Controllers for the establishment, exercise, or defence of legal claims.

8.5 Right to Data Portability
The User may request that the Data Controllers provide the personal data they have provided and that is processed automatically in a structured, commonly used, and machine-readable format and/or that it be transferred to another data controller.

8.6 Right to Object
The User may object to the processing of their personal data (i) if the processing of personal data is necessary solely for compliance with legal obligations imposed on the Data Controllers or for the enforcement of the

legitimate interests of the Data Controllers or a third party; (ii) if the purpose of processing is direct marketing, public opinion polling, or scientific research; or (iii) if the processing is carried out in the public interest. The Data Controllers will examine the legality of the User's objection, and if they determine the objection to be justified, they will cease processing and restrict the personal data being processed and will inform all parties to whom the affected personal data has previously been disclosed about the objection and the measures taken based on it.

IX. Data Processing

9.1 The Data Controllers engage the Data Processors named above in this Notice for the performance of their activities.

9.2 The Data Processors do not make independent decisions and are only authorised to act according to the contract concluded with the Data Controllers and the instructions received. The Data Controllers oversee the work of the Data Processors.

9.4 The Data Processors are only entitled to engage further data processors with the consent of the Data Controllers.

X. External Service Providers

10.1 In connection with the provision of the Services, the Data Controllers frequently engage External Service Providers with whom they cooperate. The Personal Data processed in the systems of the External Service Providers is governed by the data protection information provided by the External Service Providers. The Data Controllers will do everything within their power to ensure that the External Service Provider processes the Personal Data transmitted to them in accordance with applicable laws and uses it solely for the purpose specified by the User or recorded below in this Notice. The Data Controllers will inform Users about the data transfer to External Service Providers within the framework of this Notice.

10.2 External Service Providers Facilitating Registration or Login
The Data Controllers cooperate with External Service Providers that provide applications to facilitate registration and login for Users in connection with the provision of the Services. In this cooperation, certain Personal Data (e.g., IP address, email, registration name) may be transmitted to these External Service Providers by the Data Controllers and/or the Data Processors. These External Service Providers collect, process, and transmit Personal Data according to their own data protection policies.
The External Service Providers cooperating with the Data Controllers to facilitate registration or login include:

Name of Data Controller	Address of Data Controller	Access to Data Processing Notice
Facebook Ireland Ltd.	4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Írország	https://www.facebook.com/privacy

10.3 Web Analytics and Advertising Service External Providers
In connection with the pages of the Services, the Data Controllers cooperate with web analytics and advertising service External Providers. These External Providers may have access to the User's IP address, and in many cases, they use cookies, web beacons (web markers used to record the IP address and the visited webpage, which may appear on websites, emails, or mobile applications), click tags (markers that identify clicks on a specific advertisement), or other click measurement tools to facilitate the personalisation or analysis of the Services and to generate statistics.

Cookies placed by these External Providers can be deleted at any time from the User's device, and by selecting the appropriate settings in the browser(s), the use of cookies can generally be refused. Identification of cookies placed by External Providers can be done based on the domain associated with the particular cookie. There is no option to refuse web beacons, clicktags, or other click measurement tools.

These External Providers handle the Personal Data transmitted to them according to their own data protection notices.
The web analytics and advertising service External Providers cooperating with the Data Controllers include:

Adakezelő neve	Address of Data Controller	Access to Data Processing Notice

Digitális Közönségmérési Tanács Kft.	1053 Budapest, Kossuth Lajos utca 7-9.	http://www.gemius.hu/adatvedelmi-iranyelvek.html
Facebook Ireland Ltd.	4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Írország	https://www.facebook.com/privacy
Gemius Hungary Kft.	1053 Budapest, Szép utca 5. 1. em. 2.	https://adocean-global.com/en/company/privacy-policy/
Google Ireland Ltd.	18 Lower Leeson Street, Dublin 2, DO2 HE97	https://www.lobbying.ie/about-us/our-policies/privacy-cookies/
HOPPex Kft.	1137 Budapest, Jászai Mari tér 5-6.	http://hoppex.hu/adatvedelem/
Indamedia Sales Kft.	1036 Budapest, Lajos utca 48-66. E ép.	https://ajanlat.indamediasales.hu/adatvedelem/Indamedia_Sales_Adatkezelesi_Tajekoztato_2019.pdf
The Rubicon Project Ltd.	Walmar House 5th Floor 296 Regent St. London, W1B 3HR United Kingdom	https://rubiconproject.com/privacy-policy/

10.4 Facebook "Recommend" Button

Data Controller 1 places a Facebook "Recommend" button on its website related to certain content it edits, which allows Facebook the opportunity to collect personal data about Users who view that page. The purpose of placing the Facebook "Recommend" button is to enable Data Controller 1 to recommend content that aligns with the User's interests and to display such advertisements on its website.

By placing the Facebook "Recommend" button on the website, Data Controller 1 allows Facebook to collect data about Users who click the Recommend button using cookies. At the same time, Data Controller 1 has no information regarding whether Facebook correlates this data with other information it possesses about the Data Subjects. By clicking the Facebook "Recommend" button, the Data Subject accepts that they provide Facebook with the opportunity for data processing via cookies, which Data Controller 1 has no further influence over.

10.5 External Providers Offering Customized Messaging

Data Controller 1 collaborates with an External Provider that allows Users to access certain services they have used within the framework of the Services through other channels used by the same User (e.g., Facebook, Messenger, etc.). The External Provider can collect additional data about the User through the use of cookies and questionnaires, as well as the User's registration on the External Provider's website or interfaces, which may be capable of identifying the User either independently or in connection with other data.

These External Providers handle the Personal Data transferred to them according to their own privacy notices.

Name of Data Controller	Address of Data Controller	Access to Data Processing Notice
Facebook Ireland Ltd	4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Írország	https://www.facebook.com/privacy
Messenger	USA, Kalifornia, Menlo Park,	https://www.facebook.com/policy.php

There are External Providers with whom none of the Data Controllers have a contractual relationship or with whom they do not intentionally collaborate concerning the specific data processing. Nevertheless, these External Providers can access the Website/Services – either through the User's participation (e.g., linking their individual account to the Service) or without it—and thereby collect data about Users or user activities conducted on the Websites of the Services. This data may, in certain cases – either independently or when combined with other data collected by the External Provider – be capable of identifying the User. Such External Providers may include, but are not limited to:

Name of Data Controller	Address of Data Controller	Access to Data Processing Notice
Facebook Ireland Ltd.	Írország, Dublin 2, 4 Grand Canal Square, Grand Canal Harbour,	https://www.facebook.com/privacy https://www.facebook.com/about/privacy/update
Google Ireland Ltd.	18 Lower Leeson Street, Dublin 2, DO2 HE97, Írország	https://www.lobbying.ie/about-us/our-policies/privacy-cookies/
Instagram LLC.	Írország, Dublin, Grand Canal Dock Grand Canal Quay 4.	http://instagram.com/legal/privacy/ https://www.facebook.com/about/privacy/update
Infogram Software Inc.	USA, Kalifornia, San Francisco, CA 94107, Bryant Street 450	https://infogram.com/privacy
PayPal Holdings Inc.	USA, California, San Jose, North First Street 2211	https://www.paypal.com/us/webapps/mpp/ua/privacy-full
Pinterest Europe Ltd.	Palmerston House, 2nd Floor, Fenian Street, Dublin 2, Írország.	https://policy.pinterest.com/hu/privacy-policy
Playbuzz Ltd.	USA, New York City	https://www.playbuzz.com/PrivacyPolicy
Twitter International Company	Írország, Dublin, Fenian St 26.	https://twitter.com/en/privacy/previous/version_12

Viber Media LLC.	Luxemburg, Luxembourg 1536, Rue du Fossé 2.	https://www.viber.com/terms/viber-privacy-policy/
Vimeo INC.	USA, New York City, 10011, 555 West 18th St., 4th	https://vimeo.com/features/video-privacy
Yahoo! EMEA Ltd.	Írország, Dublin 1, North Wall Quay, Point Square 5-7.	https://policies.oath.com/ie/hu/oath/privacy/index.html
YouTube LLC.	USA, Kalifornia, San Bruno	https://policies.google.com/privacy?hl=hu

These External Providers handle the Personal Data transmitted to them according to their own privacy policies.

XI. Possibility of Data Transfer

11.1 The Data Controllers are entitled and obligated to transfer all Personal Data that is available to them and stored in compliance with regulations to the competent authorities if they are required to do so by law or a binding authority mandate. The Data Controllers cannot be held liable for such data transfers and the consequences arising from them.

11.2 The Data Controllers may transfer certain Personal Data to the Data Processors involved, considering the purpose of Data Processing. The Data Processors shall handle the received Personal Data in accordance with the provisions of the data processing contract concluded with the Data Controllers and may not use it for any other data processing purpose.

11.3 The Data Controllers will take all possible measures to ensure that External Providers do not have access to the Personal Data they manage, or only in a manner that does not allow the identification of the Data Subject.

11.4 The Data Controllers primarily engage the services of data processors operating within the EEA. However, regarding the identity of the Data Processors involved in the Data Processing, it cannot be completely ruled out that the data made available may be transferred to a country outside the EEA. To limit data transfers and enhance data security, the Data Controllers have primarily reviewed the technical settings applied, and in all cases where possible, they have excluded the possibility of further data transfer. Simultaneously, the Data Controllers have checked and continuously monitor that, where identification of the Data Subject based on the handled Personal Data is not necessary, the data will be anonymised as early as possible in the data processing phase and, where possible, will not be capable of identifying the Data Subject in any way—neither directly nor indirectly, nor through any association with other data.

11.5 If the Data Controller partially or wholly transfers the operation or utilisation of one or more Services found on the Services pages to a third party, it may transfer the Personal Data managed concerning the given Service to that third party partially or wholly without requiring the specific consent of the User, provided that the Users are properly informed in advance. However, this data transfer cannot place the User in a worse position than the data processing rules specified in the current version of this Notice. In case of data transfer, as specified in this point, the Data Controller will provide Users with the opportunity to object to the data transfer before it occurs. In the event of an objection, the transfer of that User's data according to this point is not possible.

XII. Modification of the Data Processing Notice

12.1 The Data Controller1 reserves the right to unilaterally modify this Notice at any time.

12.2 The User accepts the provisions of the Notice in effect upon their next login; furthermore, there is no need to request additional consent from individual Users.

XIII. Legal Remedies

13.1 Any inquiries or remarks related to data processing can be directed to the employees of the Data Controllers at the email address: adatvedelem@welovebudapest.hu or adatkezeles@indamediasupport.hu.

13.2 The User may direct their complaint regarding Data Processing directly to the National Authority for Data Protection and Freedom of Information (address: 1125 Budapest, Falk Miksa utca 9-11; phone: +36-1-391-1400; email: ugyfelszolgalat@naih.hu; website: www.naih.hu).

13.3 In case of violation of the User's rights, they may turn to the court. The jurisdiction for the trial is vested in the court. The trial may be initiated at the court corresponding to the User’s place of residence or habitual residence, at the User’s choice. Upon request, the Data Controllers will inform the User about the possibilities and means of legal remedy.

Budapest, January 1st, 2024