Hungarian Intellectual Property Office

21.10.2025

PRIVACY POLICY

ON ATTENDING CONFERENCES

ORGANISED BY THE HUNGARIAN INTELLECTUAL PROPERTY OFFICE

Table of Contents

I. Controllers of personal data:

Hungarian Intellectual Property Office (hereinafter the 'Office' or 'HIPO')

- address: 1081 Budapest, II. János Pál pápa tér 7.;
- postal address: 1438 Budapest, pf. 415.
- telephone number: 06-1/312-4400;
- e-mail address: sztnh@hipo.gov.hu.

Data Protection Officer's

- e-mail address: adatvedelem@hipo.gov.hu;
- phone number: 06-1/474-5941)

II. Purpose, categories, legal basis and duration of data processing:

1. Entry and guarantee the security of the attendees of the presidency events

The purpose of data processing	To ensure the admission to the presidency events and the security of the participants, in the framework of which the Controller may use your (the data subject's) data for the purposes of accreditation, logistic planning and security controls.
Categories of processed data:	Personal data given by you (the data subject) in the registration form or connected to it by other means of communication, for example • name, • surname, • delegation, • position, • representation (company, organization, country), • function (e.g. president), • photo, • date and place of birth, • country, • telephone number, • e-mail address, • optional programs chosen by the data subject
Legal basis of data processing:	your (the data subject's) consent [Article 6(1) point a) of GDPR]. You can withdraw your consent anytime. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.
Duration of data processing:	One year after the conference, unless a specific regulation does not require a longer retention period (e.g. transparency laws, contractual obligations)

2. Processing for the provision of special meals

Purpose of processing:	Protecting the life and health of the data subject by providing them with special meals.
Categories of processed data:	Name of the data subject, dietary preferences, dietary restrictions (e.g. allergies).
Legal basis of data processing:	The explicit consent of the data subject. [Articles 6(1)(a) and 9(2)(a) GDPR] You can withdraw your consent anytime. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.
Duration of data processing:	One month after the conference.

3. Ensuring accessibility and participation in conference venues for people with health problems and reduced mobility

Purpose of processing:	Ensuring the accessibility of the conference for the data subject (buses will take them to the conference venue) and ensuring access to, presence at and departure from the conference venue, safeguarding the health of the data subject
Categories of processed data:	Name of the data subject, the fact and circumstances of the accessibility need, health problems and reduced mobility, telephone number, accommodation address.
Legal basis of data processing:	The explicit consent of the data subject. [Articles 6(1)(a) and 9(2)(a) GDPR] You can withdraw your consent anytime. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.
Duration of data processing:	One month after the conference.

4. Online screening of conferences

Purpose of processing:	to enable remote participation, ensure accessibility, and facilitate the dissemination of the event's content to a broader audience. The screening may also serve documentation, transparency, and internal reporting purposes.
Categories of processed data:	Depending on the platform used and the configuration of the event, the following categories of personal data may be processed: • Identification data (e.g., name, email address, username) • Visual and audio recordings (e.g., video feed, voice, profile picture) • Interaction data (e.g., chat messages, questions asked, reactions) • Technical data (e.g., IP address, device information, connection logs)
Legal basis of data processing:	Participation: Article 6(1)(a) GDPR – data subject's consent You give your consent by attending the conference by this means. You can withdraw your consent anytime. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal. Documentation, transparency: Article 6(1)(e) GDPR – processing is necessary for the performance of a task carried out in the public interest

Duration of data processing:	Recordings and logs may be stored for a predefined period (e.g., 1 year) unless legal obligations or legitimate interests justify longer retention. Specific retention periods will be communicated in the detailed notice of each event.
Data processors, recipients	Microsoft Teams: The data processor ("Microsoft Corporation / Microsoft Ireland") can be contacted via the EU Data Protection Officer at One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland, tel. +353 1 706 3117, or via the webform at aka.ms/privacyresponse. Zoom: The data processor ("Zoom Video Communications, Inc.") can be reached through its Privacy Team at privacy@zoom.us. Its U.S. headquarters are located at 55 N Almaden Blvd, 6th Floor, San Jose, CA 95113, USA. Sales/support telephone: 1 888 799 9666.

III. Recipients of personal data, transfer of data

The personal data will be accessed and processed by the data processor contracted by the Office to organise and manage the event.

Processor's

- name: Lounge Design Kft.
- seat: 1025 Budapest, Felső Zöldmáli út 72.
- website contact details: https://lounge.hu/

In the event of a failure or other problem in the IT systems of the Office, the systems containing personal data may be accessed not only by the relevant staff of the Office but also by duly authorised staff of the data processors responsible for performing certain operational tasks of the IT infrastructure of the Office.

Processor's

- name: Novell Professzionális Szolgáltatások Magyarország Kft.
- seat: 1117 Budapest, Neumann János utca 1. A épület II. emelet
- website contact details: https://www.npsh.hu/

The log analysis for information security purposes to be carried out by the Office will also involve the duly authorised staff of the data processor entrusted with this task.

Processor's

- name: Valkyr Informatics Kft.
- seat: 2040 Budaörs, Edison utca 4.
- website contact details: https://www.invitech.hu/

The Office does not transfer personal data to other controllers, third countries or international organisations. If proceedings are instituted before a court or other authority which require the transfer of personal data or documents containing personal data to the court or authority, the court or authority may also have access to the personal data.

IV. Data security

The Office and its processors have the right to access the data subject's personal data to the extent necessary for the performance of their tasks or duties. The Office takes all security, technical and organisational measures necessary to ensure the security of personal data.

The Office allows access to its IT systems with access rights that can be linked to an individual. The principle of "necessary and sufficient rights" applies to the allocation of access, i.e. all users may use the IT systems and services of the Office only to the extent necessary for the performance of their tasks, with the corresponding rights and for the necessary duration. Only a person who is not restricted for security or other (e.g. conflict of interest) reasons and who has the professional, business and information security skills necessary to use the IT systems and services safely may have the right to access them.

The Office and its data processors are bound by strict confidentiality rules and are required to act in accordance with these confidentiality rules in the course of their activities.

The Office stores the data on its own equipment in a data centre. The IT tools that store the data are stored in a separate, locked server room with an alarm system, protected by a multi-level access control system with authorisation control.

The Office protects its internal network with multiple layers of firewall protection. The access points to the public networks used are always equipped with hardware border protection devices (firewalls). Data are stored by the Office on multiple servers to protect them from destruction, loss, damage due to malfunction of IT equipment, or from unlawful destruction.

The Office protects its internal networks from external attacks with multiple layers of active, complex malware protection (e.g. virus protection). Indispensable external access to the IT systems and databases operated by the Office is provided via an encrypted data connection (VPN).

The Office does its utmost to ensure that its IT tools and software are always in line with the technological solutions generally accepted in the market.

The Office is developing systems to control and monitor operations and detect incidents (such as unauthorised access) through logging.

V. Data subject's rights related to data processing

a) Right of access to personal data processed: the data subject has the right to obtain information about their processed personal data, the source of such data, the purpose, legal basis and duration of data processing, the circumstances and impacts of as well as the measures taken with a view to warding off any data protection incident, and in the event of any data transfer, the legal basis and recipients of such data transfer.
b) Right to rectification: the data subject has the right to request at any time the rectification of their personal data if they are incorrect, inaccurate or need to be supplemented.
c) Right to erasure: in a message sent to the Controller, the data subject may at any time request the erasure of their processed personal data. The data subject can only request the erasure of their personal data in the circumstances defined in the GDPR. A request for the erasure of data qualifies as withdrawal of the consent to data processing, in consequence of which the data subject's processed personal data will be erased with immediate effect.
d) Withdrawal of consent: in harmony with Article 7 of the GDPR, the data subject may at any time withdraw their consent to data processing. Such withdrawal will not affect the lawfulness of any data processing before the withdrawal.
e) Right to restriction of processing: If the data subject disputes the accuracy of their processed personal data, the data subject's personal data will be restricted at their request until the accuracy of such personal data is verified. If the time limit for the retention period of data set forth in Section II has expired or the processing of data is unlawful, the processed personal data will be erased. However, the data subject may request the continued storage of such data from the Controller – instead of the erasure of data – for the filing, enforcement and protection of legal claims. Any such request can be submitted in a written application sent by post; the data subject must state the legal claim to be enforced and the requested further period of storage.
f) Right to data portability: the data subject has the right to receive the personal data concerning them in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without this being hindered by the Controller to which such personal data have been made available.

The requests under points a) to f) can be sent to the e-mail address: adatvedelem@hipo.gov.hu or by post to the address indicated in Section I.

The Controller will meet any request for information, rectification, erasure due to the withdrawal of the data subject's consent to data processing as well as any request for restriction and data portability within thirty days of the receipt of such request, or if such request cannot be met, the Controller will notify the data subject of the fact thereof, stating the factual and legal reasons for refusal, as well as of the possibilities for a legal remedy.

If the Controller have well-founded doubts regarding the identity of the person submitting the request, they may request the information necessary for confirming the data subject's identity. Such instances include in particular if the data subject exercises their right to request a copy, in which case it is justified that the Controller ascertain whether the request originates from the person entitled.

VI. Data subject's possibilities for seeking an effective remedy related to data processing

In the event of a presumed unlawful processing, the data subject has the right

- to contact primarily the Controller as the processors of their personal data with a view to remedy the infringement,
- to lodge a complaint with the National Authority for Data Protection and Freedom of Information (1055 Budapest, Falk Miksa utca 9-11., ugyfelszolgalat@naih.hu, website: www.naih.hu), or
- to bring proceedings before a court, as set forth in Section 23 of the Freedom of Information Act, which will proceed with immediate effect. The Budapest-Capital Regional Court (Fővárosi Törvényszék, 1055 Budapest, Markó utca 27.) will have jurisdiction for hearing the case; however, at the data subject's discretion, the proceedings can also be brought before the tribunal with jurisdiction according to their place of residence or place of temporary residence.