Conference "Intellectual Property in the Age of Artificial Intelligence" (Budapest, 1-2 October 2024)

PRIVACY POLICY

As regards the data processed for the Conference "Intellectual Property in the Age of Artificial Intelligence" (Budapest, 1-2 October 2024) and the data processed on the Novento accreditation and logistic information platform of the Ministry for EU Affairs (hereinafter referred to as the "NOVENTO system").

Introduction

The Ministry for EU Affairs and the Hungarian Intellectual Property Office (hereinafter together referred to as "Controllers or Joint Controllers") hereby inform the persons registered via the NOVENTO system (hereinafter referred to as "data subjects") about the personal data processed by them, their practice regarding the processing of personal data, the organisational and technical precautions they adopt with a view to protecting personal data, the rights of registered persons as well as the method and possibilities for the exercise of such rights.

In every instance, the Controllers process the personal data placed at their disposal in accordance with the Hungarian and European data protection and data processing laws and ethical requirements, and take every technical and organisational precaution that may be necessary for safe data processing.

By supplying their personal data, the data subject accepts the terms and conditions laid down in the present privacy policy, and consents to the processing of their personal data. The Controllers will inform the data subjects about any changes in the privacy policy through the publication of the amended privacy policy.

This privacy policy only applies to the personal data of natural persons.

This privacy policy was drafted for the purpose of compliance with Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter referred to as the 'Freedom of Information Act') and 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").

I. Controllers

Controllers of personal data supplied for registration purposes:

- Ministry for EU Affairs (hereinafter the 'Ministry'); head office: 1051 Budapest, Arany János u. 25., mail address: 1051 Budapest, Arany János u. 25., telephone number: +361-896-3363)
- Hungarian Intellectual Property Office (hereinafter the 'Office': 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:

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

The purpose of data processing is to ensure the admission to the presidency events and the security of the participants, in the framework of which the Controllers may use the data subjects' data for the purposes of accreditation, logistic planning and security controls.

Categories of processed data:

The Controllers will process the personal data provided by the data subjects directly and voluntarily (name, surname, delegation, position, representation (company, organization, country), function (e.g. president), photo, date of birth, place of birth, country, telephone number, e-mail address, optional programmes chosen by the data subject) in accordance with the legal rules in effect.

Legal basis of data processing:

The legal basis of data processing is the data subject's consent [Article 6(1) point a) of GDPR]. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

Duration of data processing:

The Controllers will process the personal data provided by the data subject until 31 December 2024.

II.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]

Duration of data processing:

The Controllers will process the personal data provided by the data subject until 31 December 2024.

II.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]

Duration of data processing:

The Controllers will process the personal data provided by the data subject until 31 December 2024.

II.4. Organising a visit to Parliament

Purpose of processing:

Ensuring the admission of visitors and issuing of an entry permit in the framework of the organisation of a parliamentary visit

Categories of processed data:

- surname, first name
- place and date of birth
- type of official identity card and document identification number
- in the case of non-Hungarian citizens, the type of identity document of the person) in addition to those listed under c), the c), the issuing authority and the nationality of the person concerned

Legal basis of data processing:

The explicit consent of the data subject. [Articles 6(1)(a)]

Duration of data processing:

The Controllers will process the personal data provided by the data subject until 31 December 2024.

Recipients:

This data will not be processed in the Novento System, the data subjects forward the information to the Office via e-mail.

Parliament's Office (1055 Budapest, Kossuth Lajos tér 1-3., telefon: +36-1-441-4000, +36-1-441-5000, www.parlament.hu), e-mail of the data protection officer: adatvedelem[at]parlament.hu.[1]

III. Access to data and data security precautions

III.1. In the Ministry

[1] The data protection notice regarding the processing of the data of the Parliament is available in Hungarian language here: https://www.parlament.hu/documents/10181/3279576/I_7_belepteto.pdf/5c88a6a9-67c3-8093-70d5-4a632e031060?t=1575034558283

The duly authorised members of the Controller's personnel are entitled to process the personal data provided by data subjects, within the boundaries of their respective responsibilities, in the interest of the fulfilment of their job responsibilities. If necessary, the Controller will transfer information to state agencies and service providers involved in the management of events (providers involved in the management of the events (National Event Management Agency Zrt., Counter Terrorism Centre, National Police Headquarters, Budapest Police Headquarters, Incert GIE). The Controller will not transfer any data coming under the effect of this privacy policy to third countries within the meaning of the GDPR or to any international organisation referred to in Article 44 of the GDPR.

The Controller stores any recorded personal data on its own servers. The Controller does not use third-party services for the storage of personal data and engages no data processor.

In respect of any data processed electronically, the Ministry provides for the protection of personal data with appropriate data security measures as set forth in Articles 24 and 25 of the GDPR, including against unauthorised access or the unauthorised alteration of data.

The Controller makes every effort to ensure the safe processing of personal data, and has therefore taken the technical and organisational measures and has formulated the procedural rules which are necessary for the enforcement of the rules relating to data processing and data protection.

III.2. In the Hungarian Intellectual Property Office

III.2.1. Recipients of personal data, transfer of data

The Office does not use a data processor for the operation of the IPMindenkinek.hu website; for statistical data analysis, it uses the data processing services of Google LLC by using Google Analytics.

Processor's

- name: Meta Platforms Ireland Limited
- seat: 4 Grand Canal Square Grand Canal Harbour Dublin 2 Ireland
- website contact details: https://about.meta.com/

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 processor 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: Invitech ICT Services 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.

III.2.2. 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.

IV. 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: accreditation.presidency@hu24eu.hu or adatvedelem@hipo.gov.hu or by post to the address indicated in Section I.

The Controllers 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 Controllers 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 Controllers 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 Controllers ascertain whether the request originates from the person entitled.

V. 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 Controllers as the processors of their personal data with a view to remedy the infringement, or 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.

VI. Amendment of privacy policy

The Controllers reserve the right to amend this privacy policy at any time based on their unilateral decision and will inform the data subjects of any such amendment through the publication of the amended privacy policy in the usual manner.

VII. Communication

During the implementation of all presidency events, the Ministry will communicate with the data subjects at the accreditation.presidency@hu24eu.hu e-mail address and via the NOVENTO system, while the Hungarian Intellectual Property Office will communicate with the data subjects via the e-mail address: adatvedelem@hipo.gov.hu.