Hungarian Intellectual Property Office

21.10.2025

PRIVACY POLICY
ON RECORDINGS OF PERSONS ATTENDING THE HUNGARIAN INTELLECTUAL PROPERTY'S PRESS PUBLIC EVENTS

Preamble

The Hungarian Intellectual Property Office (hereinafter the 'Office') pays particular attention to act in compliance with the General Data Protection Regulation of the European Union[1] (hereinafter the 'GDPR'), the Hungarian Data Protection Act[2] (hereinafter the 'Information Act'), the Civil Code[3] and the other laws, as well as with the guidelines still in effect[4] of the European Data Protection Board (hereinafter the 'Board') and the Article 29 Data Protection Working Party, and the established data protection practice[5] of the Hungarian National Authority for Data Protection and Freedom of Information[6] (hereinafter the 'Authority').

The staff of the Office may take photographs, film and sound recordings at events, which may include the image and voice of participants. In the case of a public event open to the press, the staff of the press organs may also make recordings; these press organs are considered as independent data controllers and their data processing activities are not covered by this notice. The resulting footage may also be published on the website, magazines and social media of the Office and the media.

For other data processing not related to the registration for the Office's events or the taking of photographs, please consult the separate privacy notice on the Office's Privacy Policy at https://www.sztnh.gov.hu/en/privacy-policy.

Data subjects include staff of the Office, employees of other public bodies, representatives of international organisations or foreign partner offices, persons awarded or participating in a competition, or other persons attending events as audience members.

I. Controller of personal data

Controller's

- name: Hungarian Intellectual Property Office
- seat: 1081 Budapest, II. János Pál pápa tér 7.
- postal address: 1438 Budapest, pf. 415.
- phone number: 06-1/312-4400
- e-mail address: sztnh@hipo.gov.hu

[1] 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 (General Data Protection Regulation).
[2] Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information.
[3] Act V of 2013 on the Civil Code.
[4] http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358
[5] https://www.edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en
[6] https://www.naih.hu/about-the-authority

II. Name and contact details of the Data Protection Officer of the controller

Data Protection Officer's

- e-mail address: adatvedelem@hipo.gov.hu
- phone number: 06-1/474-5941
- postal address: 1438 Budapest, pf. 415.

III. Source of personal data

The personal data described in point VI are partly provided directly by the data subject to the Office and partly already indirectly available to the Office by the data subject.

IV. Automated decision-making

The Office does not use an automated decision-making process.

V. Categories of personal data concerned, purposes, sources, legal basis, recipients and duration of processing

1. ENGAGEMENT IN PUBLIC LIFE AND PHOTOGRAPH OF A CROWD	
Categories of personal data	Crowd shot of people participating in the event or engagement in public life: the image or voice of the data subjects, the information they provide and any other information that can be used to link them to the data subject.
Purpose of processing	Providing information to the public on the events of the Office related to the performance of its public functions and the use of public funds, in this context, recording the events of the Office, informing those interested in the event and evidencing that the events have taken place.
Legal basis for the processing	The processing of data – In accordance with Article 6(1)(e) of the GDPR and Section 5(1)(b) of the Information Act – is based on a statutory provision. The statutory provision is the following: paragraph (2) of Section 2:48 of the Civil Code, according to which the consent of the data subject concerned is not required for the making and use of a visual or audio recording in the case of public recordings and recordings of engagement in public life. <u>Recordings of a crowd:</u> Crowd shots show a crowd of people, the people depicted are not seen as individuals but as part of the crowd. If the photograph is not of individuals individually drawing attention to themselves, but of a crowd, it is a crowd shot. Engagement in public life is

1. ENGAGEMENT IN PUBLIC LIFE AND PHOTOGRAPH OF A CROWD	
	defined as an activity that influences the life of society, local or national conditions. <u>Engagement in public life:</u> Engagement in public life is based on speaking out and taking a role in the public interest. Typical examples are speaking at various cultural and social events, meetings, public participation. Anyone can be a public actor (person engaged in public life), i.e. the qualification is not linked to a formal social or legal status. <u>This legal basis typically applies to the following recordings:</u> • recordings of the audience in which the persons concerned cannot be identified, • recordings of any person who, by virtue of his or her job, awards or participation, becomes the focus of the event in front of an audience.
Recipient	The released recordings are available to anyone.
Duration of the processing	Duration of the publication of the article informing the public or, if archived, the storage period. The criterion for determining the storage period: the possible use of the recording for future articles, office publications.

2. PROCESSING OF OTHER PHOTOGRAPHS	
Categories of personal data	A recording of the people attending the event: the image or voice of the data subjects, the information they provide and any other information that can be used to link them to the data subject.
Purpose of processing	Providing information to the public on the events of the Office related to the performance of its public functions and the use of public funds, in this context, recording the events of the Office, informing those interested in the event and evidencing that the events have taken place.
Legal basis for the processing	The processing is based on the data subject's voluntary consent, which is given by the data subject when entering the event area, in knowledge of the data protection notice published on the Office's website. [pursuant to Article 6 (1)(a) of the GDPR and Section 5(1)(a) of the Information Act] This legal basis typically applies to the following recordings, so consent to the making and use of the recording is required in the following cases:

2. PROCESSING OF OTHER PHOTOGRAPHS	
	• in the case of a recordings or footage made specifically of a particular person(s), except for engagement in public life • when highlighting from the crowd, using any recording technique (e.g. telephoto lens, zoom), as it reindividualises the image, • if the crowd shot is individualised by post-editing.
Recipient	The released recordings are available to anyone.
Duration of the processing	Duration of the publication of the article informing the public or, if archived, the storage period. The criterion for determining the storage period: the possible use of the recording for future articles, office publications.

3. ACCESS CONTROL AND CCTV
In the context of possible card access to the Office's buildings and related CCTV data processing a separate information notice on data processing is available on the Data Processing sub-page of the Office's website, at the following link: https://www.sztnh.gov.hu/en/privacy-policy

4. PROCESSING OF DATA RELATING TO FOLLOWERS OF THE OFFICE'S SOCIAL MEDIA PROFILE (FAN PAGE)	
Categories of personal data	public data that has been made available on the Office's social media profile (the name and photo of the data subject), data relating to the following of the account, comments, opinions and reactions to certain content shared
Purpose of processing	informing interested parties about the activities of the Office (posting on the fan page), allowing reactions to shared content, sometimes moderating it
Legal basis for the processing	the processing is necessary for the performance of the public functions of the Office [Article 6(1)(e) GDPR], subject to Article 5 GDPR
Recipient	the Office and Meta participate as joint controllers for the processing of data on Facebook and Instagram, respectively, and LinkedIn for the processing of data related to the LinkedIn account. Recipient is anyone who can see the Office's social media posts.
Duration of the processing	- liking and following the fan page of the Office, until the withdrawal by the data subject of the reaction to the Office's post - in the absence of the foregoing, until the deletion of the social media profile of the Office

VI. Recipients of personal data, transfer of data

In addition to the recipients indicated in point VI, the personal data described in point VI of this notice may be accessed by the employees working in the relevant organisational units of the Office (Security Section, IT Department) and the persons exercising the employer's rights in the relevant units.

In the event of a failure or other problem in the IT systems of the Office, the systems containing personal data may also be accessed by duly authorised staff of the data processor responsible for performing certain operational tasks of the IT infrastructure of the Office.

Processor's	
▪ name:	V.I.X. Security Vagyon-, Információvédelmi, Kereskedelmi és Szolgáltató Kft
▪ seat:	2161 Csomád, Verebeshegy utca 12.
▪ e-mail contact details:	vix@vixkft.hu
▪ data processing activity:	Operational tasks of the asset surveillance and electronic surveillance system

Processor's	
▪ name:	ASSA ABLOY Opening Solutions Hungary Korlátolt Felelősségű Társaság
▪ seat:	8000 Székesfehérvár, Palánkai u. 5.
▪ e-mail contact details:	sales.seawing@assaabloy.com; helpdesk.seawing@assaabloy.com;
▪ data processing activity:	Software maintenance of the access control system

Where proceedings have been instituted before a court or other authority which require the transfer of personal data to that court or authority, the court or authority may also have access to the personal data. In other respects, the Office does not transfer recordings or documents containing personal data to other data controllers, third countries or international organisations.

VII. Data security

The Office and its processors shall 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 shall take all security, technical and organisational measures necessary to ensure the security of personal data.

Organisational measures

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.

Technical measures
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.

VIII. Data subjects' rights in relation to data processing

a) The rights of the data subject with regard to data processing

If the data subject submits a request concerning the processing of personal data by the Office, the latter shall inform the data subject of the measures taken or the reasons for non-taking of such measures within one month at the latest from the day following the receipt of the request, and in the case of not taking measures shall inform the data subject of his or her right to lodge a complaint and to seek judicial remedy. If the complexity or number of requests received by the Office so justifies, the Office may extend the time limit by up to two additional months. The Office will inform the person concerned of the extension and the reasons for it within one month of receipt of the request.

In order to protect the rights of the data subject and to meet the requirements of data security, the Office will verify the identity of the data subject and the person to whom the rights relate, and will request additional information where necessary.

b) Right of access

The data subject has the right to be informed by the Office whether or not his or her personal data are being processed and, if so, to be informed in particular of

- the purposes of the processing;
- the categories of personal data processed;

- the recipients or categories of recipients to whom or to which the Office has communicated or will communicate the personal data (including, where applicable, the safeguards for the transfer);
- the envisaged duration of the storage of personal data or the criteria for determining that duration;
- the right to request the rectification, erasure or restriction of the processing of personal data concerning him or her and to object to the processing of such personal data;
- the right to lodge a complaint with the National Authority for Data Protection and Freedom of Information;
- if the data is not from him, the source of the data.

Upon request, the Office will provide the data subject with a copy of the personal data it processes or of a document containing such data, provided that this does not adversely affect the rights and freedoms of others. It will comply with the first copy request free of charge, after which it will charge a reasonable fee based on administrative costs or refuse to provide a copy.

c) Right to rectification

The data subject shall have the right to obtain from the Office the rectification of inaccurate personal data concerning him or her and, taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed.

d) Right to erasure

The data subject has the right to request the deletion of his or her personal data, which the Office will comply with, unless one of the following grounds applies: the data to be erased are necessary for the exercise of the right to freedom of expression and information; for compliance with an obligation under Union or Member State law; for the performance of a task carried out by the Office in the public interest or in the exercise of official authority vested in the Office; in the public interest in the field of public health; for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes; or for the establishment, exercise or defence of legal claims.

e) Right to restriction of processing

The data subject has the right to have the processing of his or her personal data restricted by the Office at his or her request, where

- the accuracy of the personal data is contested by the data subject;
- the processing is unlawful but the data subject opposes the erasure of the data and requests the restriction of their use;
- the Office no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of legal claims;
- the processing is based on the performance of a task carried out in the public interest or in the exercise of official authority vested in the Office, and the data subject objected to the processing.

Personal data subject to restriction will be processed by the Office, except for storage, only with the consent of the data subject and for the establishment, exercise or defence of legal claims, the protection of the rights of another natural

or legal person or an important public interest of the European Union or of a Member State.

The Office will inform in advance the person at whose request the processing has been restricted of the lifting of the restriction.

f) Right to object

The data subject has the right to object at any time, on grounds relating to his or her particular situation, to the processing of his or her personal data where the processing is based on Article 6 (1)(e) of the GDPR, if the data subject considers that the Office is not processing his or her personal data fairly in relation to the purposes stated in this notice. The Office is entitled to continue to process the data despite the objection, if the processing is justified by compelling legitimate grounds which override the interests, rights and freedoms of the data subject or are related to the establishment, exercise or defence of legal claims.

g) Right to data portability

The data subject shall have the right to receive personal data concerning him or her which he or she has provided to the Office in a structured, commonly used, typewriter-readable format, or to request that the Office transfer the aforementioned data to another controller, where the processing is based on Article 6 (1)(b) GDPR and is carried out by automated means.

The exercise of this right must be without prejudice to the right to erasure and the right to be forgotten.

This right may not be exercised if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Office.

The exercise of this right must not adversely affect the rights and freedoms of others.

IX. Exercise of rights after the death of the data subject[7]

Within five years of the death of the data subject, the rights of access, to rectification, erasure, restriction of processing or objection may be exercised by the person whom the data subject has authorised by administrative act or by a declaration in a public deed or private document having full probative value made to the Office.

In the absence of a declaration, the rights to rectification and objection and, where the processing was already unlawful during the lifetime of the data subject or the purpose of the processing ceased to exist upon the death of the data subject, the rights to erasure and restriction of processing shall be exercised by the close relative of the data subject (spouse; direct relative; adopted, step- and foster child; adoptive, step- and foster parent; and sibling) who is the first to exercise this right.

[7] Provisions laid down in Section 25 of the Information Act

The person enforcing the rights must provide proof of the fact and date of the death of the person concerned by means of a death certificate or a court order, and proof of his or her identity and, where necessary, of his or her status as a close relative by means of a public deed.

The person asserting the rights shall then be granted the rights and be subject to the obligations established for the person concerned.

The Office shall, on request, inform the close relative of the person concerned of the measures taken pursuant to this point, unless the data subject has prohibited this in the administrative provision referred to in the first paragraph, in a public deed or in a private document with full probative value.

X. Right to complain and seek redress

If you believe that your rights have been infringed as a result of the processing of your data by the Office, you may

- submit a complaint to the Office using one of the following contact details: 1081 Budapest, II. János Pál pápa tér 7., postal address: 1438 Budapest, Pf. 415., central phone number: +36-1/312-4400, central fax number: +36-1/474-5534, central e-mail address: sztnh@hipo.gov.hu, e-mail address of the Data Protection Officer: adatvedelem@hipo.gov.hu;
- to protect your data, you can have recourse to the courts, which will act out of turn. The action may be brought before the Budapest-Capital Regional Court (Fővárosi Törvényszék) competent for the seat of the Office (1055 Budapest, Markó utca 27, phone number: +36-1/354-6000, website: https://fovarositorvenyszek.birosag.hu/), or the competent court in the place of residence or domicile of the person concerned, which can be found at the following website: https://birosag.hu/torvenyszekek;
- you can also lodge a complaint with the National Authority for Data Protection and Freedom of Information (seat: 1055 Budapest, Falk Miksa utca 9-11., postal address: 1374 Budapest, Pf. 603., phone number: +36-1/391-1400, fax number: +36-1/391-1410, e-mail address: ugyfelszolgalat@naih.hu, website contact details: https://www.naih.hu/).