

Privacy Policy

1. INTRODUCTION

ISZT Nonprofit Kft., as the data controller (hereinafter referred to as the **Data Controller**), within the scope of operation of the **hunog.hu/en** website (hereinafter referred to as the Website), informs the Customers and Visitors of the Website through this Privacy Policy about its data processing activities related to its services, the scope of personal data processed, the principles and practices followed during the processing of personal data, the use of data processors, and the methods and possibilities for exercising data subject rights.

The Data Controller considers it important to enforce the right to informational self-determination of the Customers and Visitors of the Website. The Data Controller also pays special attention to respecting the personal rights of the Data Subjects. The recorded personal data is handled confidentially, in compliance with the applicable data protection laws and international recommendations, in accordance with this Privacy Policy, and all necessary measures are taken to ensure the security of the data.

This Privacy Policy is always available, downloadable, and printable in an up-to-date form on the Data Controller's Website.

The Data Controller processes the personal data provided in accordance with the following legal regulations:

Regulation (EU) 2016/679 of the European Parliament and of the Council (April 27, 2016) on the protection of natural persons regarding the processing of personal data and the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation, GDPR);

Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (Infotv.);

Act V of 2013 on the Civil Code (Ptk.);

Act CLV of 1997 on Consumer Protection (Fgytv.);

Act C of 2000 on Accounting (Számv. tv.);

Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Commercial Advertising;

Act CVIII of 2001 on Electronic Commerce Services and Certain Issues Related to the Information Society (Eker. tv.).

The Data Controller undertakes to ensure that all data processing activities related to its operations comply with the provisions of this Privacy Policy and the applicable legal regulations.

The Data Controller reserves the right to modify the content of this Privacy Policy at any time. The Data Subject accepts the provisions of the currently effective Privacy Policy and consents to the data processing specified below.

1.1. Data Controller Information

Name: **ISZT INTERNET SZOLGÁLTATÓK Hálózati Koordinációs Központja Nonprofit Korlátolt Felelősségű Társaság**

Short Name: **ISZT Nonprofit Kft.**

Registered Address: 1089 Budapest, Bláthy Ottó utca 9.

Tax Number: 20763091-2-42

E-mail: info@hunog.hu

Phone: +36 1 238 0115

1.2. Definitions

1.2.1. General Definitions

The following fundamental concepts of data processing are defined in detail by Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding the processing of personal data and the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation), as well as by Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information:

Data protection: A set of principles, rules, procedures, data processing tools, and methods that ensure the lawful processing of personal data and protect the rights of data subjects.

Personal data: Any data that relates to an identified or identifiable natural person (Data Subject), as well as any conclusions drawn from such data about the Data Subject. Personal data retains this status throughout processing as long as its association with the Data Subject can be restored. The link with the Data Subject can be re-established if the Data Controller has the necessary technical means for this restoration.

Data Subject: Any natural person who is identified or identifiable based on specific information.

Identifiable natural person: A natural person who can be identified directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Special data: Any data that falls into special categories of personal data, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for uniquely identifying a natural person, health data, and data concerning a natural person's sex life or sexual orientation.

Data processing: Any operation or set of operations performed on data, regardless of the applied procedure, including but not limited to collection, recording, organization, storage, modification, use, retrieval, transmission, disclosure, alignment or combination, blocking, deletion, and destruction, as well as the prevention of further use of the data, the creation of photographic, audio, or video recordings, and the recording of physical characteristics suitable for identifying a person.

Data controller: A natural or legal person or an organization without legal personality that, within the limits defined by law or binding legal acts of the European Union, determines the purpose of data processing independently or jointly with others, makes decisions regarding data processing (including the tools used), implements them, or has them implemented by a data processor.

Data processing activities: The entire set of data processing operations carried out by a data processor on behalf of or based on the instructions of the Data Controller.

Data processor: A natural or legal person or an organization without legal personality that, within the limits and conditions defined by law or binding legal acts of the European Union, processes personal data on behalf of or based on the instructions of the Data Controller.

Consent: A voluntary, specific, informed, and unambiguous indication of the Data Subject's will, by which they, through a statement or a clear affirmative action, signify their agreement to the processing of personal data relating to them.

Objection: A declaration by the Data Subject opposing the processing of their personal data and requesting the termination of data processing or the deletion of the processed data.

Third party: A natural or legal person or an organization without legal personality that is not the same as the Data Subject, the Data Controller, or the Data Processor.

Disclosure: Making data accessible to anyone.

Data deletion: Making data unrecognizable in a way that it can no longer be restored.

Cookies: Small data files placed on the Data Subject's computer by the visited website. The purpose of cookies is to facilitate and enhance the convenience of a given information and communication service.

1.2.2. Definitions Used Exclusively in This Privacy Policy

Customer: A natural or legal person who enters into a contract with the Service Provider (Data Controller) to purchase products offered on the Website and, within this framework, purchases a product.

Visitor: A person who views the Website.

Data Subject: A collective term referring to both the Customer and the Visitor, as defined in the categories above.

1.3. Data processing is carried out particularly for the following purposes:

- Technical data processing;
- Cookie management;
- Order processing through the Website;
- Newsletter registration;
- Data processing in case of contact initiated by the Data Subject.

2. PRINCIPLES OF DATA PROCESSING

The data processing activities covered by this Privacy Policy are primarily carried out by the Data Controller for the purpose of contract performance and communication, based on the voluntary consent of the Website's Customers and/or Visitors, and in compliance with legal obligations.

The accuracy, correctness, and timeliness of the personal data provided to the Data Controller are the responsibility of the person providing the data, as the Data Controller does not generate the data itself. The Data Controller does not verify the authenticity of the personal data provided.

Requests for data **deletion** can be submitted via an inquiry sent from the registered email address to the contact address info@hunog.hu.

Any Customer and/or Visitor who provides their email address to the Data Controller assumes responsibility for ensuring that only they use the specified email address to access services from the Data Controller. Due to this responsibility, any obligations arising from transactions made with a given email address are solely the responsibility of the Customer who provided that email address through the Website.

The Data Controller informs users that if they provide personal data of individuals other than themselves, it is the responsibility of the person providing the data to obtain the consent of the other data subjects before sharing such information.

The Data Controller treats the personal data it receives confidentially and processes it only for the purposes and in the manner specified in this Privacy Policy. Personal data is shared with third parties only for reasons explicitly outlined in this Privacy Policy and exclusively for further data processing purposes.

The Website processes the personal data of its Visitors and Customers only to the extent and for the duration necessary to provide its services (full use of the Website). At all stages of data processing, the purpose of data processing is maintained.

3. SPECIFIC DATA PROCESSING ACTIVITIES

3.1. DATA PROCESSING ON THE HUNOG.HU/EN WEBSITE

3.1.1. TECHNICAL DATA PROCESSING

Certain technical data of Data Subjects browsing the Website are automatically logged on the hosting provider's server. Such technical data include the information generated during the use of the Website from the Data Subject's computer and recorded automatically by the Data Controller's system as a result of technical processes. The legal basis for data processing is the Data Subject's consent, as well as Section 13/A (3) of Act CVIII of 2001 on electronic commerce services and certain aspects of information society services. The scope of processed data includes the date and time of the visit, the IP address of the visitor's computer, and the type of browser used.

3.1.2. COOKIE MANAGEMENT

A cookie is a variable content information package sent by the web server, which is stored and retained on the Data Subject's computer for a predefined validity period. The purpose of cookies is to improve the user experience, making the use of the Website simpler and more enjoyable. Cookies alone cannot identify the Visitor of the Website, they only allow the recognition of the Visitor's computer. However, if the Visitor does not wish for cookies to be placed on their computer, they can disable this function in their browser settings.

When defining requirements for cookies, in addition to complying with applicable legal regulations, the Data Controller also takes into account and enforces the provisions of the relevant statement issued by the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) and Opinion No. 2012/4 of the Article 29 Working Party on Data Protection under the EU Data Protection Directive.

For more information on how to delete cookies, visit the following links:

Help with cookie settings:

- **Google Chrome:** [Support Page](#) or enter `chrome://settings/content/cookies` in the browser bar.
- **Microsoft Edge:** Navigate to **Settings** → **Advanced Settings** → **Cookies** (Select: "Allow cookies" / "Block all cookies" / "Block only third-party cookies") or press **F12** → **Debugger** → **Cookies**.
- **Internet Explorer (IE):** [Delete and manage cookies](#) and [Description of cookies](#).
- **Mozilla Firefox:** [Enable and disable cookies](#).

3.1.3. ORDER PROCESSING THROUGH THE WEBSITE

When placing an order on our website, the Customer is required to provide certain (personal) data that are essential for the contract established between the Data Controller and the Customer, as well as for the fulfillment of the Data Controller's related legal obligations. Our data processing activities primarily take place for the purpose of fulfilling the contract between the Data Controller and the Customer, as well as for maintaining communication.

Customers' contact details are also recorded on their virtual business cards and may be shared with event sponsors, who may contact them with their offers.

Purpose of data processing: The fulfillment of the Customer's order and the resulting contract, communication, and compliance with accounting obligations.

Legal basis for data processing: The data processing is necessary for the performance of a contract in which the Customer is one of the parties, or for taking steps at the request of the Customer prior to entering into a contract [GDPR Article 6(1)(b)], as well as for compliance with a legal obligation applicable to the Data Controller [GDPR Article 6(1)(c)].

Scope of data subjects: Natural or legal persons who register an order on the Website.

Scope of processed data: Last name, first name, company name (optional), address, phone number, email address.

Source of processed data: The data is provided by the Customer during the ordering process.

Duration of data processing: For data necessary for contract fulfillment, until the last day of the 6th calendar year following the order registration date; for billing data, until the end of the 8th year, in compliance with Section 169 of Act C of 2000 on Accounting.

Data processing related to payment by bank card:

In the case of bank card payments, the Data Controller does not process the provided bank card data; the Customer submits their payment details directly to OTP Mobil Szolgáltató Kft., the payment service provider operating SimplePay.

Independent data controller: Regarding the data provided on the OTP SimplePay page, the operator of SimplePay, OTP Mobil Kft., qualifies as an independent Data Controller. Only OTP Mobil Kft. has access to the personal data submitted on the SimplePay platform.

Required data for successful payment in the SimplePay system: Bank card number, cardholder's name, expiration date of the bank card, CVC/CVV security code.

SimplePay privacy policy: Available at the following link: <https://simplepay.hu/adatkezelesi-tajekoztatok/>.

3.1.4. NEWSLETTER SUBSCRIPTION

The Data Controller provides the option to subscribe to the newsletter independently of conference registration. The Data Controller sends newsletters only with the explicit consent of the Data Subject, which can be withdrawn at any time.

Purpose of data processing: Sending informational electronic emails about news and articles related to the conference.

Legal basis for data processing: The Data Subject's consent [GDPR Article 6(1)(a)].

Scope of data subjects: Natural persons who register for the newsletter subscription.

Scope of processed data: Name, email address.

Duration of data processing: Until the user requests the deletion of their newsletter subscription.

Data deletion: Consent withdrawal and unsubscription can be requested via email at info@hunog.hu or by postal mail.

3.1.5. DATA PROCESSING IN CASE OF CONTACT INITIATED BY THE DATA SUBJECT

If the Data Subject directly requests information or clarification from the Data Controller (e.g., regarding the registration process, the conference, billing issues, etc.) or wishes to submit a complaint and initiates contact with the Data Controller electronically or through other means (telephone or postal mail), the Data Controller processes the Data Subject's personal data as follows.

Purpose of data processing: Providing information or handling complaints.

Legal basis for data processing:

- In the case of an inquiry that does not qualify as a complaint: The Data Subject's consent [GDPR Article 6(1)(a)].
- In the case of a Customer complaint: The data processing is necessary for the performance of a contract in which the Data Subject is one of the parties or for taking steps at the Data Subject's request prior to entering into a contract [GDPR Article 6(1)(b)].

Scope of data subjects: Individuals making inquiries or requesting information, and Customers submitting complaints.

Scope of processed data: Full name, and depending on the method of inquiry and the data provided, email address and message content.

Duration of data processing: If it concerns a contractual relationship between the Data Controller and the Customer, for data necessary for fulfilling the contract, the retention period lasts until the last day of the 6th calendar year following the date of order registration, and for

billing data, until the end of the 8th year, in accordance with Section 169 of Act C of 2000 on Accounting. If it does not concern a contractual relationship between the Data Controller and the Customer, data processing continues until the purpose of data processing ceases, but for no longer than 1 year.

3.1.6. DATA PROCESSING RELATED TO PARTICIPATION IN THE EVENT

3.1.6.1. RECORDING OF IMAGES, AUDIO, AND VIDEO

Recording at the event: Photos, audio, and video recordings are made of the event in accordance with the provisions of the Civil Code regarding public appearances and mass recordings.

Purpose of recording: The preservation of HUNOG events and the verification of the event's occurrence.

Use of recordings: The organizer may publish the recordings on its website, social media platforms, and offline media. A report on the event and a promotional video for future years may also be created.

Consent through participation: By registering for the event, participants accept that image, audio, and video recordings will be made at the conference for the aforementioned purposes.

Legal basis for data processing: Section 2:48 (2) of the Civil Code, which states that no consent from the Data Subject is required for creating and using an image or audio recording in the case of mass recordings and recordings of public appearances.

Scope of data subjects: Mass recordings depict a crowd of people, where individuals are not shown separately but as part of a group. A recording qualifies as a mass recording if the individuals in the image do not draw attention to themselves separately but appear as part of a collective. Public appearance refers to an action that influences public life, local or national affairs. Public appearance is established through speaking or acting in the public interest. This typically includes speeches or public participation at cultural, social events, or gatherings. Any person can be considered a public figure, and this status is not tied to a formal social or legal position.

Purpose of data processing: To document the event, inform those interested in the event, and verify that the event has taken place.

Scope of processed data: Mass recordings of participants at the event and recordings of public appearances.

Duration of data processing: The duration of public disclosure and, in the case of archiving, the retention period. The retention period is determined based on the potential future use of the recording in later publications.

3.1.6.2. PROCESSING OF PARTICIPANTS' CONTACT AND ADDITIONAL DATA

Company name display: Registrants for the conference agree that their company name will be displayed on the event website.

Voluntary provision of additional contact details: During registration, participants may consent to the processing of additional email addresses and phone numbers beyond the

required contact details. These additional details may be included on their virtual business cards and shared with event sponsors, who may contact them with their offers.

Legal basis for data processing: The Data Subject's consent [GDPR Article 6(1)(a)].

Scope of data subjects: Individuals who consent to this data processing during registration.

Purpose of data processing: Virtual business card and the transfer of data to sponsors.

Scope of processed data: Name, company name, email address, and phone number.

Duration of data processing: Until the Data Subject withdraws their consent.

Data deletion: Consent withdrawal and requests for data deletion can be submitted via email at info@hunog.hu or by postal mail.

4. DATA PROCESSORS

Goodevent Rendezvényszervező Kft. qualifies as a Data Processor in connection with the HUNOG Conference.

Address: 1165 Budapest, Hangulat utca 14.

Postal address: 1162 Budapest, Timur utca 74.

Bank account number: 10918001-000000090-57890006

Company registration number: 01-09-174934

Tax number: 24394763-2-42

Email: info@goodevent.hu

Data processing activities: The Data Processor processes personal data to the extent necessary for performing its tasks related to event organization, including invoicing, conference participation, communication, and sending information required for order fulfillment. The processing is carried out only for the necessary duration.

5. METHOD OF STORING PERSONAL DATA

The Data Controller selects and operates the IT tools used for processing personal data in a manner that ensures the following regarding the processed data:

- a) It is accessible to authorized individuals (availability).
- b) Its authenticity and verification are ensured (data processing authenticity).
- c) Its integrity is verifiable (data integrity).
- d) It is protected against unauthorized access (data confidentiality).

The Data Controller protects the data with appropriate measures, particularly against unauthorized access, alteration, transmission, disclosure, deletion, or destruction, as well as against accidental destruction, damage, and inaccessibility resulting from changes in the applied technology.

To safeguard electronically managed data records in its various databases, the Data Controller employs appropriate technical solutions to ensure that stored data—except as permitted by law—cannot be directly linked and assigned to the Data Subject. The Data Controller, in accordance with the current state of technological advancements, implements technical, organizational, and administrative measures to ensure the highest level of security for personal

data, preventing unauthorized modification, destruction, or use, and providing a level of protection appropriate to the risks associated with data processing.

The Data Controller continuously ensures virus protection within the network that processes personal data. It takes all necessary measures to maintain the accuracy, completeness, and up-to-date status of the personal data it manages and/or processes.

The Data Controller reserves the right to inform Data Subjects if a security vulnerability is detected within the Website system and, simultaneously, to restrict access to the service provider's system, services, or specific functions until the security vulnerability is resolved.

6. RIGHTS OF DATA SUBJECTS REGARDING THE PROCESSING OF THEIR PERSONAL DATA

6.1. Right to Information

Every Data Subject has the right to request information about the data being processed. Upon the Data Subject's request, after credible verification of identity, the Data Controller provides concise, transparent, understandable, and easily accessible information in a clear and plain language without undue delay, but no later than within 25 days.

6.2. Right of Access

The Data Subject has the right to receive confirmation as to whether their personal data is being processed. If such processing is ongoing, the Data Subject has the right to access the personal data and the following information: the purposes of processing; categories of personal data concerned; recipients or categories of recipients to whom the personal data has been or will be disclosed, including in particular third-country recipients or international organizations; and the intended duration of storage. If personal data is transferred to a third country or an international organization, the Data Subject has the right to be informed of the appropriate safeguards regarding the transfer.

6.3. Right to Rectification

The Data Subject has the right and obligation to request the rectification of any incorrectly recorded data or to update changed data. Upon credible verification of identity and substantiation of the requested correction, the Data Controller carries out the rectification without delay and informs the Data Subject accordingly.

6.4. Right to Erasure

The Data Subject has the right to request the Data Controller to delete their personal data without undue delay if:

- the personal data is no longer needed for the purpose for which it was collected,
- the Data Subject withdraws their consent, and there is no other legal basis for processing,
- the Data Subject objects to the processing, and there is no overriding legitimate reason for processing,
- the personal data has been unlawfully processed.

During the term of the contract, if the legal basis for processing is contract performance or legal obligation, the Data Subject cannot request the deletion of their data.

6.5. Right to Restriction of Processing

A request for restriction of processing may occur in the following cases:

- The Data Subject disputes the accuracy of the personal data, in which case the restriction applies for the period necessary to verify its accuracy.
- The processing is unlawful, and the Data Subject opposes the deletion of the data and instead requests the restriction of its use.
- The Data Controller no longer needs the personal data for processing purposes, but the Data Subject requires it for the establishment, exercise, or defense of legal claims.
- The Data Subject has objected to the processing; in this case, the restriction applies until it is determined whether the Data Controller's legitimate grounds override those of the Data Subject.

If data processing is subject to restriction, the personal data—except for storage—may only be processed with the Data Subject's consent, for the establishment, exercise, or defense of legal claims, for the protection of another natural or legal person's rights, or for reasons of important public interest of the European Union or a Member State.

6.6. Right to Data Portability

The Data Subject has the right to receive the personal data concerning them, which they have provided to the Data Controller, in a structured, commonly used, machine-readable format and to transmit those data to another data controller. The Data Controller complies with such requests within 25 days upon credible verification of identity. However, if the request constitutes repeated or abusive exercise of rights within a calendar year, the Data Controller may refuse to fulfill it or require the reimbursement of administrative costs as a condition for execution.

6.7. Right to Object

The Data Subject may object to the processing of their personal data if:

- (i) the processing is necessary solely for the fulfillment of a legal obligation imposed on the Data Controller or for the pursuit of the Data Controller's legitimate interests,
- (ii) the purpose of the processing is direct marketing, market research, or public opinion polling,
- (iii) the processing is carried out for the performance of a task in the public interest.

The Data Controller reviews the legitimacy of the objection and, if justified, ceases data processing while blocking the affected personal data. Additionally, the Data Controller notifies all recipients to whom the personal data was previously transferred about the objection and any measures taken based on it.

PROCEDURAL RULES

The Data Controller informs the Data Subject without undue delay and in any case within **25 days** from the receipt of the request about the actions taken in response to the request under **Articles 15–22 of the GDPR**. If necessary, considering the complexity of the request and the number of requests, this deadline may be extended by an additional **two months**.

The Data Controller informs the Data Subject about the extension, stating the reasons for the delay, within **25 days** of receiving the request. If the Data Subject submitted the request electronically, the response is also provided electronically unless the Data Subject requests otherwise. If the Data Controller does not take action in response to the Data Subject's request, it informs the Data Subject without delay and at the latest within **25 days** of receiving the request, explaining the reasons for the failure to act. The Data Controller also informs the Data Subject of their right to **lodge a complaint with a supervisory authority** and to seek **judicial remedy**.

The Data Controller notifies all **recipients** to whom the personal data has been disclosed about any **corrections, deletions, or restrictions** on data processing unless this proves **impossible or requires disproportionate effort**. Upon request, the Data Controller informs the Data Subject about such recipients.

7. LEGAL REMEDIES

7.1. Complaint to the Data Controller

If you believe that the Data Controller is not complying with or violating applicable legal provisions or obligations undertaken in this Privacy Policy, you may report this using the following contact details of the Data Controller:

Name: ISZT Nonprofit Kft.

Registered address: 1089 Budapest, Bláthy Ottó utca 9.

Email: info@hunog.hu

Phone: +36 1 238 0115

The Data Controller will respond in writing to the Data Subject's complaint without delay, but no later than **25 days**, and if justified, will take corrective action regarding the complained activity.

7.2. Right to Seek Legal Remedy

If the Data Subject's rights have been violated, they may take legal action against the Data Controller. The court will proceed with the case **without delay**. The case falls under the jurisdiction of the **competent regional court (törvényszék)**. The Data Subject may initiate the lawsuit at the **court competent for the Data Controller's registered office** or at the **court of their residence**, at their discretion. A list of **regional courts** and their contact information is available at the following link: <http://birosag.hu/torvenyszekek>, while information on jurisdiction can be found at: <http://birosag.hu/ugyfelkapcsolati-portal/illetekessegkereso>.

7.3. Supervisory Authority Name and Contact Information

Data protection complaints can be submitted to the **National Authority for Data Protection and Freedom of Information (NAIH)**:

National Authority for Data Protection and Freedom of Information

Registered address: 1055 Budapest, Falk Miksa utca 9-11.

Mailing address: 1363 Budapest, Pf.: 9.

Phone: +36 1 391-1400

Fax: +36 1 391-1410

Email: ugyfelszolgalat@naih.hu

8. OTHER PROVISIONS

Scope of the Privacy Policy:

Temporal scope: This Privacy Policy is effective from **February 20, 2025**, until further notice or withdrawal.

Personal scope: This Privacy Policy applies to individuals whose data is processed under the scope of the data processing activities covered by this Privacy Policy, as well as to individuals whose **rights or legitimate interests** are affected by the data processing.

DISCLAIMER: The whole text of the present Policy, as well as the documents derived from it, including those in the Annexes, have been written in Hungarian and English, both versions being deemed authentic, but for legal purposes the text in Hungarian is to be given priority of interpretation.