# PRIVACY POLICY

#  /Information for visitors of www.humda.hu /

While processing personal data within its system, including the management, storage and use of data, Data Controller shall observe in particular the provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council 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).

Regarding the processing of data, Data Controller hereby informs the visitors of its website (hereinafter: User) about the personal data processed, the principles and practices of processing personal data and the ways and possibilities of exercising User's rights.

User shall have the right to partially or completely withdraw his consent to data processing by means of sending a written notification to Data Controller, or to request the erasure of his data in the manner specified in this Policy.

# NAME OF DATA CONTROLLER

Data are processed by **HUMDA Zrt.**

|  |  |  |
| --- | --- | --- |
| Data of Data Controller  |  |  |
| Name:  |   | **HUMDA Zrt.**  |
| Seat:  |   | Kálmán Imre utca 1 Budapest, H-1054  |
| Company reg. no.:  |   | Cg. 01-10-048684 |
| E-mail:  |   | info@humda.hu  |
| Webpage:  |   | [www.humda](http://www.humda).hu  |

Data control is based on the following regulations

* Act CXII of 2011 on Informational Self-Determination and Freedom of Information (Hereinafter: Privacy Act)
* Regulation (EU) 2016/679 of the European Parliament and of the Council 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: Regulation)
* Act XLVIII of 2008 on Essential Conditions of and Certain Limitations to Business Advertising Activity.
1. **PROCESSING SITUATIONS**

#  1. Personal data logged by the system

|  |  |
| --- | --- |
| Personal data | Purpose of data processing  |
| IP address  | Identification number assigned by the internet provider to the device of User when logging into the system. IP addresses are processed by Data Controller to provide for the IT security of its system |
| Browser type  | Sending an html code complying with the browser.  |

Legal basis of processing: Free consent of User according to Point a) of Article 6(1).

Potential consequences of not processing the data: inaccurate analytics, poor user experience.

Duration of processing: The system will store the data referred for 6 months from the date of their creation and then erasure them automatically.

#  2. Management of cookies

|  |  |  |  |
| --- | --- | --- | --- |
| Types and names of cookies  | Controlled data  | Purpose of data control | Duration of processing |
| Persistent cookie:\*\*\*  | Recording visits to the page  | Promote improved user experience (optimum navigation, displaying relevant ads only).  | They are stored for a long duration in the cookie folder of the browser. The duration depends on the browser settings of User.  |

Legal basis of processing: Free consent of User according to Point a) of Article 6(1).

Source of data: Taken directly from User.

Potential consequences of not processing the data: inaccurate analytics, lack of relevant, targeted ads.

#  3. Deleting cookies

User shall have the right to delete cookies from his own computer or to disable the use of cookies in his browser. Cookies can usually be managed in the Tools/Settings menu of browsers under Privacy/History/Custom Settings, being referred to as “cookies” or “tracking”.

Should User wish to know more about the cookies used by his browser, he should visit one of the following websites complying with his browser:

 Google Chrome (https://support.google.com/chrome/answer/95647?hl=hu)

Mozilla Firefox (https://support.mozilla.org/hu/kb/sutik-engedelyezese-es-tiltasa-amitweboldak-haszn )

Windows Internet Explorer (https://support.microsoft.com/hu-hu/help/260971/description-ofcookies)

Safari (https://support.apple.com/hu-hu/guide/safari/manage-cookies-and-website-datasfri11471/mac)

Potential consequences of not processing the data: incomplete webpage services, inaccurate analytics.

1. **ACCESS TO DATA, DATA SECURITY, DATA TRANSFER**

#  1. Access to data, data transfer

Personal data may only be accessed by Data Controller and the employees of Data Controller's Data Processor, for the purpose of performing their duties.

Data Controller shall only transfer the personal data processed by it to other bodies or administrative bodies in the manner and for the purpose specified by law.

Data Controller informs User that other bodies authorized by the court, the prosecutor, the investigating authority, the infringement authority, the administrative authority, the National Data Protection and Freedom of Information Authority or the law may request Data Controller to provide information, disclose or transfer data or make documents available.

Data Controller may only transfer personal data to the authorities in the quantity and to the extent strictly necessary for the purpose of the action specified by the request, provided that the requesting authority has indicated the exact purpose and the scope of the requested data.

#  2. Data security

Data Controller shall take all measures necessary to ensure the security of the controlled data, providing for an adequate level of protection, in particular against unauthorized access or damage to and alteration, transmission, disclosure, erasure, destruction and accidental erasure of data. Data Controller shall ensure the security of the data by appropriate technical and organizational measures.

Data Controller shall select and operate the IT tools used for processing personal data during the provision of its services in such a way that:

* authorised access to the controlled data is provided (availability);
* the authenticity and validation of the controlled data are provided for (authenticity);
* the unaltered status of the controlled data may be verified (integrity);
* unauthorised access to the controlled data is prevented (confidentiality).

While processing data, Data Controller shall preserve

* the confidentiality of data: Data Controller shall protect the information and only provide authorised access to it;
* the integrity of data: Data Controller shall preserve the accuracy and integrity of the information and the control method;
* the availability of data: Data Controller shall guarantee that, when an authorized user needs it, he can access the information he requires and that the means to do so are available.
1. **USER RIGHTS**

#  1. Information and access to personal data

User may request written information from Data Controller through the contact details provided above about the following:

* the personal data processed by Data Controller,
* the basis for the processing the data,
* the purpose of processing the data,
* the source of data,
* the duration of processing
* to whom and when was access provided by Data Controller to his personal data and on what legal basis, which data are involved; who received the personal data transferred by Data Controller.

Data Controller shall provide the information to User in a widely used electronic format, unless User requests a printed copy instead. Data Controller shall not provide verbal information by telephone.

Upon the first request by User, Data Controller shall provide a copy of the personal data (in person, at the Customer Desk) to User free of charge. For additional copies requested by User, Data Controller may charge a reasonable fee calculated from the administrative costs. If User requests an electronic copy, Data Controller shall provide the information by e-mail in a widely used electronic format.

When, having received the relevant information, User contests data processing and the accuracy of the processed data, he may request the rectification, supplementation and erasure of his personal data, the restriction of their processing and he may also object to the processing of such personal data as specified under Section III or may initiate a legal proceedings as specified under Section IV.

#  2. Right to rectify and supplement the processed personal data

At the written request by User, Data Controller shall, without undue delay, rectify the inaccurate personal data specified by User in writing or in person in one of Data Controller's shops, or supplement the incomplete data with the content specified by User. Data Controller shall inform all recipients to whom these particular personal data have been transferred of the rectification or supplementation, unless such an action proves impossible or requires a disproportionate effort. Data Controller shall inform User about these recipients if User so requests in writing.

#  3. Right to restrict data processing

User shall have the right to request in writing from Data Controller restriction of processing where one of the following applies:

* the accuracy of the personal data is contested by User, for a period enabling the controller to verify the accuracy of the personal data,
* the processing is unlawful and User opposes the erasure of the personal data and requests the restriction of their use instead,
* Data Controller no longer needs the personal data for the purposes of the processing, but they are required by User for the establishment, exercise or defence of legal claims,
* User objects to the data management pending the verification whether the legitimate grounds of Data Controller override those of User.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with User's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

#  4. Right to erasure (‘right to be forgotten’)

User shall have the right to obtain from Data Controller the erasure of personal data concerning him without undue delay where one of the following grounds applies:

1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
2. User withdraws consent on which the processing is based and there is no other legal ground for the processing;
3. User objects to the processing on grounds relating to his particular situation and there are no overriding legitimate grounds for the processing,
4. User objects to the processing for direct marketing purposes, including profiling to the extent that it is related to such direct marketing,
5. the personal data have been unlawfully processed by Data Controller;
6. personal data were collected in connection with the provision of information society services directly provided to children.

User shall not have the right to erasure to the extent that processing is necessary:

1. for exercising the right of freedom of expression and information;
2. for reasons of public interest in the area of public health;
3. for archiving purposes in the public interest, scientific or historical research purposes or statistical in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing;
4. for the establishment, exercise or defence of legal claims.

#  5. Right to data portability

When requested by the Data Processing Contract or where data processing is based on User’s free consent, User shall have the right to receive the personal data concerning him in a machine-readable format. Where technically feasible, User shall have the right to request Data Controller to transmit those data to another controller. The right of portability shall only apply to data provided by User. Other data (statistical data etc.) may not be transmitted.

Regarding the data concerning him and stored in the system of Data Controller (e.g. subscription to Newsletter) User shall have the right to:

* receive such data in a structured, commonly used and machine-readable format,
* transmit such data to other controllers,
* request the direct transmission of such data to other controllers, where technically feasible in the system of Data Controller.

Data Controller shall only fulfil the request for data portability upon receiving User’s written request by e-mail or post. In order to fulfil the request, Data Controller shall make sure that the User wishing to exercise this right is indeed eligible. As specified by the Right to Data Portability, User may request the portability of the data which he has provided to Data Controller. Exercising this right does not automatically erasure the data from Data Controller's systems, therefore User will be registered in Data Controller's systems even after exercising this right, unless he also requests the erasure of his data.

#  6. Objection against processing personal data

User shall have the right to object any time to processing of his personal data by means of submitting a relevant declaration to Data Controller where the legal basis of data processing is

* the performance of a task carried out in the public interest as defined by point (e) of Article 6(1) of the GDPR Regulation or
* legitimate interests as defined by point (f) of Article 6(1) of the GDPR Regulation.

When the Right to Object is exercised, Data Controller shall no longer process the personal data unless Data Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of User or for the establishment, exercise or defence of legal claims. Data Controller shall decide whether data processing is justified by compelling legitimate reasons and inform User about this position.

User may object in writing (by e-mail or post) or, in the case of having subscribed to the newsletter, by clicking on the unsubscribe link.

#  7. Enforcement of the rights of the deceased User by another party

Within 5 years of the death of the User concerned, such rights of the deceased that he had while alive including the right to access to and rectification and erasure of data, to data portability and restriction of processing and to object processing may be exercised by the person authorized so by „ügyintézési rendelkezés”[[1]](#footnote-1) or a declaration in the form of an authentic instrument or a private document providing conclusive evidence made at Data Controller. If the deceased made more than one such declaration at Data Controller, the person named in the one of the latest date may exercise these rights.

If the deceased has not made such a declaration, such rights of the deceased that he had while alive and specified in the preceding paragraph may be exercised by a close relative of the deceased as defined by the Civil Code within five years of the deceased's death (in the case of several close relatives, the first one to exercise the above rights shall be deemed eligible).

According to Point 1) of 8:§1(1) of the Civil Code, close relatives are: spouse, direct relatives, adopted children, stepchildren and foster children, adoptive parents, stepparents and foster parents and siblings. The close relative of the deceased shall provide evidence as follows:

* death certificate or court decision confirming the fact and date of death concerning the deceased and
* authentic instrument confirming the close relative’s identity and, where necessary, his capacity as a close relative.

The person exercising the rights of the deceased has the rights and obligations of the deceased that he had while alive as defined by the Privacy Act and the Regulation, in particular in proceedings against Data Controller and before the National Data Protection and Freedom of Information Authority or in court.

When requested in writing, Data Controller shall inform the close relative in writing about the actions taken except when specifically prohibited by the deceased in his declaration.

#  8. Deadline for fulfilling requests

Data Controller shall, without undue delay, but in any case within one month of receiving the request, inform User of measures taken. If necessary, this deadline may be extended by another two months, taking into account the complexity of the particular request and the number of requests. In this case, Data Controller shall inform User, within one month of receiving the request, about this fact and User’s eligibility to submit a complaint to the supervisory authority and appeal in court.

Where User's request is clearly unfounded or excessive (when the request is repeated several times in particular), Data Controller may charge a reasonable fee for the fulfilment of the request or refuse to oblige. It is the responsibility of Data Controller to prove the above.

If User submits the request in an electronic form, the information shall be provided electronically by Data Controller, unless otherwise requested by User.

Data Controller shall inform all entities receiving personal data from Data Controller of any rectification, erasure or restriction applying to data processing, unless such an action proves impossible or requires a disproportionate effort. Upon request, Data Controller shall inform User about these recipients.

#  9. Compensation and „sérelemdíj”[[2]](#footnote-2)

Any person who has suffered financial or non-financial damage as a result of a breach of the Regulation is entitled to compensation from Data Controller or Data Processor for the damage suffered. Data Processor shall be liable for damages caused by data processing only when Data Processor did not comply with the obligations specifically imposed on data processors by the relevant legislation or disregarded or acted contrary to Data Controller's lawful instructions. Data Controller or Data Processor shall be released from this liability if Data Controller or Data Processor is able to prove not being liable in any way for the event causing the damage.

1. **ENFORCEMENT**

User may exercise his rights by e-mail or written request sent by mail.

User will not be able to enforce his rights if Data Controller is able to prove not being able to identify him. Where User's request is clearly unfounded or excessive (when the request is repeated several times in particular), Data Controller may charge a reasonable fee for the fulfilment of the request or refuse to oblige. It is the responsibility of Data Controller to prove the above. Should Data Controller have doubts about the identity of the natural person submitting the request, Data Controller may request additional information necessary to confirm the identity of the requester.

According to the Privacy Act, the Regulation and the Civil Code (Act V of 2013), User may

* contact Nemzeti Adatvédelmi és Információszabadság Hatóság (National Authority for Data Protection and Freedom of Information, Falk Miksa utca 9-11 Budapest, H-1055; www.naih.hu) or
* assert his rights in court. Depending on User's choice, the proceedings may also be brought in the court within whose jurisdiction User resides (please find the list and contact details of the courts at http://birosag.hu/torvenyszekek).

#  V. MANAGING PRIVACY INCIDENTS

A privacy incident is a security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized access to personal data transferred, stored, or otherwise processed. In order to control the measures related to privacy incidents and inform the supervising authority and Users, Data Controller shall keep a log recording the scope of personal data involved in the incident, the date, circumstances and impacts of the incident and the measures taken to control it. In the event of a privacy incident, Data Controller shall inform User and the supervisory authority of it without undue delay, but within a maximum of 72 hours, except in the cases where the incident does not threaten the rights and freedoms of natural persons.

#  VI. BACKUP DATA MANAGEMENT

Within the scope of IT protection, Data Controller shall, in particular, provide for measures to restore data files, including regular backups and the separate, secure management of the created copies (backup data).

Accordingly, Data Controller shall, in order to prevent the loss of electronically stored data, regularly create backups of the data of its database containing personal data to a separate data carrier three times a day.

The backups of the data of the website server are stored at the Seat of Data Controller

Backup storage period: 5 years

Rules of erasing backups: in the anonym registry, individual erasures may be tracked. Automatic erasures are performed according to the setting.

Access to backup data: Access to backups is restricted to those having specific access rights. Backup data may only be accessed following proper identification (username and password as a minimum).

# VII. MISCELLANEOUS

Data Controller shall reserve the right to unilaterally amend this Privacy Policy upon prior notice sent to User by means of the website. Such changes shall take effect in relation to User on the date specified in the notice, unless User objects to the changes.

In the case of User having provided the data of a third party when subscribing to the newsletter or for other purposes in order to use the service, or caused any damage during the use of the Website, Data Controller shall reserve the right to claim damages against User.

Data Controller shall not be responsible for verifying the personal data provided by User. The person providing the data is solely responsible for the validity of the information provided. When User provides his personal data, User shall also be responsible for the validity of the provided data, for the personal data being his own and using the services based on these data only himself.

Unless the context otherwise demands, words importing any gender shall be interpreted to mean any or all genders in this Policy.

This Privacy Policy enters into force on 10 January 2021.

1. A specific will including a power of attorney personally made and uploaded via the unified digital administration portal of Hungary („ügyfélkapu”)

 [↑](#footnote-ref-1)
2. A fee paid for non-material damages as defined by the Civil Code of the Republic of Hungary [↑](#footnote-ref-2)