

PRIVACY NOTICE

on online data processing and the processing of personal data within the framework of membership in the school cooperative

PannonDiák Iskolaszövetkezet, as data controller (registered office: 8000 Székesfehérvár, Berényi út 72-100.; e-mail: info@pannondiak.hu; Data Protection Officer: Dr Krisztián Bölcskei, who may be contacted by post at the Data Controller's registered office or by e-mail at info@adatvedelmiauditor.hu), hereby informs you of the details and other material facts concerning online data processing and the processing of personal data within the framework of membership in the school cooperative:

- Data processing in connection with online contracting
- Data processing related to the Job Alert service
- Data processing related to creating a CV through the website
- Data processing related to submitted CVs
- Data processing related to communication through social media
- Data processing related to the membership relationship
- Data processing related to the electronic delivery of payslips
- Data processing related to cookies and tracking technologies

Common characteristics of the processing activities:

- The website <https://pannondiak.hu/> is operated by the Data Controller.
- Pannonjob Kft. (8000 Székesfehérvár, Berényi út 72-100.) provides server and hosting services to the Data Controller.
- You may exercise your rights as a data subject - including the right of access, rectification, erasure and the right to be forgotten, restriction of processing, objection, data portability and withdrawal of consent; detailed descriptions are provided at the end of this Notice - by sending a statement to the Data Controller or the Data Protection Officer using the contact details above. You may also lodge a complaint with the Hungarian National Authority for Data Protection and Freedom of Information (NAIH; ugyfelszolgalat@naih.hu; 1363 Budapest, Pf. 9.; www.naih.hu), and, if you consider that your rights have been infringed, you may seek judicial remedy before the court having jurisdiction at your place of residence. The Data Controller draws attention to the fact that the exercise of rights may be subject to conditions and limitations in relation to certain processing activities. The Data Controller is required to examine these factors when a data subject exercises a right. If a right cannot be exercised in relation to a particular processing activity, the Data Controller will inform the data subject in writing, including electronically, of the factual and/or legal grounds excluding or limiting the exercise of the right, and will keep a record thereof.
- The Data Controller has established a framework of internal rules, procedures and training concerning data protection, confidentiality and data security and regularly reviews the measures adopted to safeguard the available data. It ensures the physical and information technology (logical) security of data and protects data through appropriate organisational and technical measures against unauthorised access, alteration, transmission, disclosure, deletion or destruction, accidental destruction or damage, and unavailability resulting from changes in technology. When determining and implementing security measures, the Data Controller takes account of the current state of technology and science and selects, from among possible processing solutions, the solution providing the higher level of protection for personal data, unless this would involve disproportionate difficulty.

In particular, but not exclusively, the Data Controller ensures:

- that unauthorised persons are denied access to the equipment used for processing (the data processing system);
- that unauthorised reading, copying, modification or removal of data media is prevented;
- that unauthorised entry of personal data into the data processing system and unauthorised inspection, modification or deletion of stored personal data are prevented;
- that unauthorised persons cannot use data processing systems by means of data transmission equipment;
- that persons authorised to use the data processing system can access only the personal data covered by their access authorisation;
- that it is possible to verify and establish the recipients to whom personal data have been or may be transmitted or otherwise made available by means of data transmission equipment;
- that it is possible to verify afterwards which personal data were entered into the data processing system, when and by whom;
- that unauthorised reading, copying, modification or deletion of personal data during transmission or transport of data media is prevented;
- that the data processing system can be restored in the event of disruption;
- that the data processing system remains operational, errors are reported, and stored personal data cannot be altered through malfunctioning of the system.

The Data Controller also carries out other processing activities, about which data subjects can find further information in separate privacy notices.

Online contracting

Main purpose of processing	Conclusion of contracts online; acceleration of the contracting process; implementation of paperless contracting in the interests of sustainability; and performance of the contract.
Data subjects	Natural persons identifiable from the data provided during online contracting.
Source of data	The data subjects.

Categories of personal data	Purpose	Legal basis	Retention period
Student identification data: name; place and date of birth; mother's name; permanent address; temporary address; social security number (TAJ); tax identification number.	Identification; contact; proof of student status; payment of financial consideration; provision of information and subsequent evidence; conclusion of the contract and subsequent evidence.	Conclusion and performance of an agreement (Article 6(1)(b) GDPR).	For 5 years after termination of the contractual relationship or, to comply with accounting legislation, for 8 years from the last day of the financial year containing the date of approval of the annual financial statements. The Data Controller applies the later expiry date.
Contact details: telephone number; e-mail address.			
Student-status data: name of educational institution; field/faculty; course; student card number; data from the student-status certificate.			
Payment data: bank account number.			
Acknowledgement of this Privacy Notice and its timestamp; declaration of data accuracy and its timestamp;			

Categories of personal data	Purpose	Legal basis	Retention period
student's electronic signature; name and electronic signature of the person authorised to sign for the Data Controller; timestamp.			

How does processing take place?	The data subject enters their data in the online contracting section of the website, attaches proof of student status, acknowledges this Privacy Notice and declares that the data are accurate. Based on the information provided, the Data Controller automatically completes the contract and sends it by automated e-mail for digital signature through the web interface supplied by CollectSign. The data subject signs the contract. After the signature and timestamp have been added, the contract is returned to the Data Controller and is also signed electronically by an authorised employee. The system then automatically sends the fully signed and timestamped contract to the e-mail address supplied by the data subject.
Where are the data stored?	The data are stored in the CollectSign system for 1 year and thereafter in the Data Controller's IT system for 5 years following termination of the contractual relationship, because the general limitation period for contractual claims is 5 years under Section 6:22 of Act V of 2013 on the Civil Code. If the contract qualifies as an accounting document supporting the accounting recognition of an economic event, it is retained for 8 years under Section 169(2) of Act C of 2000 on Accounting, calculated from the last day of the financial year containing the date of approval of the annual financial statements. The Data Controller applies the later expiry date. Storage takes place within the European Union.
Who may access the data?	The executive officer, the Data Protection Officer, and employees authorised to perform contracting, contract performance and accounting tasks, solely to the extent and for the period required by their authorisation.
Are data disclosed to third parties?	Yes. Data are disclosed to InfoScope Kft., the developer of CollectSign/mySigno, which enables electronic signatures. Data may also be disclosed to a legal representative, authority or court, but only where necessary.
Automated decision-making or profiling	None.
Other information	The Data Controller submits the PDF document intended for electronic (biometric or digital) signature via an application programming interface (API). The service can be used only through the Data Controller's own application account (host). CollectSign uses mySigno system components to manage electronic signatures applied to PDF documents. In the case of biometric signatures, the mySigno/SignPad application links the signature to the person and the document and guarantees integrity during network communication. At the end of the signing process, if all parties have signed and all technical and security checks have been passed, the PDF receives an advanced electronic certificate based on a qualified certificate and a qualified electronic timestamp. CollectSign performs adequate logging to make it possible to trace who worked with which document and when. Neither InfoScope Kft.'s system administrators and developers nor those of the Data Controller can access the signatory's biometric data, thereby safeguarding their security and integrity. The mySigno product has independent certification confirming that the handwritten signature it creates meets the requirements for an advanced electronic signature under the EU eIDAS framework.

Job Alert

Main purpose of processing	To provide the data subject with personalised information about the latest job vacancies in the categories selected by the data subject.
Data subjects	Any natural person who subscribes to the Job Alert service and provides personal data.
Source of data	The data subjects.

Categories of personal data	Legal basis	Retention period
Subject; e-mail address; keyword; county; field of work; acknowledgement of the privacy information and its timestamp.	Prior, freely given consent (Article 6(1)(a) GDPR).	Until the data subject unsubscribes.

How does processing take place?	The data subject enters their data on the website when subscribing to Job Alert.
Who may access the data?	The executive officer, the Data Protection Officer, and employees authorised to operate Job Alert, solely to the extent and for the period required by their authorisation. These employees are not authorised to access passwords.
Are data disclosed to third parties?	Data may be disclosed to a legal representative, authority or court, but only where necessary.
Automated decision-making or profiling	None.
Other information	The data subject may unsubscribe from Job Alert messages at any time by clicking the unsubscribe link at the bottom of the e-mail or by sending a request to info@pannondiak.hu. Unsubscription by post is possible at: 8000 Székesfehérvár, Berényi út 72-100.

Creating a CV through the website, submitting a CV and applying for a job

Main purpose of processing	To create a CV with content suitable for an employer while complying with data protection requirements; to send the CV to the Data Controller; and to apply for a job vacancy.
Data subjects	Any natural person who creates or submits a CV or applies for a job through the Data Controller's website.
Source of data	The data subject.

Categories of personal data	Legal basis	Retention period
CV data: name, birth name, title; place and date of birth; telephone number; sex; nationality; address; period available for work; studies, qualifications and duration of studies; professional experience and skills; language skills; driving licence; work-related preferences (location, roles, willingness to relocate); how the data subject learned about the Data Controller. Data provided when submitting a CV: name; e-mail address; telephone number; acknowledgement of the Privacy Notice; indication and timestamp of CV submission.	Prior, freely given consent (Article 6(1)(a) GDPR).	The Data Controller does not store data entered solely for creating a CV on the website. The generated and downloaded CV may be sent to the Data Controller by the data subject. If it is sent, the personal data contained in it are retained until consent is withdrawn.

How does processing take place?	The data subject may enter the specified data through the relevant interface on the website and download the CV generated from those data. The data are transmitted to the server hosting the website through an encrypted channel using the HTTPS protocol. By pressing the 'Create CV' button, the data subject generates and downloads the CV and may then send it to the Data Controller.
Who may access the data?	The Data Controller does not store data entered while a CV is being created. If the data subject sends the generated and downloaded CV to the Data Controller, its personal data may be accessed by the executive officer, Data Protection Officer, and the managers and employees of the Data Controller's HR, selection and recruitment units, solely to the extent and for the period required by their authorisation.
Are data disclosed to third parties?	Data may be disclosed to a legal representative, authority or court, but only where necessary.
Automated decision-making or profiling	None.
Other information	-

Communication through social media

Main purpose of processing	Establishing and maintaining contact with the Data Controller through the social media platform facebook.com.
Data subjects	Any natural person identified or identifiable from data provided through interaction or communication on social media.
Source of data	The data subjects.

Categories of personal data	Purpose	Legal basis	Retention period
Identification data made public on the social media platform under its rules (e.g. name); interactions performed under the platform's rules (e.g. likes and shares); data provided in messages; technical data such as the time of an interaction or message.	Identification; carrying out the interaction; replying; traceability and subsequent evidence.	Freely given consent (Article 6(1)(a) GDPR).	Until consent is withdrawn or the data are deleted, but no later than deletion of the Data Controller's social media page.

How does processing take place?	The data subject performs an interaction under the rules of the social media platform, such as sharing or liking a post, or sends a message to the Data Controller through the platform.
Automated decision-making or profiling	None by the Data Controller.
Joint controllership	The Data Controller informs data subjects that their data are also processed jointly by the operator of facebook.com, Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland. Information created by Meta concerning Page Insights data is available at: https://www.facebook.com/legal/terms/information_about_page_insights_data . Meta implements data protection as described at: https://www.facebook.com/legal/terms/page_controller_addendum . The Data Controller excludes liability for the lawfulness of processing performed by Meta.
Processor	The Data Controller has not appointed a processor for this activity.

Processing related to the membership relationship

Main purpose of processing	Establishing, performing and terminating the membership relationship with the Data Controller, and exercising rights and fulfilling obligations arising from that relationship in accordance with the membership agreement and Act X of 2006 on Cooperatives (the Cooperatives Act).
Data subjects	Persons having a membership relationship with the Data Controller.
Source of data	The data subject.

Categories of personal data	Legal basis	Retention period
Identification data (surname, given name, birth name, title, place and date of birth, mother's name, nationality); contact details (telephone number, permanent address, residence); social security number (TAJ); tax identification number; copy and number of student card; sex; marital status; bank account number; driving licence category; education and qualification data (schooling, vocational qualifications, copy of the document certifying the highest level of education, language skills); documents required for performance of tasks (required driving licence, health certificate booklet and other documents required by law or the role); relationship data (commencement, role, working time, place of performance, date, method and conditions of termination); proof of medical fitness; payroll data (working time, service fee and benefits); classification and other relationship data; employment-related personal data; personal data related to tax allowances.	Conclusion and performance of an agreement (Article 6(1)(b) GDPR); compliance with a legal obligation (Article 6(1)(c) GDPR) under the Cooperatives Act and other applicable legislation.	Personal data are erased when the purpose of processing ceases or at the data subject's request, except for data that must be retained under a statutory obligation. Personal data processed in connection with establishing, performing and terminating the relationship are retained until expiry of legal claims arising from that relationship - 5 years after termination under Section 6:22 of Act V of 2013 on the Civil Code - or for any longer period required by law.

Who may access the data?	The executive officer, the Data Protection Officer, and employees authorised to perform tasks related to membership relationships, solely to the extent and for the period required by their authorisation.
Are data disclosed to third parties?	In the course of providing services and on the basis of agreements with partners, the Data Controller may share the above data with the recipient of the service and with its partner so that it can exercise its rights and fulfil its obligations under the service agreement. For the purpose of occupational medical fitness examinations required by Decree 33/1998 NM on medical examinations and opinions concerning occupational, professional and personal-hygiene fitness, the Data Controller transfers the following data to the service provider carrying out the examination: name, job, social security number (TAJ), address and FEOR occupational code. Personal data may also be disclosed to a legal representative, authority or court, but only where necessary.
Automated decision-making or profiling	None.
Other information	-

Electronic delivery of payslips

Main purpose of processing	Electronic delivery of payslips.
Data subjects	Persons having a membership relationship with the Data Controller.
Source of data	The data subject.

Categories of personal data	Legal basis	Retention period
Name; e-mail address; payslip data.	Freely given consent (Article 6(1)(a) GDPR).	Personal data are processed while the purpose exists and until administration relating to termination of the membership relationship is completed. If the data subject withdraws consent to electronic delivery, the Data Controller will no longer send payslips electronically and will no longer process the data for this purpose.

Who may access the data?	The executive officer, the Data Protection Officer, and authorised employees of the Data Controller, solely to the extent and for the period required by their authorisation.
Are data disclosed to third parties?	Data may be disclosed to a legal representative, authority or court, but only where necessary.
Automated decision-making or profiling	None.
Other information	-

No personal data processing takes place in the following cases:

- use of the student wage calculator
- completion of the research questionnaire

The Data Controller does not save, store, retain or otherwise use personal data entered when the student wage calculator is used.

The Data Controller ensures the anonymity of respondents to the research questionnaire. It does not collect personal data and processes answers provided in the questionnaire solely in aggregated form for research purposes. Research results are published in professional materials and at events only in aggregated and anonymous form.

Cookies and tracking technologies

Cookies

Cookies are small text files containing IT data that ensure the proper operation of the website. They are stored on endpoint devices. The files recognise the device and adapt the display of the website to the user's preferences. Cookies are necessary for logging in and ensure the uninterrupted operation of functions. Cookie settings can be modified through the menu available in the pop-up window in the footer.

Types of cookies

Strictly necessary / functional cookies

These cookies are required to provide the website's functions. If functional cookies are disabled, certain website functions may not operate properly.

Performance cookies

These collect information about use of the website and user activity. They do not allow personal identification but may provide information about browser type, screen resolution and navigation through the website. Their purpose is to provide the website owner with information that can be used to improve the operation and quality of the website.

Advertising cookies

Their purpose is to tailor advertisements displayed on the website as closely as possible to visitors' needs and interests. Such cookies are provided only by websites on which advertisements are displayed.

Deleting cookies

All modern browsers allow cookie settings to be changed. Most browsers accept cookies automatically by default, but these settings can generally be changed to prevent automatic acceptance and to offer a choice each time. Because cookies are intended to make the website easier to use, preventing or deleting them may mean that you cannot use all website functions or that the website operates differently from intended in your browser.

Disabling cookies

Cookies are created and stored by the browser and may therefore be disabled in the browser. Please note that familiar websites may not operate correctly when cookies are disabled. Information on disabling cookies is available in your browser's Help section.

- Google Analytics browser opt-out plugin: <https://tools.google.com/dlpage/gaoptout>
- Disabling cookies in Chrome: <https://support.google.com/chrome/answer/95647?hl=en>
- Disabling cookies in Firefox: <https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop>
- Disabling cookies in Internet Explorer: <http://windows.microsoft.com/en-us/windows-vista/block-or-allow-cookies>

Facebook plugin

The website contains a Facebook plugin (Meta Inc., 1601 Willow Road, Menlo Park, California 94025, USA), indicated by the Facebook logo. The plugin establishes a direct connection between you and the Facebook profile hosted on the server. Facebook then learns from your IP address that you have visited our website. If you visit while logged in to your Facebook profile, Meta records information relating to the visit. Meta does not inform the Data Controller about the data it collects or how it uses them. For more information, contact Meta or read its privacy terms at <https://www.facebook.com/about/privacy/>.

Facebook Pixel

The website uses Facebook Pixel. This enables the Data Controller to display advertisements relating to job opportunities to data subjects whenever they visit Facebook or another website that also uses this tool. You may therefore encounter personalised advertising intended to draw attention to the website and its offers

and reflect your needs as closely as possible. Further information is available at <https://www.facebook.com/about/privacy/>.

Information about social media profiles

The Data Controller has profiles on Facebook and Instagram (together, 'social media'), where it publishes or may publish information. Social media administrators use cookies and similar technologies to record data subjects' behaviour during interactions with profiles. The full scope and purposes of personal data processed on social media are determined by the administrators of the relevant platform.

When you visit a profile, social media administrators create general statistical information about your interests and demographic data, such as age, sex and region, to which the Data Controller also has access. The Data Controller is fully responsible for management of its social media profiles and posts, information published by users, private messages and communications taking place on the specific platforms. Facebook and Instagram are operated by Meta Ltd., 4 Grand Canal Square, Dublin 2, Ireland ('Meta'). If you have an account on a social media website, the Data Controller has access to data you have marked as public under the same conditions as other users of that website.

Further information about data protection rights relating to the creation of website statistics and the possibility of exercising those rights directly against the social media platform is available at:

- Facebook: https://www.facebook.com/legal/terms/information_about_page_insights_data
- Instagram: <https://help.instagram.com/5195221251078753>

Google Analytics privacy statement

The website uses web-service analytics mechanisms supplied by Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA): Google Analytics, Google DoubleClick and Google Tag Manager. These services use cookies to analyse how websites are used. Information collected by cookies is sent to and archived on Google's servers in the United States.

If IP anonymisation is activated when you visit the website, Google truncates the user's IP address. This applies to EU Member States and countries listed in the Agreement on the European Economic Area. Only in exceptional cases is the full IP address sent to a Google server in the United States, where it is then truncated. IP anonymisation is active on the website.

At the website operator's request, Google uses the information collected to analyse website traffic and prepare reports on website use and services related to website use. The IP address transmitted by your browser within Google Analytics is stored separately from other Google data.

Cookie settings can be changed in the web browser. Depending on your choice, certain website functions may become unavailable. You can prevent collection of website data by cookies, including the IP address, its transmission to Google and its processing by Google by downloading and installing the following plugin: <https://tools.google.com/dlpage/gaoptout>.

Google Ads

The Data Controller uses Google Ads to promote the website on external websites in the form of Google advertisements. Data collected from advertising campaigns make it possible to measure the effectiveness of promotional activities. When you visit the website through a Google advertisement, this information is stored on your device in the form of a cookie, but is not in itself sufficient to identify you. The data collected may include information about specific advertisements displayed on websites and in the Google search engine and advertisements from Google partners. If you are a registered Google user, Google may store the fact of your

visit in connection with your account. If you are not registered or not logged in, Google may also store your IP address.

If you do not wish to receive such advertising, you may:

- disable third-party cookies by changing the relevant settings in your browser;
- disable conversion-tracking cookies from the domain www.googleadservices.com through your browser or at <https://www.google.de/settings/ads>; these settings are also deleted when cookies are removed;
- disable personalised advertisements forming part of the 'About Ads' campaign at <http://www.aboutads.info/choices>; these settings are also deleted when cookies are removed;
- permanently disable cookies in Firefox, Internet Explorer or Google Chrome; details are available at <http://www.google.com/settings/ads/plugin>.

Further information about Google's privacy policy is available at <https://policies.google.com/privacy>.

What rights do I have?

Legal basis	Information	Access	Rectification	Erasure	Restriction	Portability	Objection	Withdraw consent
Consent	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Agreement	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Legal obligation	Yes	Yes	Yes	No	Yes	No	No	No
Vital interests	Yes	Yes	Yes	Yes	Yes	No	No	No
Public task / official authority	Yes	Yes	Yes	No	Yes	No	Yes	No
Legitimate interests	Yes	Yes	Yes	Yes	Yes	No	Yes	No

The table above shows the relationship between data-subject rights and the applicable legal bases so that it is clear which rights may be exercised in each case.

Right to information (Articles 13 and 14 GDPR)

Where the Data Controller processes personal data concerning a data subject, it must provide the data subject, without a request being necessary, with information on the principal characteristics of the processing. This includes the purpose, legal basis and duration of processing; the identity and contact details of the Data Controller and its representative; the contact details of the Data Protection Officer; the recipients of the personal data; where processing is based on legitimate interests, the legitimate interests of the Data Controller and/or a third party; the data subject's rights and remedies, including the right to lodge a complaint with a supervisory authority; and, where the data are not obtained from the data subject, the source and categories of the personal data, unless the data subject already has this information. The Data Controller provides this information by making this Notice available.

Right of access (Article 15 GDPR)

The data subject has the right to obtain confirmation from the Data Controller as to whether personal data concerning them are being processed and, where that is the case, access to the personal data and information concerning the circumstances of processing. Where personal data are transferred to a third country or international organisation, the data subject has the right to be informed of the appropriate safeguards under Article 46 GDPR. At the data subject's request, the Data Controller will provide a copy of the personal data undergoing processing.

Right to withdraw consent (Article 7 GDPR)

The data subject may withdraw consent at any time. Withdrawal does not affect the lawfulness of processing based on consent before its withdrawal.

Right to rectification (Article 16 GDPR)

The data subject has the right to have inaccurate personal data concerning them rectified by the Data Controller without undue delay.

Right to object (Article 21 GDPR)

The data subject has the right to object at any time, on grounds relating to their particular situation, to processing based on Article 6(1)(e) or (f) GDPR. In that case, the Data Controller may no longer process the personal data unless it demonstrates compelling legitimate grounds that override the data subject's interests, rights and freedoms.

Right to restriction of processing (Article 18 GDPR)

The data subject has the right to request restriction of processing where any of the conditions laid down in the GDPR applies. In such a case, the Data Controller may perform no operation on the data other than storage. Where the data subject has objected to processing, restriction applies while it is being established whether the Data Controller's legitimate grounds override those of the data subject.

Right to erasure / right to be forgotten (Article 17 GDPR)

The data subject has the right to have personal data concerning them erased by the Data Controller without undue delay where the purpose of processing has ceased, consent has been withdrawn and there is no other legal basis, there are no overriding legitimate grounds following an objection, the data have been processed unlawfully, or erasure is necessary for compliance with a legal obligation. Where the Data Controller has made the personal data public and is required to erase them, it will, taking account of available technology and implementation costs, take reasonable steps, including technical measures, to inform controllers processing the data that the data subject has requested erasure of links to, copies of or replications of those personal data.

Right to data portability (Article 20 GDPR)

The data subject has the right to receive personal data concerning them that they have provided to the Data Controller in a structured, commonly used and machine-readable format, and to transmit those data to another controller without hindrance from the controller to which they were provided, where the statutory conditions apply, namely automated processing based on consent or an agreement.

Where and how can detailed information be requested and rights exercised?

Requests for information, access and the exercise of other rights may be submitted by a statement sent to the Data Controller's postal or e-mail address. The Data Controller will examine and answer the statement as soon as possible after receipt and will take the necessary measures in accordance with the statement, its Internal Data Protection Rules and applicable law.

Supervisory authority for complaints (Article 77 GDPR)

Hungarian National Authority for Data Protection and Freedom of Information

Address: 1055 Budapest, Falk Miksa utca 9-11.

Postal address: 1363 Budapest, Pf. 9.

Telephone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

Website: <http://www.naih.hu>

E-mail: ugyfelszolgalat@naih.hu

Further information about rights and lodging a complaint with the Authority is available at <http://naih.hu/panaszuegyintezes-rendje.html>.

If their rights are infringed, the data subject may also bring proceedings before the court having jurisdiction at their place of residence and may, among other remedies, claim damages for non-material harm.

The court having jurisdiction at your place of residence can be found at: <https://birosag.hu/birosag-kereso>

Finalised: 31 August 2026

Version: V3