

## PRIVACY NOTICE

regarding data processing carried out online, as well as the processing of personal data handled within the framework of membership in the school cooperative

The Data Controller, PannonDiák Iskolaszövetkezet (registered office: 8000 Székesfehérvár, Berényi út 72–100., Hungary; e-mail: [info@pannondiak.hu](mailto:info@pannondiak.hu); Data Protection Officer: Dr. Krisztián Bölcskei, reachable by post at the Data Controller’s registered office or by e-mail at [info@adatvedelmiauditor.hu](mailto:info@adatvedelmiauditor.hu)), hereby informs you about the details of data processing carried out online, as well as the processing of personal data handled within the framework of membership in the school cooperative, and other relevant facts:

- [Data processing related to registration on the website](#)
- [Login to the website](#)
- [Data processing carried out during online contract conclusion](#)
- [Job newsletter service](#)
- [CV creation via the website](#)
- [Data processing related to communication via social media platforms](#)
- [Data processing related to membership legal relationship](#)
- [Electronic transmission of payroll statements](#)
- [Cookies and tracking technologies](#)

### **Common Characteristics of the Data Processing Activities**

- The website <https://pannondiak.hu/> is operated by the Data Controller.
- Pannonjob Kft. (8000 Székesfehérvár, Berényi út 72–100., Hungary) provides server and hosting services to the Data Controller.
- You, as the data subject, may exercise your rights (right of access, right to rectification, right to erasure and the “right to be forgotten,” right to restriction of processing, right to object, right to data portability, and the right to withdraw consent – see detailed description of rights at the end of this Notice) by sending a statement to the contact details of the Data Controller or the Data Protection Officer indicated above. Furthermore, you may lodge a complaint with the supervisory authority (current contact details available at: National Authority for Data Protection and Freedom of Information (NAIH), [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu); 1363 Budapest, P.O. Box 9; [www.naih.hu](http://www.naih.hu)). If you believe that your rights have been violated, you may also turn to the court having jurisdiction based on your place of residence. The Data Controller draws the attention of data subjects to the fact that the exercise of their rights may be subject to certain conditions and limitations in relation to specific data processing activities. The Data Controller is obliged to examine such factors when a data subject exercises their rights. If a data subject is unable to exercise a specific right in relation to a given data processing activity, the Data Controller shall inform the data subject in writing (including by electronic means) of the factual and/or legal reasons restricting or excluding the exercise of that right and shall keep a record thereof.
- The Data Controller has established a framework including internal regulations, procedures, and training programs relating to data protection, confidentiality, and data security, and regularly reviews the measures implemented to ensure the security of the data available. Based on the above, the Data Controller ensures both the physical and

IT (logical) security of the data. Accordingly, the Data Controller protects the data through appropriate organizational and technical measures against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction or damage, and against becoming inaccessible due to changes in the applied technology. When defining and implementing measures serving data security, the Data Controller takes into account the current state of technology and scientific development, and, from among several possible data processing solutions, selects the one that ensures a higher level of protection of personal data, unless this would involve disproportionate difficulty. Within the scope of its tasks related to logical, i.e. IT security protection, the Data Controller ensures, in particular but not exclusively, the following:

- to prevent unauthorized persons from accessing the devices used for data processing (hereinafter referred to as the “data processing system”);
- to prevent the unauthorized reading, copying, modification, or removal of data storage media;
- az adatkezelő rendszerbe a személyes adatok jogosulatlan bevitelének, valamint az abban tárolt személyes adatok jogosulatlan megismerésének, módosításának vagy törlésének megakadályozásáról,
- to prevent the unauthorized entry of personal data into the data processing system, as well as the unauthorized access to, modification, or deletion of personal data stored therein;
- to ensure that persons authorized to use the data processing system have access only to the personal data specified in their access authorization;
- to ensure that it can be verified and established to which recipient personal data have been or may be transmitted or made available via data transmission equipment;
- to ensure that it can subsequently be verified and established which personal data were entered into the data processing system, at what time, and by whom;
- to prevent the unauthorized access to, copying, modification, or deletion of personal data during their transmission or while the data carrier is being transported;
- to ensure that the data processing system can be restored in the event of a malfunction;
- to ensure that the data processing system remains operational, that reports are generated on errors occurring during its operation, and that the stored personal data cannot be altered as a result of incorrect system operation.

- **The Data Controller also carries out additional data processing activities, about**

**which the data subject may find more detailed information in separate privacy notices that are formally distinct from this Notice.**

<b>Data Processing Related to Website Registration</b>		
<b>What is the main purpose of the data processing?</b>	Recording the data of the data subject for registration purposes, granting access, and facilitating login.	
<b>Who are the data subjects?</b>	Natural persons who can be identified based on the data provided during registration on the website.	
<b>What is the source of the data?</b>	The data subjects.	
<b>Categories of Processed Data</b>	<b>Legal Basis for Processing</b>	<b>Retention Period</b>
Identification data – name, date of birth	Prior and voluntary consent (Article 6(1)(a) of the GDPR)	Until the deletion of the registration – name, date of birth Contact details
Contact details - e-mail address, mobile phone number, landline phone number		
indication of full-time status		
indication of relevant geographical area		
password		
indication and time of acceptance of the privacy notice		

<b>How is the data processing carried out?</b>	<p>Activity and process related to the data processing:</p> <ol style="list-style-type: none"> <li>The data subject may provide the above-mentioned data via a designated section of the website and submit them to the Data Controller by clicking.</li> <li>The provided data are transmitted to the server hosting the website via an encrypted channel.</li> <li>The Data Controller sends a verification code to the provided e-mail address to confirm the registration. After the code is entered on the website, the registration becomes final.</li> <li>The data required for login are automatically recorded in an electronic registration system serving this purpose.</li> </ol>
<b>Who is authorized to access the data?</b>	Authorized employees of the Data Controller, strictly within the scope and duration of their authorization.
<b>Is data disclosed (access provided, transferred, or shared) to third parties?</b>	It may be disclosed to a legal representative, authority, or court, exclusively if necessary.
<b>Does automated decision-making or profiling take place?</b>	No.
<b>Additional information:</b>	Providing the data is essential for the execution of the purpose of data processing.

<b>Login to the Website</b>		
<b>What is the main purpose of the data processing?</b>	Identification of the data subjects logging in, ensuring and verifying their access rights, and modifying previously provided data where necessary.	
<b>Who are the data subjects?</b>	All natural persons who can be identified based on the data provided and who are identified (registered users).	
<b>What is the source of the data?</b>	The data subject.	
<b>Categories of Processed Data</b>	<b>Legal Basis for Processing</b>	<b>Retention Period</b>
Data used for identification of the data subject		Until the termination of registration; however, data generated during login are retained for the duration specified in the system's records

<ul style="list-style-type: none"> <li>- e-mail address</li> <li>- password</li> </ul>	Prior and voluntary consent (Article 6(1)(a) of the GDPR)	Recorded in a log file and stored for the duration of the log file retention period
Data generated during login:		
<ul style="list-style-type: none"> <li>- Time of login</li> <li>- IP address used during login</li> </ul>		
<b>How is the data processing carried out?</b>	The data subject may provide the above-mentioned data via the website's login interface and submit them to the Data Controller by clicking. If the e-mail address and password combination exists in the system, the user is granted access.	
<b>Who is authorized to access the data?</b>	Authorized employees of the Data Controller, strictly within the scope and duration of their authorization; however, employees are not authorized to access passwords.	
<b>Is data disclosed (access provided, transferred, or shared) to third parties?</b>	It may be disclosed to a legal representative, authority, or court, exclusively if necessary.	
<b>Does automated decision-making or profiling take place?</b>	No.	
<b>Additional information:</b>	Providing the data is essential for the execution of the purpose of data processing.	

<b>Online Contract Conclusion</b>			
<b>What is the main purpose of the data processing?</b>	Execution of contract conclusion in an online manner, thereby accelerating the contracting process and enabling a paperless contract in line with sustainability principles.		
<b>Who are the data subjects?</b>	Natural persons identifiable based on the data provided during online contract conclusion.		
<b>What is the source of the data?</b>	The data subjects.		
<b>Categories of Data</b>	<b>Purpose of Processing</b>	<b>Legal Basis</b>	<b>Retention Period</b>
Student identification data	Student identification data	Student identification data	Student identification data
<ul style="list-style-type: none"> <li>- Name</li> <li>- Place and date of birth</li> <li>- Mother's name</li> <li>- Permanent address</li> <li>- Temporary address</li> <li>- Social security number</li> <li>- Tax identification number</li> </ul>			
Student contact details	Communication		
<ul style="list-style-type: none"> <li>- Phone number</li> </ul>			

- E-mail address			
Student status data	Verification of student status		
- Name of educational institution - Faculty/field of study  - Major - Student ID number - Study certificate details			
Payment-related data	Performance of financial consideration		
- Bank account number			
Indication and date of acknowledgment of the privacy notice	Later proof of information		
Declaration of data accuracy and its date	Later proof		
Student's electronic signature	Confirmation of contract conclusion; later proof		
Name and electronic signature of the authorized person on the Data Controller's side			
Time stamp	Later proof		
<b>How is the data processing carried out?</b>	<p>The data subject provides their data on the website under the "online contract conclusion" tab, uploads proof of their student status, acknowledges receipt of the privacy notice, and confirms that their data are accurate.</p> <p>Based on the provided data, the Data Controller automatically completes the contract and sends it for digital signature via automatic e-mail through the web interface provided by CollectSign.</p> <p>The data subject signs the document. After signing and timestamping, the document is returned to the Data Controller, where an authorized employee also signs it electronically. The system then automatically sends the fully signed and timestamped contract to the data subject's provided e-mail address.</p>		
<b>Where are the data stored?</b>	<p>In the CollectSign system for 1 year, and thereafter in the Data Controller's IT system until the end of the retention period. Storage takes place within the territory of the European Union.</p>		
<b>Who is authorized to access the data?</b>	<p>Authorized employees of the Data Controller, strictly within the scope and duration of their authorization.</p>		

<b>Is data disclosed to third parties?</b>	Yes, to the developer of the electronic signature solution CollectSign / mySigno, namely InfoScope Kft.
<b>Does automated decision-making or profiling take place?</b>	No.
<b>Additional Information</b>	<p>The Data Controller submits the PDF document intended for electronic (biometric or digital) signature via an interface (API). The service can only be used through the Data Controller's own application account (host).</p> <p>The CollectSign system uses components of the mySigno system to manage electronic (biometric, digital) signatures applied to PDF documents. The mySigno/SignPad application ensures, in the case of biometric signatures, the link between the signature, the person, and the document, as well as data integrity during network communication.</p> <p>At the end of the signing process, provided that all parties have signed and all technical and security checks have been successfully completed, a qualified certificate-based advanced electronic signature and a qualified timestamp are applied to the PDF document. The CollectSign system ensures appropriate logging so that it can be tracked who worked on which document and when.</p> <p>Even the system administrators and developers of InfoScope Kft. do not have access to the signatories' biometric data, thereby ensuring the security and integrity of such data. Likewise, the Data Controller's own system administrators and developers do not have access to these biometric data.</p> <p>The mySigno product has independent certification confirming that the handwritten signature it generates complies with the EU eIDAS requirements for advanced electronic signatures.</p>

<b>Job Newsletter (Job Alert Service)</b>		
<b>What is the main purpose of the data processing?</b>	To provide the data subject with personalized information about the latest job offers arriving in the categories set by the data subject.	
<b>Who are the data subjects?</b>	Any natural person who subscribes to the job newsletter service.	
<b>What is the source of the data?</b>	The data subjects.	
<b>Categories of Data</b>	<b>Legal Basis for Processing</b>	<b>Retention Period</b>
Subject	Subject	Subject
E-mail address		
Search keyword		
County		

Field of study		
Indication and date of acknowledgment of the privacy notice		
<b>How is the data processing carried out?</b>	The data subject provides their data on the website when subscribing to the job newsletter service.	
<b>Who is authorized to access the data?</b>	Authorized employees of the Data Controller, strictly within the scope and duration of their authorization. However, employees are not authorized to access passwords.	
<b>Is data disclosed to third parties?</b>	No.	
<b>Does automated decision-making or profiling take place?</b>	No.	
<b>Additional Information</b>	The data subject may unsubscribe from the job newsletter at any time via the link provided at the bottom of the electronic messages, or by sending a cancellation request to the e-mail address: <a href="mailto:info@pannondiak.hu">info@pannondiak.hu</a> . Unsubscription can also be submitted by post to the following address: 8000 Székesfehérvár, Berényi út 72–100, Hungary.	

<b>CV Creation via the Website</b>		
<b>What is the main purpose of the data processing?</b>	To create a curriculum vitae (CV) with content that is suitable for employers while also complying with data protection requirements.	
<b>Who are the data subjects?</b>	Any natural person who creates a CV through the Data Controller's website.	
<b>What is the source of the data?</b>	The data subject.	
<b>Categories of Data</b>	<b>Legal Basis for Processing</b>	<b>Retention Period</b>
CV data fields (see on the website)	Prior and voluntary consent (Article 6(1)(a) of the GDPR)	If the data subject registers, the CV may be saved and will be stored until deletion of the registration. If the data subject does not register, the Data Controller does not store the data.
<b>How is the data processing carried out?</b>	The data subject may provide the above-mentioned data via a designated section of the website and submit them to the Data Controller by clicking. The provided data are transmitted to the server hosting the website through an encrypted channel via the HTTPS protocol. By clicking the "Create CV" button, the data subject generates the CV, which they may download, and they may also choose to register.	
<b>Who is authorized to access the data?</b>	If the CV is stored, authorized employees of the Data Controller, strictly within the scope and duration of their authorization.	

<b>Is data disclosed to third parties?</b>	No.
<b>Does automated decision-making or profiling take place?</b>	No.
<b>Egyéb információk:</b>	

<b>Data Processing Related to Communication via Social Media</b>			
<b>What is the main purpose of the data processing?</b>	Contacting and maintaining communication with the Data Controller via the social media platform (facebook.com).		
<b>Who are the data subjects?</b>	Any natural person who can be identified based on the data provided during interaction, contact, and communication on the social media platform.		
<b>What is the source of the data?</b>	The data subjects.		
<b>Categories of Data</b>	<b>Purpose of Processing</b>	<b>Legal Basis</b>	<b>Retention Period</b>
Personal identification data made publicly available on the social media platform in accordance with the platform's rules (e.g., name)	Identification	Voluntary consent (Article 6(1)(a) of the GDPR)	Until withdrawal of consent or deletion, but no later than the deletion of the Data Controller's page on the social media platform
Interaction performed by the data subject in accordance with the platform's rules (e.g., like, share, etc.)	Performance of interaction		
Data provided in messages	Responding to inquiries		
Technical data: time of interaction or message sending	Traceability, later evidence		
<b>How is the data processing carried out?</b>	The data subject performs interactions in accordance with the rules of the social media platform (e.g., shares or likes a post, etc.) or sends a message to the Data Controller via the social media platform.		

<b>Automated decision-making / profiling</b>	No such processing is carried out by the Data Controller.
<b>Joint Controllershship</b>	The Data Controller hereby informs data subjects that their data are also processed jointly with the operator of facebook.com, Meta (Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland). Data subjects may read Meta’s information regarding page insights data here: <a href="https://www.facebook.com/legal/terms/information_about_page_insights_data">https://www.facebook.com/legal/terms/information_about_page_insights_data</a> Meta processes data in accordance with the provisions set out in the following notice: <a href="https://www.facebook.com/legal/terms/page_controller_addendum">https://www.facebook.com/legal/terms/page_controller_addendum</a> . The Data Controller excludes any responsibility regarding the lawfulness of data processing carried out by Meta.
<b>Data Processor</b>	The Data Controller has not engaged a data processor for this processing activity.

<b>Data Processing Related to the Membership Legal Relationship</b>		
<b>What is the main purpose of the data processing?</b>	To exercise the rights and fulfill the obligations arising from the establishment, performance, and termination of the membership legal relationship with the Data Controller, in accordance with the provisions of the membership agreement and Act X of 2006 on Cooperatives (hereinafter: the “Cooperatives Act”), as well as other applicable legislation.	
<b>Who are the data subjects?</b>	Persons in a membership legal relationship with the Data Controller.	
<b>What is the source of the data?</b>	The data subject.	
<b>Categories of Processed Data</b>	<b>Legal basis:</b>	<b>Retention Period</b>
Personal identification data: Surname, first name, birth name, title, place of birth, date of birth, mother’s name, citizenship. Contact details: Phone number, permanent address, residence.	The Cooperatives Act and other relevant applicable legislation.	The personal data are deleted upon the termination of the purpose of data processing, or upon request of the data subject, except for data that the Data Controller is required to retain for a period specified by law. In connection with the establishment, performance, and termination of the legal relationship with the data subject, the Data Controller retains the processed personal data until the statute of limitations of any legal claims arising from the legal relationship expires, or for a longer period if required by law.

<p>Identification numbers: Social security number (TAJ), tax identification number. Education-related data: Copy and number of student ID card, gender, marital status, place and date of birth, tax number. Financial data: Bank account number. Driver's license data: Type of driving license. Study and qualification data: Educational qualifications, professional qualifications, highest education certificate copy, language skills. Documents required for task performance: Required driving license copy, medical health booklet, and other documents required by law or by the scope of the task. Data related to the legal relationship: Start date of the relationship, job/task description, duration of task performance, location of task performance, termination date, method and conditions of termination. Medical fitness certificate. Payroll-related data: Task performance time data; service fee/remuneration data; legal relationship data (dates, characteristics, classification data, etc.); personal data related to employment tax benefits.</p>		
<p><b>Who is authorized to access the data?</b></p>	<p>Authorized employees of the Data Controller, strictly within the scope and duration of their authorization.</p>	
<p><b>Is data disclosed (access provided, transferred, or shared) to third parties?</b></p>	<p>es. During the provision of services by the Data Controller, based on agreements concluded with partners, the Data Controller may share the above-mentioned data with the service recipient and with its partner in order to exercise its rights and fulfill its obligations under the service agreement. Furthermore, for the purpose of occupational medical fitness examinations required under Government Decree 33/1998 (NM Decree on the medical examination and evaluation of occupational, professional, and personal hygiene fitness), the Data Controller transfers the following data to the service provider conducting the examination: name, job position, social security number (TAJ), address, FEOR code.</p>	

<b>Does automated decision-making or profiling take place?</b>	No.
<b>Additional Information</b>	-

<b>Electronic Transmission of Payroll Statements</b>		
<b>What is the main purpose of the data processing?</b>	Electronic transmission of payroll statements.	
<b>Who are the data subjects?</b>	Persons in a membership legal relationship with the Data Controller.	
<b>What is the source of the data?</b>	The data subject.	
<b>Categories of Data</b>	<b>Legal Basis for Processing</b>	<b>Retention Period</b>
Name, e-mail address, payroll statement data	Voluntary consent (Article 6(1)(a) of the GDPR)	The Data Controller processes the personal data for the duration of the purpose of data processing, until the completion of administrative matters related to the termination of the legal relationship.
<b>Who is authorized to access the data?</b>	Authorized employees of the Data Controller, strictly within the scope and duration of their authorization.	
<b>Is data disclosed (access provided, transferred, or shared) to third parties?</b>	It may be disclosed to a legal representative, authority, or court, exclusively if necessary.	
<b>Does automated decision-making or profiling take place?</b>	No.	
<b>Additional Information</b>	-	

## **Cookies and Tracking Technologies**

### **Cookies**

Cookies are small text files containing IT data that ensure the proper functioning of the Website. They are stored on end-user devices. These files recognize the device and adapt the appearance of the Website to the user's preferences. Cookies are essential for logging into the Website and ensure the smooth operation of its functions.

You may modify your cookie settings in the menu available in the pop-up window located in the footer.

### **Characteristics of Cookie Types**

#### *Essential Cookies / Functional Cookies*

These are necessary to ensure the functionality of the website.

If functional cookies are disabled, certain features of the website may not work properly

### *Performance Cookies*

These collect information about the use of the website and user activity. They are not suitable for personal identification, but they provide information about the type of browser, screen resolution, and the way the website is navigated. Their purpose is to provide data to the website owner to improve the operation and quality of the website.

### *Advertising Cookies*

Their purpose is to ensure that advertisements displayed on the website are as relevant as possible to the visitor's needs and interests. Such cookies are only provided by websites that display advertisements.

### *Deletion of Cookies*

All modern browsers allow users to change cookie settings. By default, most browsers automatically accept cookies, but these settings can usually be modified to prevent automatic acceptance and to prompt the user each time to decide whether to allow cookies.

Please note that since cookies are intended to facilitate the usability of our website, preventing or deleting cookies may result in you being unable to fully use the website's functions, or the website may function differently in your browser than intended.

### *Disabling Cookies*

Cookies are created and stored by the browser; therefore, they can be disabled within the browser settings. However, please note that disabling cookies may cause commonly used websites to function improperly.

For information on how to disable cookies, please refer to the Help section of your browser.

- Disable Google Analytics via browser plugin: <https://tools.google.com/dlpage/gaoptout>
- Disable cookies in Chrome: <https://support.google.com/chrome/answer/95647?hl=en>
- Disable cookies in Firefox: <https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences>
- Disable cookies in Internet Explorer: <http://windows.microsoft.com/en-us/internet-explorer/block-or-allow-cookies>

### **Facebook Plugin**

The Website contains a Facebook plugin (Meta Inc., 1601 Willow Road, Menlo Park, California, 94025, USA). The Facebook plugin on our Website is indicated by the Facebook logo. The plugin establishes a direct connection between you and the Facebook server. Facebook then becomes aware of your visit to our Website via your IP address.

If you visit our Website while logged into your Facebook account, Meta will record information related to the visit. Meta does not inform the Data Controller about the data it collects or how it uses such data.

If you would like to learn more about Meta's privacy policy, please contact Meta or read its terms of use: <https://www.facebook.com/about/privacy/>

### **Facebook Pixel**

The Website uses Facebook Pixel. This allows the Data Controller to display advertisements related to the services to data subjects whenever they visit Facebook or other websites that also use this tool. As a result, you may encounter personalized advertisements designed to ensure that the Website and its offerings capture your interest and best reflect your needs.

If you would like to learn more about the protection of your personal data, please visit the relevant subpage of Meta: <https://www.facebook.com/about/privacy/>

### **Information About Social Media Profiles**

The Data Controller maintains profiles on the following social media platforms: Facebook, Instagram (hereinafter referred to as “social media”). Information may be published on these platforms. Social media administrators record user behavior through cookies and other similar technologies during interactions with the profiles. The full scope and purposes of personal data processed on social media are determined by the respective social media platform operators. When you visit the profile, the social media administrators generate general statistical information about your interests and demographic data (such as age, gender, and region), to which the Data Controller also has access. The Data Controller is fully responsible for managing its social media profiles and posts, user-published information, private messages, and communication conducted on the specific social media pages. Facebook and Instagram are operated by Meta Ltd., 4 Grand Canal Square, Dublin 2, Ireland (“Meta”). If you have an account on a given social media platform, the Data Controller may access the data you have marked as public under the same conditions as other users of the platform. For more detailed information about your data protection rights related to website statistics and the possibility of exercising such rights directly with social media providers, please visit:

1. Facebook: [https://www.facebook.com/legal/terms/information\\_about\\_page\\_insights\\_data](https://www.facebook.com/legal/terms/information_about_page_insights_data)
2. Instagram: <https://help.instagram.com/5195221251078753A>

### **Google Analytics Privacy Statement**

The Website uses web analytics services provided by Google Inc. (“Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA”), including Google Analytics, Google DoubleClick, and Google Tag Manager.

Google Analytics, Google DoubleClick, and Google Tag Manager use cookies to analyze how websites are used. The information collected by cookies is transmitted to Google’s servers located in the United States, where it is stored.

If the IP anonymization feature is activated while you visit the Website, Google shortens your IP address. This applies to member states of the European Union and countries listed in the Agreement on the European Economic Area (EEA). The full IP address is only transmitted to Google’s servers in the United States in exceptional cases, and even then, in shortened form. Therefore, the IP anonymization feature is active on the Website.

Upon request of the website operator, Google uses the collected information to analyze website traffic and to prepare reports on website usage and related services. The IP address transmitted by your browser within Google Analytics is stored separately from other Google data.

You may modify your cookie settings in your web browser. Please note that as a result of your choices, certain features of the website may no longer be available.

You can disable the storage of website data collected by cookies (including your IP address) and their transmission to Google, as well as their sharing by Google, by downloading and installing the following plugin: <https://tools.google.com/dlpage/gaoptout>

### Google Ads

Google Ads is used by the Data Controller to promote the website on external websites in the form of Google advertisements. Based on data collected from advertising campaigns, the effectiveness of promotional activities can be measured. When you visit the Website through a Google advertisement, your device stores this information in the form of a cookie; however, this alone is not sufficient for identification. Among the collected data, information related to specific advertisements displayed on websites and in the Google search engine, as well as advertisements originating from Google’s partners, may also be collected. If you are a registered Google user, Google may store the fact of your visit linked to your account. If you are not a registered Google user or are not logged in, Google may also store your IP address.

If you do not wish to see advertisements, you may:

a. Disable the use of third-party cookies in your browser by adjusting your cookie settings accordingly;

b. Disable conversion tracking cookies (i.e., cookies originating from the [www.googleadservices.com](http://www.googleadservices.com) domain) in your browser; settings can also be managed at <https://www.google.de/settings/ads> – please note that settings will also be deleted after cookies are removed;

c. Disable personalized advertisements that are part of the “About Ads” campaign at <http://www.aboutads.info/choices> – settings will also be deleted after cookies are removed;

d. Permanently disable cookies in browsers such as Firefox, Internet Explorer, or Google Chrome – for details, please visit: <http://www.google.com/settings/ads/plugin>. If you would like to learn more about Google’s privacy policy, please visit: <https://policies.google.com/privacy>

### What Are My Rights?

**The relationship between the data subject’s rights and the legal bases applied is shown in the table below to clearly indicate which rights may be exercised depending on the legal basis used.**

	Right to Information	Right of Access	Right to Rectification	Right to Erasure	Right to Restriction	Right to Data Portability	Right to Object	Right to Withdraw Consent
Consent	✓	✓	✓	✓	✓	✓	✗	✓
Contract	✓	✓	✓	✓	✓	✓	✗	✗
Legal Obligation	✓	✓	✓	✗	✓	✗	✗	✗
Vital Interest	✓	✓	✓	✓	✓	✗	✗	✗
Public Task / Official Authority	✓	✓	✓	✗	✓	✗	✓	✗
Legitimate Interest	✓	✓	✓	✓	✓	✗	✓	✗

### **Right of Access (Article 15 GDPR)**

The data subject has the right to obtain confirmation from the Data Controller as to whether or not personal data concerning them are being processed, and, where such processing is taking place, the right to access the personal data and information related to the circumstances of the processing. Where personal data are transferred to a third country or an international organization, the data subject has the right to be informed about the appropriate safeguards pursuant to Article 46 of the GDPR relating to the transfer. The Data Controller shall provide a copy of the personal data undergoing processing to the data subject upon request.

### **Right to Withdraw Consent (Article 7 GDPR)**

The data subject has the right to withdraw their consent at any time. Withdrawal of consent shall 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 obtain from the Data Controller, without undue delay, the rectification of inaccurate personal data concerning them.

### **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 of personal data concerning them which is based on Article 6(1)(e) or (f) of the GDPR. In such a case, the Data Controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject..

### **Right to Restriction of Processing (Article 18 GDPR)**

The data subject has the right to obtain from the Data Controller restriction of processing where one of the conditions set out in the GDPR applies. In such cases, the Data Controller shall only store the data and shall not perform any other operations with them.

If the data subject has objected to the processing, restriction shall apply for the period necessary to determine whether the legitimate grounds of the Data Controller override those of the data subject..

### **Right to Erasure (“Right to Be Forgotten”) (Article 17 GDPR)**

The data subject has the right to obtain from the Data Controller the erasure of personal data concerning them without undue delay where:

- the data are no longer necessary for the purposes for which they were collected;
- consent has been withdrawn and there is no other legal basis for processing;
- in case of objection, there are no overriding legitimate grounds for processing;
- the data have been unlawfully processed; or
- the data must be erased to comply with a legal obligation.

Where the Data Controller has made the personal data public and is obliged to erase them, it shall take reasonable steps, including technical measures, taking into account available technology and the cost of implementation, to inform other controllers processing the data that the data subject has requested the erasure of any links to, or copies or replications of, those personal data.

### **Right to Data Portability (Article 20 GDPR)**

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 has the right to transmit those data to another controller without hindrance from the Data Controller, where the legal conditions are met (automated processing and legal basis of consent or contract).

### **Where and How Can the Data Subject Request Information or Exercise Their Rights?**

The Data Controller informs data subjects that requests for information, requests for access, and the exercise of other rights may be submitted via postal mail or e-mail. The Data Controller shall examine and respond to such requests as soon as possible after receipt and shall take the necessary measures in accordance with the statement, the Internal Data Protection Policy, and applicable legislation.

### **Supervisory Authority Contact Details (Article 77 GDPR – Complaint)**

National Authority for Data Protection and Freedom of Information (NAIH)

Address: 1055 Budapest, Falk Miksa utca 9–11, Hungary

Postal address: 1363 Budapest, P.O. Box 9

Phone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

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

E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

For more information regarding rights and the procedure for filing a complaint, please visit: <http://naih.hu/panaszuegyintezes-rendje.html>

In case of violation of their rights, the data subject may also apply to the competent court at their place of residence and may claim compensation, among other remedies.

The competent court can be found here: <https://birosag.hu/birosag-kereso>

Closed: 06/10/2022

Version number: V2