

## PRIVACY POLICY

Dear Reader!

Below we would like to supply you with information in accordance with the General Data Protection Regulation 2016/679 of the European Parliament and Council (– “GDPR” - On the Protection of Natural Entities with Regard to the Processing of Personal Data and the Free Flow of Such Data)

Interested parties are informed that the data manager described in point 1 is the maintainer and operator of the website <https://archeodanube.eu> (hereinafter referred to as the Website) created during the implementation of the ArcheoDanube (DTP3-413-2.2) project (hereinafter referred to as the Project). With this data management information, we would like to inform you about the legal basis and conditions of data management on the Website, as well as the rights of the data subjects.

### 1. Data of the data controller:

Name: Westpannon Regional and Economic Development Public Nonprofit Ltd.  
Headquarters, mailing address: 9700 Szombathely, Horváth Boldizsár körút 9.  
phone number: +36/94/500-495  
e-mail address: [info@westpannon.hu](mailto:info@westpannon.hu)  
Representative of the data controller: Eszter Varga, Managing Director  
phone number: +36/94/500-495  
e-mail address: [info@westpannon.hu](mailto:info@westpannon.hu)

### 2. Types of data management:

#### 2.1. Data management related to registration on the Website by the Data Controller

On the Website, it is possible to register for Interested Parties that can be persons who are specifically active in the professional field of archaeology or regional development, and that declare this at the time of registration. By registering, the Interested Party expressly consents to the following data being recorded on the website, and for the purpose of establishing a professional relationship, to be known by registered persons also engaged in the same professional activity for the purpose of contact.

- **scope of managed data:** name, workplace e-mail address, title (Mr., or Miss, or Ms. or Dr, or PHD), organization (of which you register as a representative or employee), workplace phone number, description of the professional work performed by the inquirer, password,
- **purpose of data management:** implementation of the Project, verification of fulfilment, verification of fulfilment of the indicators undertaken in the Project, implementation of professional contact
- **legal basis for data management:** Article 6, paragraph (1) point a) GDPR, the consent of the data subject

- **is the automated decision-making implemented:** Automated decision-making is not implemented.
- **data transfer to third countries:** none
- **deadline for data deletion:** until the data subject withdraws his/her consent, in case of its nonexistence the deadline for deletion is the end of the project's maintenance period.

## 2.2. Data management related to analytical services and cookies

Cookies are small programmes that assist the functional operation of the visited website, collect data for traffic analysis purposes, or serve marketing purposes. The Data Controller uses cookies and tracking codes from third-party providers (in particular: Google, Facebook) to create page statistics, to measure user interest and demographic data, as well as behaviour on the website. In addition, the Data Controller may use aggregate data obtained from interest-based advertising services or audience data (such as age, gender and interests) for general website reporting and development as well as for use in advertisement remarketing lists.

The purpose of the above stated rules are to continuously develop our internet interfaces, and to increase the effectiveness of our internet interfaces and advertisements related to our campaigns.

On the Advertising Settings website made available by Google (<https://www.google.com/settings/u/0/ads/authenticated>), the Google Analytics service can be disabled in the case of Display ads, and the ads of the Google Display Network can be customized. In addition, all tracking by Google Analytics can be disabled using the <https://tools.google.com/dlpage/gaoptout/> browser module. We also use Facebook's remarketing code to display targeted ads. If you do not want to see ads based on page visits and interest, the service can be turned off at this link <https://www.facebook.com/settings?tab=ads>.

More information about the use of cookies can be found at <https://www.allaboutcookies.org> - including detailed instructions on how to delete cookies from your computer. For information on how to delete cookies from your mobile phone, read your device's manual. By using the website of the Data Controller, the data subject accepts the use of technical data and cookies as described above. It is important that they cannot in themselves be used to identify your identity and are deleted after leaving the page in accordance with the settings of the browser programme.

## 2.3. Newsletter subscription

You can subscribe to the data manager's newsletters by clicking on the advertisement appearing on the data manager's website or Facebook page, and also by filling out a paper-based form at the data manager's events. When sending newsletters, the e-mail address is used to uniquely identify users.

- **Purpose of data management:** sending e-mail newsletters to interested parties, providing information on the current information,
- **Legal basis for data processing:** voluntary consent of the data subject [GDPR Article 6 (1) point a)]
- **Scope of processed data:**

o date, time, e-mail address, name, address, telephone number, mobile phone number, position, date of consent given or opt-out of direct marketing inquiries,

- **is automated decision-making implemented:** Automated decision-making is not implemented.
- **data transfer to third countries:** none
- **deadline for data deletion:** The data controller deletes the personal data from the newsletter system two years after the user's last activity (e.g. e-mail opening, clicking), or if the data subject withdraws his/her consent, the given data will be deleted immediately after the withdrawal of consent data.

### **3. Those entitled to access data, the potential data processors**

#### **3.1. Persons entitled to access data within the management organization**

With regard to the personal data written in point 2, the following employees are entitled to access the personal data within the company's organization:

Executive Director

company managers

Director of Transnational Programmes

project managers

#### **3.2. Data processors**

On the basis of the conditions prescribed by the law, or on the basis of the agreement concluded with the company, the following persons are classified as data processors if necessary:

- **Fezo Informatics Limited Liability Company**, which created the website on the basis of a separate contract for the data controller and performs IT and system administration activities as required
- SalesAutopilot Ltd. (headquarters 1016 Budapest, Zsolt utca 6/C. IV. em. 4.; Tax number: 25743500-2-41): the company provides the technological solution necessary for data management to manage and store personal data managed by the data controller.

### **4. The rights of those concerned**

#### **4.1. Request for information**

The data subject may request information about the processing of his/her personal data, the current occurrence of data processing, his/her rights and guarantees any time, including, in particular, the person of the data controller or data processor, the legal basis, purpose, duration of data processing, the location of data storage, as well as the data security measures.

At the request of the data subject, the data controller provides information about its activities related to data management and data transmission.

The data controller shall provide the information in writing in an understandable form within a reasonably short time from the submission of the request, but within a maximum of 30 days.

Information is provided free of charge unless the applicant has submitted an information request for the same activity or data area to the data controller in the same year.

In other cases, the data controller determines reimbursement and provides the information after payment of the reimbursement.

#### **4.2. Deletion**

The data manager deletes the personal data if its processing is illegal, if the data subject requests it, if the purpose of the data management has ceased, or if the statutory period for storing the data has expired, or if it has been ordered by the court or the data protection authority.

The data controller notifies the data subject of the correction and deletion, as well as all those to whom the data was previously transmitted for the purpose of data management. The notification can be omitted if this does not harm the legitimate interests of the data subject in view of the purpose of the data management.

The data subject can request the correction or deletion of his/her personal data at the contact details of the data controller indicated in this information. The only **reason** to fail to delete it can be a legal restriction.

#### **4.3. Dissent**

The data subject may object to the processing of his/her personal data if

- processing (transmission) the personal data is necessary only to enforce the rights or legitimate interests of the data controller or the data processor, unless the data processing is ordered by law;
- personal data is used or forwarded for the purpose of direct business acquisition, public opinion polls or scientific research;
- exercising the right to dissent is otherwise permitted by law.

The data controller. - with the simultaneous suspension of data management - examines the objection within the shortest time from the submission of the application, but no more than 15 days, and informs the applicant of the result in writing.

If the dissent is justified, the data controller will terminate the data management - including further data collection and data transmission - and block the data, as well as notify about the dissent and the measures taken, all those to whom the personal data affected by the dissent was previously transmitted, who are obliged to take measures to enforce the right to dissent.

If the data subject does not agree with the decision made by the data controller, he/she may appeal to the court within 30 days of the decision being made.

The data controller cannot delete the data subject's data if the data processing is ordered by law. However, the data cannot be forwarded to the data recipient if the data controller has agreed to the dissent, or the court has established the legitimacy of the dissent.

#### **4.4. Right to transfer data**

The data subject may request the data provided by him/her to be received in a widely used, machine-readable format, or the data controller to transmit it directly to another data controller (GDPR Article 20).

#### **4.5. Authority, court corrective action order**

##### **4.5.1. Filing a complaint, starting a procedure with the data protection authority:**

Complaints can be filed against the activities of the data controller, and proceedings can be initiated:

Name: National Data Protection and Freedom of Information Authority (NAIH)

Headquarters: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

Postal address: 1534 Budapest, Pf.: 834

Phone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

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

##### **4.5.2. Legal remedies**

In the event of a violation of his/her rights, the affected person can also go to court against the data controller, if he or she has suffered a violation of rights by the controller of his or her personal data, or there is a direct risk of such violation.

#### **5. Security of data management:**

The data manager takes appropriate measures to protect the data managed, especially in connection with unauthorized access, change, transmission, making it available, disclosure, deletion, destruction, damage, as well as inaccessibility resulting from changes in the technology used.



The data controller selects and operates the IT tools used for the management of personal data during the provision of the service in such a way that the processed data:

- a) is accessible to those authorized to do so (availability);
- b) its authenticity and authentication are ensured (authenticity of data management);
- c) its immutability can be verified (data integrity);
- d) be protected against unauthorized access (data confidentiality).

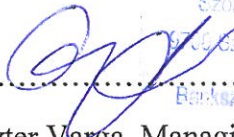
In order to protect the data files managed electronically in its various records, the data controller ensures with an appropriate technical solution that the stored data cannot be directly linked and assigned to the data subject, unless permitted by law.

In view of the ongoing development of technology, the data controller ensures the protection of the security of data management with technical, managerial and organizational measures that provide a level of protection corresponding to the risks arising in connection with data management.

During the data management the data manager keeps

- a) confidentiality: protect the information so that only those who are authorized to do so can access it;
- b) integrity: protects the accuracy and completeness of the information and the method of processing;
- c) availability: it ensures that when the authorized user needs it, he/she can really access the desired information and that the related tools are available.

Date: Szombathely, 1st November, 2022.

  
Nyugat-Pannon Terület- és Gazdaságfejlesztési  
Szolgáltató Közhasznú Nonprofit Kft.  
9700 Szombathely, Horváth Boldizsár krt. 9.  
Adószám: 21464912-3-02  
Beküldés: 13203198-06017916-40010012

Eszter Varga, Managing Director

representing Westpannon Regional and Economic  
Development Public Nonprofit Ltd., Data Manager