PRIVACY NOTICE

1. Purpose of the Privacy Notice

The purpose of this Privacy Notice is to set out the data protection and processing principles applicable to the documents sent and attached by the suppliers during the prequalification process via the SAP Ariba system, received by **ALTEO Energiaszolgáltató Nyilvánosan Működő Részvénytársaság** (registered address: 1117 Budapest, Dombóvári út 25.; company registration number: 01-10-045985; hereinafter referred to as the "**Company**" or the "**Data Controller**") and the related procedures, such as:

- the prequalification questionnaire,
- an extract from the Company Register,
- the Specimen Signature,
- the professional experience and qualifications of the persons involved in the project,
- the documents describing the business activity,
- the registration in the SAP Ariba supplier qualification system,
- conducting the prequalification processes in the SAP Ariba system, communication with the supplier,

as well as the Company's Data Protection and Processing Policy, which is considered to be binding on the Company.

The Company complies with its prior information disclosure obligation under Article 16 of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter referred to as the General Data Protection Regulation or "GDPR") and Act CXII of 2011 on the Right of Informational Self-determination and Freedom of Information (hereinafter referred to as the "Info Act"), by publishing this Privacy Notice.

2. Purpose of the data processing

2.1 The purpose of the Data Processing activities is to assess the professional experience and qualifications of the Data Subject, on the basis of the information provided during the business pre-qualification process, and to subsequently verify them (during the term of the contract), to prepare and conclude the contract, and to inform the Data Subject.

2.2 The Data Controller shall not use the personal data provided by the Data Subject under section 5 for any purpose other than the purpose set out in section 2.1. Unless otherwise provided by the law, the disclosure of the personal data to any third party, or to the courts or other authorities, is only possible on the basis of the relevant court or authority decision, or the Data Subject's prior express consent. The Company's subsidiaries within the meaning of Article 3 (2) (2) of Act C of 2000 on Accounting shall not be considered as unauthorized third parties, and by accepting this Privacy Notice, the Data Subject gives his/her express consent to the data transfer to his/her subsidiaries.

3. Legal basis of the Data Processing, the Data Controller's legitimate interest

3.1. The processing of the documents requested for pre-qualification and the personal data in them is necessary to enforce the legitimate interest of the Data Controller, so that the Data Controller, as the Customer, can be sure that its prospective supplier and the professionals employed by it have the skills and expertise to ensure the successful performance of the contract to be concluded.

Further, the purpose is also to be able to determine that there is no reason or circumstance excluding the conclusion of the contract with the prospective business partner.

3.2. The prequalification process, and the provision of the documents and data required to perform the prequalification process, are a prerequisite for the conclusion of the contract. In order to conclude the contract, the applicant supplier is obliged to provide the Data Controller with the documents and data requested by the Data Controller. In the event of refusal or late data provision, the Data Controller may withdraw from the conclusion of the contract, even if the other conditions are fulfilled.

3.3. If the contract is concluded, the Data Controller intends to keep the requested documents and data during the term of the contract, for possible future verification, so if the contract is concluded, the legal basis for the processing of the provided data is the Contract itself.

4. Duration of the Data Processing

The Company processes the personal data only for the shortest period necessary to achieve the purpose specified in section 2.1, or for the period specified by law, or, in the absence of such provision, for one (1) year from the date the personal data is provided to the Data Controller. The Data Controller may process the personal data of the Data Subject for as long as the purpose of the data processing exists (conducting the pre-qualification process, and if the contract is concluded, during the term of the contract). The Data Controller will terminate the processing of the personal data if the Data Subject has requested the erasue of his/her personal data pursuant to Article 14 (e) of the Info Act or pursuant to Article 17 of the GDPR.

5. Scope of the personal data processed

The Company only processes the documents sent or attached by the Data Subject, and the personal data included in them:

- contact details: name, email address, phone number, job title,
- CV data: education, name,
- the document attesting the qualification,
- declarations: name, mother's maiden name, address, personal ID card number, signature
- reference data: name, phone number, email address of the contact person for checking the reference provided

6. Principles of the Data Processing

6.1 The personal data may only be recorded and processed for the purpose specified in section 2, in accordance with the requirements of fairness and lawfulness.

6.2 The personal data may only be processed to the extent and for the time necessary to achieve the given purpose.

6.3 The data processing must be proportionate to what is specified in section 3.

6.4 The Company undertakes to process the personal data obtained and processed by it in full compliance with the Info Act, the GDPR and the data processing guidelines set out in this Privacy Notice, and not to disclose it to any third party not specified in this Privacy Notice or unauthorized.

6.5 The Company makes the personal data of the Data Subject available to third parties only in exceptional cases - on the basis of a judicial, official decision or statutory provision.

6.6 The Company undertakes to ensure the integrity and confidentiality of the data in accordance with Article 5 (1) (f) of the GDPR, and to ensure the security of the data processing in accordance with Article 32 of the GDPR. To this end, it will take technical and organizational measures to ensure the protection of the data recorded, stored or processed, and to prevent their destruction, unauthorized use or unauthorized alteration.

7. Right of disposal over the personal data

7.1 The Data Subject may request information from the Company about the processing of his/her personal data at any time in writing, by registered letter or by email sent to the following email address: compliance@alteo.hu . A request for information sent by regular mail will be considered authentic by the Company only if the Data Subject can be clearly identified from it. In the case of a request for information sent by email, the request will only be considered authentic if it is made from the email address used by the supplier in the procurement procedure/tender.

7.2 When such a request is received, the Company will provide the Data Subject with the necessary information within a maximum of twenty-five (25) days from the receipt of the request.

7.3 Information is provided by the Company free of charge. Providing information to the Data Subject may only be refused in the cases specified in Article 19 of the Info Act.

7.4 If the personal data is incorrect, and the correct personal data is available to the Data Controller, or the Data Subject requests the rectification of any of his/her personal data, the Data Controller shall rectify the personal data. Instead of erasure, the Data Controller will block the personal data, if the Data Subject requests it, or if, on the basis of the information available to it, it can be assumed that the erasure would be against the Data Subject's legitimate interests. The personal data thus blocked may only be processed as long as the purpose of the data processing that excluded the erasure of the personal data exists. The Data Subject shall be notified of the rectification, blocking, marking or erasure, as well as all those to whom the data have previously been transferred for the purpose of the Data Processing. If the Data Controller does not comply with the Data Subject's request for rectification, blocking or erasure, it shall provide the factual and legal reasons for the rejection of the request for rectification, blocking or erasure in writing within twenty-five (25) days of receipt of the request. If the request for rectification, erasure or blocking is rejected, the Data Controller shall inform the Data Subject about the possibility of judicial remedy, and the possibility of turning to the National Authority for Data Protection and Freedom of Information.

8. Data processing, data transfer

The Company uses the following data processors in the course of the Data Processing:

a. SAP SE - SAP Deployment Team
registered office: Dietmar-Hopp-Allee 16 69190 Walldorf,
registration authority: Mannheim HRB 719915
EU VAT number: DE143454214,
authorized signatory: Christian Klein (CEO),
phone: +49-6227-7-47474

email address: info@sap.com

b. DOQSYS Business Solutions Zrt.,

registered office: 1131 Budapest, Babér u. 1-5.,
company registration number: 01-10-048955,
VAT number: 25703133-2-41,
authorized signatory: Ákos Gergely, CEO,
phone: +36 20 444 0505
email address: info@doqsys.com

The Company may transfer the personal data to its own subsidiaries, if the possibility of concluding a contract with a given supplier (tenderer) arises at the subsidiary level. In this case, the data processing will be carried out by multiple data processors. If the Data Subject wishes to assert a claim in connection with the Data Processing by a subsidiary of the Company, the Company will forward the claim to the relevant subsidiary.

9. Amendments to this Privacy Notice

The Company reserves the right to amend this Privacy Notice at any time, by unilateral decision.

10. Enforcement options

10.1 The Data Subject may object to the processing of his/her personal data in the cases specified in Articles 21-24 of the Info Act and Article 21 of the GDPR. The Data Controller shall examine the objection as soon as possible, but not later than within fifteen (15) days from the submission of the application, make a decision on its merits and inform the Data Subject in writing of its decision. The Data Subject shall have the right to bring an action before the competent court within thirty (30) days of receipt of the information, or if no information is received.

10.2 In order to enforce his/her rights, in addition to the above, the Data Subject may also apply to the courts, in accordance with the provisions of the Info Act and Act V of 2013 on the **Civil Code,** which shall proceed in the case as a matter of urgency. The lawsuit will be adjudicated by the regional court. The lawsuit may also be brought before the court of the Data Subject's address or place of temporary residence, at the option of the Data Subject.

10.3 If you have any questions about the processing of your personal data, you can contact the National Authority for Data Protection and Freedom of Information (contact details: 1055 Budapest, Falk Miksa utca 9- 11; postal address: 1363 Budapest, Pf.: 9.).

10.4 In case of questions related to the data processing, you can contact the Company at the following email address: compliance@alteo.hu .

11. Definitions

1. data processing: the performance of technical tasks related to data processing operations, regardless of the method and means used to perform the operations and the place of application, provided that the technical task is performed on the data.
2. data processor: a natural or legal person, or an organization without legal personality, who processes data on the basis of a contract, including a contract concluded on the basis of a statutory provision.

3. data management: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
4. data controller: a natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of the processing are determined by Union or Member State law, the data controller or the specific criteria for the designation of the data controller may be determined by Union or Member State law. For the purposes of this Privacy Notice, the term Data Controller shall be understood as ALTEO itself.
5. data owner: the person responsible for ensuring that the assigned (supervised) data fulfils their role in the value creation process. Also responsible for ensuring that this is done effectively (keeping in mind the return on investment, exploiting new opportunities through developments, etc.) and safely (ensuring confidentiality, integrity and availability; requesting/approving effective and efficient protection). In terms of access management, it is his/her responsibility and liability to establish the access rules for the data he/she owns (e.g. defining the roles) and to approve the changes in the privileges (requests, withdrawals, etc.) in his/her own area.
6. personal data breach: the unlawful processing of personal data, in particular unauthorised access, alteration, transfer, disclosure, erasure or destruction, as well as accidental destruction and damage.
7. confidentiality: when the data has the feature that it is only accessible to a predefined group of users (authorized persons), not to everyone else. The loss of confidentiality means disclosure, when the confidential information becomes known and accessible to unauthorized persons.
8. criminal personal data: personal data relating to criminal convictions and criminal offences and the related security measures.
9. user: a person or organization that uses one or more IT systems to perform its duties.
10. third country: any State which is not an EEA State.
11. consent: a voluntary and definite expression of the will of the data subject, which is based on appropriate information and by which he/she gives his/her unambiguous consent to the processing of personal data concerning him/her, either in full or covering certain operations.
12. information security (IT security): a state of the information (IT) system - to the satisfaction of the Data Subject - in which the protection of the IT system is closed, complete, continuous and proportionate to the risks in terms of the confidentiality, integrity and availability of the data processed in the IT system, as well as in terms of the integrity and availability of the elements of the system.
13. entitlement: the right to data processing, information processing, and the use of various systems, programs, and tools.
14. sensitive personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic and biometric data for the purpose of uniquely identifying natural persons, health data and personal data relating to the sexual life or sexual orientation of natural persons.
15. personal data: data relating to the data subject, in particular the data subject's name, identification number, and one or more physical, physiological, mental, economic, cultural or social characteristics, as well as the conclusion that can be drawn from the data concerning the data subject.