



PRIVACY NOTICE

FOR CLIENTS

Name of relevant process	Privacy Notice – For clients	
Issue date	31. 01. 2025	
Modified	28. 02. 2025	
Version No.	2	
By	Reviewed by	Approved by
Tünde Székely Privacy Coordinator	Dr. Ágnes Dzodzoglu-Papp Head of Quality Management	Daniel Sperczel Managing Director



1 INTRODUCTION

This notice contains the processing practices of VantaSec Kft. (hereinafter referred to as the “**Controller**”) as described in Section 2.

The purpose of this notice is to provide information, pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter referred to as **GDPR**), about the data processing activities of the Controller in relation to its contractual partners and customers, and about the data processing practices it follows and applies.

In order to promote the transparency of information, the Controller shall prepare separate privacy notices concerning the data processing activities related to individual services and processes, each containing the information related to the specific activity. Therefore, this data privacy policy is not intended to present the entire range of activities and related processes of the Controller beyond those described in Section 2. Should further data processing activities occur or the processing of the data of the data subjects be used in further processes, we will make a separate information notice available, for example, in the case of training-related activities, we will publish a separate privacy notice for the participants.

1.1 Data and contact details of the Controller

Name of the Controllers	VantaSec Kft.
Representative of the Controllers	Daniel Sperczel
Seat	H-1123 Budapest, Nagyenyed utca 16 I/6
Telephone number	+36 70 407 4000
E-mail address	info@vantasec.hu

1.2 Privacy coordinator

Name	Tünde Székely
E-mail address	info@vantasec.hu



2 DATA PROCESSING ACTIVITIES

2.1 Activities related to the conclusion of contracts and the submission of quotations

The Controller processes the following personal data in connection with the contracting parties and Clients with whom it has a relationship. The data may be obtained from direct data provision by the contracting party or the person in question.

Processed personal data	Purpose of data processing	Legal basis for data processing	Duration of data processing
Name and title of the company representative and/or name, e-mail address, and phone number of the contact person	Conclusion of contracts, coordination of the parties' economic activities, fulfilment of obligations, communication	<p>In the case of natural persons, fulfilment of a contract or steps preceding it, pursuant to Article 6(1)(b) of the GDPR</p> <p>In the case of a non-natural person, the legitimate economic interest of the Controller pursuant to Article 6(1)(f) of the GDPR</p>	In the case of data related to a contract, the termination of the contract or the deadline for enforcing legal claims, i.e. 8 years (Act C of 2000 [Accounting Act])
Name and contact details of the contracting party, billing information			
Name of company representative, contact person's name, e-mail address, telephone number, subject of inquiry, message	Responding to requests for quotations, initiating contact via the Controller's website		Until consent is withdrawn*, or the right to deletion is exercised, but no longer than 1 year from the date of the relevant data collection

2.2 Activities related to the provision of services

Based on contracts concluded with its Clients, the Controller may have access to additional personal data during the performance of the ordered service(s), such as auditing services and the performance of tasks related to designated roles.

Processed personal data	Purpose of data processing	Legal basis for data processing	Duration of data processing
Personal data included in evidence relating to the subject of certification, processed during certification and audits in the course of service provision activities	Accredited certification activities, Auditing services Retention of evidence	Necessary for compliance with a legal obligation pursuant to Article 6(1)(c) of the GDPR – based on Decree 1/2015 SZTFH; and fulfilment of a contract pursuant to Article 6(1)(b) of the GDPR	For 4 years based on the internal regulations of VantaSec Kft., approved by the accrediting authority in accreditation procedures as a designated certification body, for 5 years based on Decree 1/2015 SZTFH, and for 10 years based on Decree 3/2003. (X.3.) IHM, Section 13(1).



2.3 Activities related to measuring customer satisfaction

In order to improve its services, the Controller monitors customer feedback and regularly assesses customer satisfaction, in the course of which it carries out the following data processing activities.

Processed personal data	Purpose of data processing	Legal basis for data processing	Duration of data processing
Company name, name and e-mail address of contact person, responses given in the evaluation	Operation of an Integrated Management System, monitoring customer feedback and customer satisfaction, development of services	the legitimate economic interest of the Controller pursuant to Article 6(1)(f) of the GDPR	A maximum of 5 years from the date of the assessment or until a successful objection by the data subject

*Consent may be withdrawn at any time, but withdrawal does not affect the lawfulness of data processing performed prior to the withdrawal.

2.4 Automated decision-making, profiling

Please note that the Controller does not undertake any profiling or automated decision-making.

3 ACCESS TO DATA

3.1 Persons entitled to access the data

During the performance of data processing activities, personal data may be accessed by employees and contractors of the Controller who are involved in the performance of the given task, to the extent and for the duration necessary for the performance of such task.

3.2 Recipients of personal data

In order to ensure that our services are provided in full, we work with subcontractors and collaborating partners who participate in the processing of personal data. In such cases, personal data will be transferred to data processors to the extent necessary for them to perform their tasks, as summarised in the table below.

Recipient	Purpose of data transfer	Personal data affected
Contributors	Those providing financial and other operational services to the Controller, and performing business consulting activities	Personal data necessary for the performance of services and tasks provided by a contributor
CLUSTER Informatika Kft. H-2112 Veresegyház, Baragödör utca 2. 1.	IT services, system operation, website operation	Data stored on file servers and on the administrator interface of the website



Recipient	Purpose of data transfer	Personal data affected
Supervisory bodies, authorities (e.g., National Accreditation Authority, Supervisory Authority for Regulatory Affairs)	Transmission of data required for official accreditation procedures	Personal data necessary for performing accredited certification and auditing activities
	Provision of audit services	Personal data necessary for performing auditing activities regulated by the legal framework**
	Auditing the use and appropriation of national budget and European Union funds, official investigations	Data requested by supervisory bodies and authorities
Service providers (Microsoft product family, EasyProject)	Performing activities necessary for the operation of the Controller, utilising tax, accounting, payroll, and IT services	Personal data necessary for the performance of activities offered by the service provider

**Legal framework:

- Act LXIX of 2024 on the Cybersecurity of Hungary
- Government Decree No. 418/2024 (XII. 23) on the implementation of the Act on the Cybersecurity of Hungary
- Decree No. 7/2024. (VI. 24.) MK

Security of data processing

The Controller takes the necessary technical and organisational measures and establishes appropriate procedural rules to ensure the security of personal data throughout the entire data processing process.

The Controller selects and operates the IT tools used for the processing of personal data in such a way that

- the data processed be accessible to those entitled to access it (availability);
- the authenticity and verification of the data processed be guaranteed (authenticity of data processing);
- the integrity of the data processed can be verified (data integrity);
- the data processed be protected against unauthorised access (data confidentiality).

Controller

- protects the data with appropriate measures against accidental or unauthorised destruction, loss, alteration, damage, unauthorised disclosure or unauthorised access;
- restricts access to personal data by assigning authorisation levels;
- protects IT systems using firewalls and virus protection;
- ensures that, during electronic data processing, data is only accessed by those persons who need it in order to perform their duties, in a controlled manner and only for the purpose for which it is intended;



- in order to protect the data files processed electronically in its various registers, it ensures, by means of appropriate technical solutions, that the stored data cannot be directly linked and assigned to the data subject, unless permitted by law;
- selects its subcontractors and contractual partners in such a way that those parties have adequate guarantees and protection with regard to compliance with the relevant data protection and information security requirements.

The Controller takes technical, organisational and administrative measures to ensure the security of data processing in line with the current state of technology, providing a level of protection proportionate to the risks associated with data processing.

The Controller ensures the security of data processing and the compliance and quality of service provision by introducing and certifying standardised management systems, a requirement it also imposes onto its suppliers. For the sake of accountability, it keeps all records required by law.

4 RIGHTS OF DATA SUBJECTS AND CONDITIONS FOR ENFORCING SUCH RIGHTS

The persons affected by the data processing, i.e. the data subjects may request information about the processing of their personal data at any time, and may request the rectification, clarification, deletion, or restricted use of their personal data, and may exercise all rights to which they are entitled by law.

4.1 The process of fulfilling requests

The Controller provides the requesting party with the information in writing, in an easily understandable form, within the shortest possible time following the submission of the request, but no later than within one month, via the contact details provided by the requesting party for this purpose. The submission and processing of the application can be initiated free of charge. The Controller may only refuse to fulfil the request in cases specified by law. Regardless of whether the request is denied or fulfilled, the Controller provides information about the measures taken, in accordance with the enforcement of rights referred to in the request. If the Controller has reasonably justified doubts about the identity of the data subject at the time of submitting the request, additional information may be required to confirm the identity of the data subject. If the Controller does not take measures in response to your request without delay, but no later than one month from the receipt of the request, it shall still be obliged to inform you of the reasons for not taking measures and to inform you that you may lodge a complaint with the Authority and exercise your right to judicial remedy before the court with jurisdiction over your place of residence or domicile.

4.2 Right to information and access

At your request, the Controller provides information about the data processed by the Controller or by the data processor commissioned by the Controller, the source of the data, the purpose of the data processing, the legal basis, the duration, the name and address of the data processor and its activities related to data processing, and – if your personal data is transferred – the legal basis and the recipient of the data transfer.

4.3 Right to rectification

Based on your right to rectification, you are entitled to request that the Controller rectify inaccurate personal data regarding you without undue delay, and you are also entitled to request that incomplete personal data be completed.



4.4 Right to erasure, right to be forgotten

You have the right to request that the Controller delete your personal data, and the Controller is obliged to delete it without undue delay, provided that certain conditions are met.

Personal data shall be deleted if its processing is unlawful; the purpose of data processing has ceased to exist or the statutory time limit for retaining the data has expired; or a court or the Authority has ordered its deletion.

It is not possible to delete and "forget" personal data when any of the cases specified in Article 17(3) of the General Data Protection Regulation apply, including, among others, when the Controller is subject to an obligation under EU or Member State law to retain such data.

4.5 Right to restriction of processing

The Controller will restrict the processing of personal data if you so request, or if, based on the information available:

- you contest the accuracy of your personal data. In this case, the restriction applies to the period of time that allows the Controller to verify the accuracy of your personal data;
- the processing is unlawful, and you object to the erasure of the personal data and instead request the restriction of the use of such data;
- the Controller no longer needs the personal data for the purposes of the processing, but you require such data for the establishment, exercise, or protection of legal claims;
- you have objected to the processing of data. In this case, the restriction applies for the period until it is established whether the legitimate grounds of the Controller prevail over your legitimate grounds or not.

4.6 Right to object

You have the right to object to the processing of your personal data at any time for reasons related to your specific situation, if the processing of your personal data is based on the legitimate interests of the Controller. If you object to the processing of your personal data, your personal data may no longer be processed for this purpose, unless there are compelling legitimate grounds for processing that override your interests, rights, and freedoms, or for the establishment, exercise, or protection of legal claims.

If the Controller determines that your objection is justified, it will terminate the data processing, including further data collection and data transfer, and will restrict the data, and also notify about the actions taken based on the objection all those to whom it has previously transferred the personal data subject to the objection, and who are obliged to take action in order to enforce the right to object.

4.7 Right to data portability

Based on this right, you are entitled to receive your personal data having been made available to the Controller in a structured, commonly used, machine-readable format, and you are also entitled to transfer this personal data to another controller without the Controller to whom you have made available the personal data preventing you from doing so. You may exercise this right when the data processing is based on consent or a contract, and the data processing is carried out in an automated manner.



4.8 Right to remedy

Should the Controller fail to fulfil any of your requests in a verifiable manner, subject to the statutory deadlines, you may submit a complaint to the Authority. Should your rights be violated, you may also take legal action before a court in the cases specified by law. The court will hear the case as a matter of urgency. If you have suffered material or non-material damage as a result of a breach of the General Data Protection Regulation, you are entitled to compensation from the Controller or the data processor in respect of the damage suffered. The Controller or the data processor shall be exempt from liability if they can prove that the damage was caused by an unavoidable cause outside the scope of data processing. The damage shall not be reimbursed if it resulted from your intentional or grossly negligent conduct. Submitting an objection or complaint shall not affect your other rights specified in the data protection legislation.

You may submit a complaint:

- To the Controller via the contact details provided above;
- to the Authority (H-1055 Budapest, Falk Miksa utca 9-11, ugyfelszolgalat@naih.hu, H-1363 Budapest, Pf.: 9., +36 (1) 391 1400);
- you can ultimately refer the matter to a court (information on the contact details of courts is available at the following link: <http://birosag.hu/torvenyszekek>).

Should you have any further questions regarding this notice, the processing of personal data by the Controller, or the interpretation of the relevant legislation, please contact us using one of the contact details provided.