Data processing agreement

Under Article 28 of the General Data Protection Regulation (EU) 2016/679, between the public body as controller and TresBizz BV as processor, for assessments, phase 0, pilots and support on NEXZOS.

Template version of 5 September 2026 · Fields marked like this are completed per assignment · Annexes 1 to 3 form part of the agreement

Your own model is welcome. Many public bodies work with a prescribed model, such as the Dutch government model processing agreement or the one attached to ARBIT-2022. We accept those; this template exists so that the content can be checked before the order, and so that nothing waits on a lawyer's calendar.

The parties

Controller	[Name of the public body], [registration number], [address], represented by [name and role], hereinafter the Controller
Processor	TresBizz BV, VAT BE 1033.718.409, 231 Avenue Louise, 1050 Brussels, Belgium, represented by its director, hereinafter the Processor
Main agreement	The quotation or order for [assessment level / phase 0 / pilot / support] dated [date], reference [reference]

Article 1. Definitions

1.1 Terms written with a capital letter have the meaning given to them in Article 4 of the GDPR: Personal Data, Processing, Data Subject, Personal Data Breach, Supervisory Authority. Sub-processor means any third party engaged by the Processor to process Personal Data on behalf of the Controller.

1.2 In the event of conflict between this agreement and the main agreement, this agreement prevails in matters of data protection.

Article 2. Subject matter, duration, nature and purpose

2.1 The Processor processes Personal Data solely for the performance of the main agreement, as specified in Annex 1: the subject matter, the duration, the nature and purpose of the Processing, the types of Personal Data and the categories of Data Subjects.

2.2 This agreement runs for the duration of the main agreement and for as long as the Processor holds Personal Data on behalf of the Controller thereafter.

Article 3. Instructions of the Controller

3.1 The Processor processes Personal Data only on documented instructions from the Controller, including with regard to transfers to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject. In that case the Processor informs the Controller of that legal requirement before Processing, unless the law prohibits such information on important grounds of public interest.

3.2 The main agreement, this agreement and Annex 1 together constitute the documented instructions. Further instructions are given in writing, including by e-mail.

3.3 The Processor informs the Controller immediately if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

Article 4. Confidentiality

4.1 The Processor ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that they process the Personal Data only on the Controller's instructions.

4.2 Access is limited to the persons who need it for the performance of the main agreement. The Processor keeps a list of those persons and provides it on request.

Article 5. Security of Processing

5.1 The Processor implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR. The measures in place at the date of signature are set out in Annex 3.

5.2 The Processor may update the measures in Annex 3 provided the level of security does not fall below the level at the date of signature. Material changes are notified to the Controller in writing.

5.3 Personal Data is stored and processed within the European Economic Area, on systems designated in Annex 2.

Article 6. Sub-processors

6.1 The Controller gives general written authorisation for the engagement of the Sub-processors listed in Annex 2.

6.2 The Processor informs the Controller in writing of any intended addition or replacement of a Sub-processor at least 30 days in advance, thereby giving the Controller the opportunity to object. If the Controller objects on reasonable grounds relating to data protection, the parties consult in good faith; if no solution is found, the Controller may terminate the affected part of the main agreement without penalty.

6.3 The Processor imposes on each Sub-processor, by way of a written contract, the same data protection obligations as set out in this agreement. Where a Sub-processor fails to fulfil its obligations, the Processor remains fully liable to the Controller for the performance of that Sub-processor's obligations.

Article 7. Transfers outside the European Economic Area

7.1 The Processor does not transfer Personal Data to a country outside the European Economic Area, and does not permit access from such a country, without the prior written instruction of the Controller.

7.2 Where such a transfer is instructed, it takes place only under an adequacy decision of the European Commission, or under the Standard Contractual Clauses adopted by the Commission together with any supplementary measures required.

Article 8. Assistance to the Controller

8.1 Taking into account the nature of the Processing, the Processor assists the Controller by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Controller's obligation to respond to requests for exercising the Data Subject's rights under Chapter III of the GDPR. Requests

received directly by the Processor are forwarded to the Controller within five working days and are not answered by the Processor on its own account.

8.2 The Processor assists the Controller in ensuring compliance with Articles 32 to 36 of the GDPR (security, breach notification, data protection impact assessment and prior consultation), taking into account the nature of the Processing and the information available to the Processor.

8.3 Assistance that falls within the scope of the main agreement is provided without additional charge. Assistance that goes beyond it is charged at the hourly rate stated in the main agreement, after prior agreement on the effort.

Article 9. Personal Data Breach

9.1 The Processor notifies the Controller without undue delay after becoming aware of a Personal Data Breach, and in any event within 48 hours, at the contact address in Annex 1.

9.2 The notification contains, to the extent known at that moment: the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point for further information. Information that is not yet available is provided in phases as soon as it becomes available.

9.3 The Processor does not inform Data Subjects or a Supervisory Authority of a breach on its own initiative, unless required by law. Any such communication is made by the Controller, or by the Processor on the Controller's instruction.

Article 10. Deletion and return

10.1 At the end of the provision of services, the Processor, at the choice of the Controller, deletes or returns all Personal Data and deletes existing copies, unless Union or Member State law requires storage of the Personal Data. The default choice, absent instruction, is deletion within 30 days after the end of the main agreement.

10.2 Return takes place in a common, machine-readable format. The Processor confirms deletion in writing on request.

Article 11. Information and audit

11.1 The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR.

11.2 The Processor allows for and contributes to audits, including inspections, conducted by the Controller or by an auditor mandated by the Controller. An audit is announced at least 14 days in advance, takes place during working hours, is limited to what is necessary to verify compliance with this agreement, and takes place at most once per calendar year unless a Personal Data Breach or an instruction of a Supervisory Authority gives reason for more. The auditor is bound by confidentiality.

11.3 Each party bears its own costs of an audit. Where an audit reveals a material breach of this agreement by the Processor, the Processor bears the reasonable costs of the audit.

Article 12. Liability

12.1 The liability of the parties towards each other for damage resulting from a breach of this agreement is governed by the liability provisions of the main agreement, without prejudice to Article 82 of the GDPR as regards liability towards Data Subjects.

Article 13. Term, termination and final provisions

13.1 This agreement ends when the main agreement ends and the Processor has fulfilled its obligations under Article 10. The obligations of confidentiality survive that ending.

13.2 This agreement is governed by the law that governs the main agreement. Where the main agreement is subject to ARBIT-2022, the data protection provisions of ARBIT-2022 apply and this agreement is read in conformity with them.

13.3 Amendments are valid only in writing and signed by both parties. If any provision proves invalid, the remaining provisions remain in force and the parties replace the invalid provision by a valid one that comes closest to its purpose.

Controller	**Processor**
[Name of the public body]	TresBizz BV
Name: [ ]	Name:
Role: [ ]	Role: Director
Date and signature:	Date and signature:

Annex 1. Details of the Processing

Subject matter	[Assessment at level ... / Phase 0 / Pilot on ... workstations / Support and updates] under the main agreement
Duration	The term of the main agreement, plus the deletion period of Article 10
Nature of the Processing	Collection from exports supplied by the Controller, analysis, storage for the duration of the assignment, reporting in aggregated form, deletion. During a pilot: installation and configuration of workstations, and remote support at the Controller's request
Purpose	Judging the Controller's workstation estate and applications for a migration to NEXZOS, and, during a pilot, delivering and supporting that migration on the workstations in scope
Types of Personal Data	Assessment and phase 0: names, roles and business contact details of the Controller's staff involved; device names and asset identifiers that may identify a user; names of application owners; interview notes. Pilot and support: in addition, user account names on the workstations in scope, and system and support logs that may contain user identifiers. [Strike out or add per assignment]
Special categories	None are required. The Controller does not supply, and the Processor does not request, special categories of Personal Data within the meaning of Article 9 of the GDPR. Should any appear in an export, the Processor deletes it and informs the Controller
Categories of Data Subjects	Employees and contractors of the Controller who use or manage the workstations in scope, and staff involved in the assignment
Contact for breaches and requests	Controller: [name, role, e-mail, telephone] Processor: nexzos@tresbizz.com, marked "data protection", [telephone]

Annex 2. Sub-processors and processing locations

Personal Data is processed at the following locations and by the following Sub-processors. All are established in, and process within, the European Economic Area.

Sub-processor	Service	Location of processing	Established
[E-mail and document hosting provider]	Business e-mail, storage of exports and reports for the duration of the assignment	[EU member state]	[country]
[Calendar and booking provider]	Scheduling of calls and demos; business contact details only	[EU member state]	[country]
[Remote support tooling]	Remote sessions during a pilot, at the Controller's request and with the user's consent per session	[EU member state]	[country]

Freelance specialists engaged by the Processor work under the Processor's own confidentiality undertaking and access controls and are not Sub-processors in their own right; they act as persons authorised under Article 4.

Annex 3. Technical and organisational measures

Area	Measure
Access control	Named accounts only, multi-factor authentication on all systems holding Controller data, access granted per assignment and withdrawn at its end, review of access rights at the end of every assignment
Encryption	Data encrypted in transit (TLS 1.2 or higher) and at rest (full-disk encryption on all devices and storage holding Controller data)
Data minimisation	Exports are requested in the smallest form that answers the question; the Processor asks for device and application data first and for user identifiers only where the assignment requires them
Segregation	Data of each Controller is kept in a separate, assignment-specific location; no mixing between clients
Devices	Company-managed devices with automatic security updates, screen lock, remote wipe, and no local copies on personal devices
Retention and deletion	Working copies deleted within 30 days after the end of the assignment; deletion logged and confirmed on request; aggregated report retained as a business record without Personal Data
Logging	Access to storage holding Controller data is logged; logs retained for twelve months and available for audit under Article 11
Incident handling	Written incident procedure with a single point of contact, 48-hour notification to the Controller under Article 9, post-incident review
Staff	Confidentiality clause in every employment and freelance contract; data protection instruction at the start of every assignment
Business continuity	Backups of assignment data within the EEA, encrypted, tested for restore, deleted on the same schedule as the primary copy

Area	Measure
Product	NEXZOS itself is built GDPR-by-design: centrally vetted code, with data and administration inside the jurisdiction the Controller chooses. What that means concretely is set out in the technical note that accompanies every pilot

ISO 27001: a certification programme is in preparation and not yet completed. The Processor states this rather than implying otherwise.