

FOR SECURITY, DATA PROTECTION AND PROCUREMENT TEAMS

Your tenant. Your data. Your control over our access.

SightPulse is deployed as an Azure Managed Application into the customer's own Azure subscription. This summary explains where data lives, who can access it, how it is protected and which documents govern it. Binding terms: Terms and Conditions, Data Processing Agreement and the customer's private offer or order.

1 WHO DOES WHAT

Entity	Role
SightPulse AG , Zug, Switzerland (UID CHE-344.951.907)	Contracting party and Microsoft Marketplace publisher. Processor of customer personal data.
CBS Systems d.o.o. , Belgrade, Serbia	Majority shareholder of SightPulse AG. Builds, operates and supports the platform as sub-processor. Commercial analytics since 2007.
Microsoft	Azure infrastructure under the customer's own Microsoft agreement; Marketplace invoicing and payment.

2 WHERE DATA LIVES AND WHO CAN ACCESS IT

Data stays in the customer tenant

Platform resources sit in a managed resource group in the customer's subscription, in the region the customer chooses. SightPulse connects to data in place (lake, lakehouse, warehouse). No copy to SightPulse or CBS systems unless the customer instructs it in writing for a defined purpose. Where the order selects it, processing outside the tenant runs in a dedicated EU Processing Environment on servers in Germany (quoted separately). Data from customer datasets is never stored in Serbia.

Activation gate

Paid deployments process customer data only after activation under an accepted private offer. The Demo plan runs on synthetic data only.

Customer-controlled access

Standard operational access: named, role-based, limited to the managed resource group. **Just-in-time access:** no standing elevated access; each request time-limited and approved by the customer. **Both:** multi-factor authentication, control-plane operations logged in the customer's Azure Activity Log, no access outside the managed resource group.

Deletion

Deleting the managed application deletes the platform resources. Source systems are untouched. Any copies held under instruction are deleted within 30 days of contract end, with written confirmation on request.

3 SECURITY MEASURES

Commitments in the signed CBS Information Security Policy v2.0 (26 September 2026) and Annex 2 of the SightPulse DPA. CBS Systems d.o.o. is certified by TÜV NORD CERT GmbH to ISO/IEC 27001:2022 (no. 44 121 26430130) and ISO 9001:2015 (no. 44 100 26430130), both valid until 2 September 2029; scope: design, integration and maintenance of software solutions for data mining, business analysis and AI agents.

- **Least privilege:** named, trained personnel; MFA; access logged and reviewed at defined intervals
- **Segregation:** each customer's data kept separate and used only for that customer
- **Encryption** in transit and at rest; controlled management of keys and secrets
- **Data minimisation:** personal data only where a use case needs it; pseudonymised identifiers preferred
- **Secure development:** security requirements, peer review, separate dev, test and production, no production customer data in dev or test without approval; automated dependency and vulnerability scanning and an external penetration test being introduced in Q1 2027
- **Monitoring and incidents:** events logged and monitored; personal data breaches notified to the customer without undue delay and within 48 hours
- **Resilience:** backup, business continuity and disaster recovery defined, maintained and tested
- **People:** background checks as permitted by law, confidentiality undertakings, regular security training
- **Suppliers:** assessed before engagement and bound by security and data protection terms
- **Responsible disclosure:** security@sightpulse.ai

4 DATA PROTECTION AND TRANSFERS

Topic	Position
Scope	The DPA applies to all personal data processed for the customer, always including authorised users' account and activity data. Personal data in customer datasets (CRM, loyalty, CDP, respondent-level) is processed only where the private offer or order puts it in scope.
Roles	Customer = controller. SightPulse AG = processor. CBS Systems d.o.o. = sub-processor.
Contract	SightPulse DPA (Art. 28 GDPR, Art. 9 FADP) applies to every paid subscription; countersigned copy on request. 30 days' notice of sub-processor changes with a right to object. Audit rights once a year on 30 days' notice.
EU to Switzerland	Switzerland holds an EU adequacy decision; no further safeguards are needed for data reaching SightPulse AG.
Access from Serbia	Serbia has no Swiss or EU adequacy decision. The AG–CBS transfer is covered by the EU Standard Contractual Clauses (Module Three) with the FDPIC Swiss adaptations and a transfer impact assessment. Remote access counts as a transfer even when data sits in the tenant or in Germany, so the SCCs apply in both cases. Supplementary measures: data at rest only in the customer tenant or the EU Processing Environment, never in Serbia; remote access only; personal data pseudonymised by default where the use case allows, to limit identifiable data accessible remotely, direct identifiers viewed only to debug, support or resolve incidents; MFA; Activity Log and optional JIT approval in the tenant.
Individual-level data	Mainly the Pro plan (CRM, loyalty, CDP). Where records are linked across sources, the customer decides the legal basis and carries out any DPIA; SightPulse assists.
Sub-processors	CBS Systems d.o.o. (Belgrade): engineering, operations, support. Hosting provider of the EU Processing Environment (Germany), only where selected, named with address in the order. Language model provider, only where SightPulse provides the model service, named in the order. For the customer tenant, Microsoft Azure and any customer-provided model endpoint or AI service (e.g. Fabric data agents, Databricks Genie) are contracted by the customer and are not SightPulse sub-processors.

5 HOW AI IS USED

- Statistical and machine-learning models perform the analysis; language models interpret, orchestrate and explain. They do not produce the numbers.
- Every output is traceable to its source data, model and drivers, and validated before release. Inferred results are flagged.
- Every AI agent is evaluated against a defined test set before release; its accuracy is reported to the customer.
- No training on customer data for other customers; third-party AI providers may not train on it. The model endpoint is set in the order: the customer's own (e.g. Azure OpenAI) or one SightPulse provides. Models receive only the data a task needs, pseudonymised where possible.

6 DOCUMENTS AND CONTACTS

Document	Link
Terms and Conditions (incl. Marketplace and Demo plan terms)	sightpulse.ai/terms-and-conditions
Data Processing Agreement	sightpulse.ai/data-processing-agreement
Privacy Policy	sightpulse.ai/privacy-policy
Trust & Data Protection, sub-processor list	sightpulse.ai/trust
Information Security Policy · Quality Policy (CBS, signed v2.0)	sightpulse.ai/information-security-policy · sightpulse.ai/quality-policy
ISO/IEC 27001:2022 and ISO 9001:2015 certificates (TÜV NORD)	sightpulse.ai/trust (section 4)
On request	SCC copy (commercial terms redacted), TIA summary, Statement of Applicability, completed security questionnaires

Contacts Security: security@sightpulse.ai · Privacy: privacy@sightpulse.ai · Legal: legal@sightpulse.ai · Support: support@sightpulse.ai · Sales and private offers: sales@sightpulse.ai