sara
Powered by Real Time Analytics

Version	Date	Classification
2.0	**June 2026**	**Confidential**

SARA BI

Customer Trust & Security Pack

Security · Privacy · Data · Governance

Real Time Analytics LLC
realtimeanalyticsus.com · soporte@realtimeanalyticsus.com

STATEMENT OF CONFIDENCE

SARA BI is a business intelligence platform that accesses, processes, and analyzes critical information from our clients' ERP. This document describes precisely **how we protect your data**, who is involved in the process, what information leaves the customer's environment, how data is isolated between organizations, and what the control, auditing, and contractual liability mechanisms are that govern our operation.

> ✦ **SARA BI's core commitment**
> Your corporate data is never shared with third parties, is not used to train external AI models, and always remains under the customer's control. This document is binding and forms part of the service agreement.

1. ARCHITECTURE MAP AND DATA FLOW

1.1 Data processing chain

When a user performs a query in SARA BI, the data flow follows the following sequential chain:

Step	Component	What happens to the data
01	**User Browser (HTTPS)**	The query travels encrypted with TLS 1.3 from the browser to the SARA BI servers. Never in plain text.
02	**SARA BI App**	The user's identity, role, and organization are validated. Only data from the active tenant is processed.
03	**SARA BI Database**	The context of the organization is retrieved: SAP connection, prompts, history. The context of each company is logically isolated.
04	**SAP Business One Service Layer**	SARA BI performs read-only queries to the customer's ERP (GET). You don't write, modify, or delete data in SAP.
05	**Azure OpenAI (AI processing)**	Only data relevant to the current query is sent to the model. They are not stored on Azure OpenAI servers. See section 1.3.
06	**Response to User**	The result returns encrypted to the browser. Data is never caught on the client side.

1.2 What data comes out of the customer's environment?

This is one of the most critical points for our customers. The following table specifies exactly what information leaves the customer's ERP and for what purpose:

Data type	Leaves the customer	Destination and purpose
SAP financial and transactional data (invoices, payments, inventory, etc.)	Yes — on request	SARA BI (RTA/Azure) servers. Only the fields are required to answer the active query.
SAP credentials (username, password)	**They never come out**	They are stored encrypted in the SARA BI DB. They are never exposed in logs, interfaces, or AI calls.
Data Fragment for AI Processing	Yes — temporary	Azure OpenAI (active query only). They are not retained on OpenAI post-processing servers.
Conversation history	**They do not leave the SARA BI environment**	They are stored in the SARA BI DB under the same security policy.
Access and audit logs	**They don't come out**	They remain in the RTA infrastructure and are available for customer auditing.
Personal data of users (name, email, role)	**They don't come out**	Only for internal access management within SARA BI.

1.3 Specific flow to the AI model

Since the AI model is the most sensitive component, we detail how it works precisely:

- A dynamic System Prompt is constructed for each query that includes only the context of the active organization (name, SAP data schema, configured tables).
- Only the data fields relevant to the user's question are included in the payload sent to Azure OpenAI.
- Azure OpenAI processes the request and returns the response. The data is not stored on Microsoft/Azure servers after the response is processed.
- The model used is GPT-5.2-chat deployed on the Azure OpenAI infrastructure within the Azure service agreement that includes enterprise data privacy guarantees.
- No data from SARA BI is used to train, fine-tune, or improve third-party AI models.

> ⚠ **Important**
> Data is sent to the AI model with explicit organizational context instructions that prevent the model from mixing data between tenants, even if prompt manipulation is attempted.
>
> The data in multi-company and/or subsidiary environments that are integrated into Sara BI maintain governance between companies, preventing data from one or the other from being mixed and can be viewed by roles that are not assigned their visualization.

2. SUB-PROCESSORS AND INFRASTRUCTURE PROVIDERS

Below, all the suppliers and sub-processors involved in the operation of SARA BI are identified, with their role, location, and relevant certifications:

Role at SARA BI	Data Location	Certifications / Warranties
Main hosting of the SARA BI application	USA	Managed environment in Microsoft Azure, which provides: □ ISO 27001 □ SOC 2
Primary database — stores organization data, configurations, and history	USA (same)	Managed environment in Microsoft Azure, which provides: □ ISO 27001 □ SOC 2
Natural Language Processing and Conversational AI	US (Azure region configured)	Azure OpenAI under Microsoft Data Processing Agreement. The data is not used for model training.
Customer ERP — SARA BI connects via Service Layer (read)	At the customer's premises or their SAP cloud provider	Read only. No writing or modification.
Primary Responsible for Platform, Technical Support, Governance and Compliance	USA	Data controller under service contract.
Technical facilitator of the SAP connection and initial onboarding. No continuous access to production data.	Variable (depending on partner region)	Contractually bound by RTA's confidentiality policies.

3. SECURITY ARCHITECTURE — DEFENSE-IN-DEPTH

3.1 Layered Security Model

#	Layer	Description and technology	Status
L1	**Network and transport**	HTTPS/TLS 1.3 required. HTTP connections are automatically redirected. No data travels in plain text.	**Active**
L2	**Authentication**	NextAuth.js with signed JWT (NEXTAUTH_SECRET). Crypts with cost factor 10 for passwords. Email verification required.	**Active**
L3	**Single Session**	Each login generates a session Token UUID v4. If the user logs in from another device, the previous session is automatically invalidated.	**Active**
L4	**Access Control (RBAC)**	5 roles with granular permissions: superadmin, admin, analyst, viewer, support agent. Each API validates role and organization before responding.	**Active**
L5	**Multi-tenant isolation**	Every organization has its own data space. The organization is validated on each query. A user in Company A can never view data from Company B.	**Active**
L6	**Data protection at rest**	Data in PostgreSQL with SSL. SAP credentials are encrypted in the database. Passwords are hashed. SAP credentials never appear in logs.	**Active**
L7	**AI Context Security**	The System Prompt is built dynamically by the organization. Explicit guidance to prevent data mixing between tenants.	**Active**
L8	**SAP Access Control**	Only admin roles can create or modify SAP connections. SAP passwords are masked in all API responses.	**Active**

3.2 Password and Credential Management

- Applies to accounts with native SARA BI authentication (without SSO). When the customer uses an external IdP, that IdP's password policy takes precedence over that of SARA BI.

Password Requirement	Policy Detail	Reference Standard	Status
Minimum length	12 characters minimum (recommended: 16+). Passphrases of 4+ random words are accepted and promoted.	*NIST SP 800-63B*	**Active**
Complexity	It must contain at least: 1 uppercase, 1 lowercase, 1 digit, and 1 special character (!, @, #, $, %, ^, &, *, etc.).	*CIS Controls v8*	**Active**
Prohibited characters	The use of the username, company name, or obvious sequences (12345678, aaaabbbb, qwerty) is rejected.	*NIST SP 800-63B §5.1.1*	**Active**
Hashing algorithm	crypts with cost factor 10. Passwords are never stored in plain text or passed on in API responses.	*OWASP Password Storage Cheat Sheet*	**Active**
Expiration	No periodic forced rotation (aligned with NIST 2024). The password is only forced to change upon evidence of compromise or request from the administrator.	*NIST SP 800-63B §5.1.1*	**Active**
Account Lock	Temporary block after 5 consecutive failed attempts. Unlocking by admin or by reset link sent to verified email.	*OWASP Authentication Cheat Sheet*	**Active**
Email verification	Applies only to accounts with native authentication (no SSO). Every new user must verify their email before they can log in. SARA BI sends an email with a one-time verification link that expires in 24 hours. Without verification completed, the account remains inactive.	*OWASP Authentication Cheat Sheet*	**Active**
Email password recovery (token)	Applies only to accounts with native authentication (no SSO). The user requests the reset from the login screen. SARA BI sends a one-time recovery token (UUID v4) embedded in a secure link to the verified email. The token expires in 24 hours and is invalidated immediately after use. No clues are revealed as to whether the mail exists in the system (protection against user enumeration).	*OWASP Forgot Password Cheat Sheet*	**Active**

SARA BI supports the full delegation of authentication to the customer's corporate identity provider. This means that users can log in to SARA BI using the same credentials and security flow that they use for the rest of their business applications, including the MFA controls already established by the customer's IT team.

3.3 Multi-tenant isolation — technical details

- Model: Shared Database, Separate Schema approach.
- Each query to the database must include the organization filter before returning any data.
- AI context is built exclusively with data from the active tenant. There is no cross-memory between organizations.
- User limits per organization (maxUsers) are enforced in real-time.
- SAP connections are tied exclusively to the organization that sets them up.

4. DATA STORAGE, RETENTION, AND DELETION

4.1 Where data is stored

Data type	Storage Location	Applied protection
Data imported from SAP	PostgreSQL in Abacus.AI Cloud (US)	SSL in connection. Isolation by organization. Vendor disk encryption.
SAP Connection Credentials	PostgreSQL (encrypted field)	Encryption at rest. Never exposed in logs or API responses.
AI conversation history	PostgreSQL under the same SARA BI DB	Restricted access to the corresponding tenant. Available for export by customer.
Organization settings (prompts, colors, automations)	PostgreSQL	Isolated by organization.
Data processed by the AI model (during the query)	Azure OpenAI server RAM (processing only)	It does not persist. It is discarded at the end of the answer.
Access and operations logs	Infrastructure: Abacus.AI / SARA BI	Available for audit. Retention according to the provider's log policy.

4.2 Retention periods

Data type	Retention period	Action at maturity
Business data imported from SAP	During the term of the contract	Secure disposal within 30 days of contract termination

AI conversation history	During the term of the contract	Secure disposal within 30 days of contract termination
Data processed by AI model (Azure OpenAI)	Zero — not retained	Discarded upon completion of the answer
Audit and access logs	12 months	Archiving or deletion according to current policy
User accounts	During the term of the contract	Immediate deactivation upon revoking access; 30-day removal
Database backups	Configurable retention (minimum 7 days)	Automatic rotation. Daily backups.

4.3 Backups and Recovery

- Automatic daily database backups with configurable retention.
- Backups are stored on the same secure Abacus.AI Cloud infrastructure.
- Each organization's data is completely segregated even in backups.
- Disaster Recovery Plan (RTO/RPO) available upon request.

5. ACCESS CONTROL, ROLES, AND PERMISSIONS

5.1 System Role Matrix

Role	Level	Access to routes	Key Capabilities	Key Restrictions
Superadmin	Platform	/superadmin/*	Management of all organizations, licenses, and global settings	Only accessible to RTA equipment
admin	Organization	/dashboard/*	Management of users of your org., SAP connections, configuration, automations	You can't see data from other organizations
Analyst	Organization	/dashboard/*	BI Query, Reports, Documents	Cannot manage SAP users or connections

viewer	Organization	/dashboard/*	Read-only dashboards and reports	No free consultation capacity or documents
support agent	Support	/superadmin/support/*	Support ticket handling	Tickets only; No access to business data

No self-registration
New user registration is disabled in SARA BI. Only organization admins can create accounts by invitation with a one-time link (expires in 24 hours). This eliminates the unauthorized access vector by open registration.

6. MONITORING, AUDITING, AND INCIDENT MANAGEMENT

6.1 Continuous monitoring

- 24/7 monitoring of availability and infrastructure through Abacus.AI Cloud.
- Detection of anomalies in access patterns and query behavior.
- Automatic alerts for unauthorized access attempts or unusual behavior.
- Audit logs of all operations: user creation, access, configuration changes, SAP connections.
- Limit control of concurrent connections to the database (maximum 25 concurrent connections) to prevent resource exhaustion attacks.

6.2 Customer Traceability and Auditing

As a SARA BI customer, you have the right to request the following audit trails:

Registration Available	Contents
Access to the platform	Date, time, user, source IP, and result of each login
Queries made on SAP data	Which SAP endpoints were queried and at what time
Configuration changes	Modifications to roles, users, SAP connections, and automations
AI conversation history	Complete record of queries and responses by user and date
Failed Login attempts	Failed authentication attempts with source IP

Data Operations	Data imports, exports, and deletions

6.3 Security Incident Management Protocol

Phase	Activity	Maximum Time	Responsible and action
Detection	Incident identification	**Continuous monitoring**	Automatic system + RTA equipment
Containment	Isolation of the affected component	**< 2 hours (critical)**	RTA technical team — immediate activation
Notification	Communication to affected customers	**< 72 hours**	RTA notifies the organization's admin by email and phone
Research	Forensic analysis of scope and cause	**< 5 business days**	RTA with infrastructure provider support
Remediation	Implementation of corrective measures	**According to severity**	RTA — documented action plan
Final Report	Detailed customer report	**< 10 business days**	RTA delivers report with cause, impact and measures taken

7. CORPORATE DATA POLICY

7.1 Data collected by SARA BI

Category	Description	Source
Business data	Sales, inventory, finance, customers, purchasing — from SAP B1 and connected sources	SAP Business One Service Layer (read-only)
User Data	Name, email, and role for access management	Created by the organization administrator
Usage Data	Queries made and session history for service improvement	Generated by interaction with the platform

> ⚠ **Sensitive data**
> SARA BI does not collect sensitive personal data (biometrics, medical, sexual orientation, religion or political affiliation) unless it is explicitly part of the business data set up by the client at its own risk.

7.2 Customer rights over their data

Law	Description	How to exercise it
Access	Request a copy of all the data stored for your organization	Contact soporte@realtimeanalyticsus.com
Rectification	Request correction of incorrect data	Contact soporte@realtimeanalyticsus.com
Elimination	Request total data deletion at any time	Contact soporte@realtimeanalyticsus.com
Portability	Export data in standard formats (CSV, JSON)	Features available on the dashboard
Audit	Request access and operations report on your data	Contact soporte@realtimeanalyticsus.com
Suspension of service	Request immediate deactivation of your organization	Contact soporte@realtimeanalyticsus.com

8. RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE

8.1 SARA BI AI Principles

SARA BI uses advanced artificial intelligence models to analyze business data. The following principles govern the design, operation, and evolution of the AI component of the platform.

Principle	How we apply it at SARA BI
🔍 **Transparency**	SARA BI always identifies when a response is generated by AI. The user can request the data sources and context used in any analysis.
🔒 **Privacy**	The data is not used to train external models. Queries are protected under the same corporate data policy and are not retained on Azure OpenAI post-processing servers.

Principle	How we apply it at SARA BI
🏢 **Insulation**	The AI context is built by organizations. There is no shared memory between tenants. A user in Company A can never get data from Company B through the model.
⚖️ **Bias Management**	SARA BI operates exclusively on client data in the United States. However, we recognize that biases can emerge from the business data itself. That's why we apply the following controls: – Source transparency: Each response in the model can be audited against the SAP data that originated it, allowing the user to detect inconsistencies. – No implicit optimization: The model has no hidden business objectives. Respond to the user's query without biasing results towards any supplier, customer or product. – Stated limitation: SARA BI explicitly warns that predictive analytics are estimates based on historical data, not guaranteed predictions. – Mandatory human review: Strategic decisions based on AI analysis must be validated by the responsible user before being executed. **Roadmap:** *RTA is developing a statistical anomaly detection module in the input data that will alert the user when the data distribution presents unusual patterns that may affect the quality of the analysis.*
👤 **Liability**	Business decisions are the responsibility of the user. SARA BI is a support tool, not a substitute for business judgment. RTA assumes no responsibility for decisions made solely based on AI analysis without human validation.
🚫 **No modification**	SARA BI only reads data from SAP. By default, you cannot create, modify, or delete records in the customer's ERP. Writing functions require explicit enablement and additional SAP permissions.

✦ **Assurance on the AI model**
Your organization's data is not used to train, fine-tuning, or improve any third-party AI models. This is contractually guaranteed in the service agreement with Azure OpenAI.

9. RESPONSIBILITIES AND GOVERNANCE

9.1 Matrix of responsibilities

Activity / Responsibility	RTA	Channel / Partner	Client
Security of the SARA BI platform	**Main**	None	None
End-user password management	Policy and tools	Initial Support	Responsible
Customer's SAP Server Security	None	N2 Support	Responsible
SAP Connection Configuration	Configuration in SARA BI	Network/firewall configuration	Approval
User management in SARA BI	Tools & Support	Onboarding support	Manager (admin)
Data quality and veracity in SAP	None	None	Responsible
Security Incident Notification	Main (< 72 hrs)	Collaboration	Informed
Auditing and access reporting	Provides tools	None	You can request
Customer's local regulatory compliance	None	None	Responsible

10. OFFICIAL CONTACT AND ESCALATION CHANNELS

Type of request	Main channel	Response Time
General Technical Support	soporte@realtimeanalyticsus.com	< 24 business hours
Exercising data rights (access, deletion, portability)	soporte@realtimeanalyticsus.com	< 5 business days
Security Vulnerability Report	seguridad@realtimeanalyticsus.com	< 24 hours
Critical Security Incidents	seguridad@realtimeanalyticsus.com + direct call	< 2 hours
Commercial and contractual consultations	ventas@realtimeanalyticsus.com	< 48 business hours
Platform Support Ticket	'Support' button in the SARA BI dashboard	According to the SLA of the contract

Corporate website and documentation	realtimeanalyticsus.com	Available 24/7

11. DECLARATION OF COMPLIANCE AND VALIDITY

This document has been prepared by Real Time Analytics LLC (RTA) and accurately describes the security, data processing, and governance controls that apply to the SARA BI platform in its current production version.

Document version	Last Updated	Next Review
2.0	June 2026	June 2027

✦ **Living document**
This document is reviewed and updated at least once a year, or whenever a significant change occurs in SARA BI's architecture, suppliers, certifications or data processing policies. The current version is always available to customers upon request to soporte@realtimeanalyticsus.com.