

BLITZSUPPORT SECURITY POLICY

Last updated: February 2026

You are here because security matters to you. We understand you need to be confident that your service providers take security as seriously as you do. Below, you will find information on how we ensure the safety of your data in BlitzSupport.

1. Our Team

We keep operational access intentionally limited and controlled.

- **Restricted production access**
Access to production systems and customer data is limited to a small number of designated administrators.
- **Least privilege**
Access is granted only when required and only to the minimum scope needed to operate and support the service.
- **Strong authentication**
Administrative access is protected using strong authentication, including multi-factor authentication where available.
- **Access logging**
Administrative access to production systems is logged to support traceability and review.
- **Secure work environment**
Production access is performed only from trusted personal work devices that use full-disk encryption, password protection, and automatic screen locking.
- **Operational security practices**
We follow practical security best practices such as using password managers, unique credentials, and keeping systems up to date.
- **Future access control**
Before any employee or contractor is granted production access, they must be contractually bound by confidentiality and appropriate security obligations.

2. Infrastructure and Hosting

BlitzSupport runs on Microsoft Azure in the Germany West Central (Frankfurt) region.

We rely on Azure's built-in security controls and apply the following measures:

- Infrastructure access is limited to authorized administrators.
- The primary database is Azure SQL Database with Transparent Data Encryption (TDE).
- Files and attachments are stored in Azure Storage with encryption at rest (AES-256).
- Infrastructure is configured within the European Union to support data residency.
- Cloud resources are configured to minimize unnecessary exposure.
- Regular automated backups are performed and stored securely within the EU.
- Restore procedures are documented and tested periodically where feasible.

Microsoft publishes independent security and compliance documentation for Azure, which forms part of our infrastructure security assurance.

3. Network and Application Security

Security is built into the platform architecture and development process.

- All external connections use TLS 1.2 or higher.
- Internal service communication uses encrypted connections where applicable.
- HTTP Strict Transport Security (HSTS) is enabled.
- We follow secure development practices to reduce common web risks such as:
 - Cross-site scripting (XSS)
 - SQL injection
 - Cross-site request forgery (CSRF)
- Administrative functions require authenticated access.
- The application supports role-based access controls for customer workspaces.

4. AI Processing Security

BlitzSupport includes AI features that interact with external language model services.

- Data sent to AI services is encrypted in transit using HTTPS.
- Requests to AI providers are authenticated and limited to service functionality.
- We select providers and configurations intended to limit the use of customer data to processing the requested functionality.
- AI features can only be used by authenticated users within a workspace.
- We log security-relevant AI feature usage events (for example feature invocation metadata) for operational visibility.

5. Monitoring and Logging

We maintain operational visibility into system activity.

- Security-relevant events such as authentication and administrative actions are logged.
- Logs are stored securely within our cloud environment.
- Logs are reviewed as part of operational activities to identify potential issues.
- We investigate and respond to suspicious or unexpected behavior when detected.

6. Backup and Recovery

We protect customer data against loss and service disruption.

- Regular automated backups of customer data are performed.
- Backups are encrypted and stored within the European Union.

Blitz Support

- Documented restore procedures are maintained.
- Our architecture and recovery approach are designed to minimize downtime in the event of a major incident.

7. Data Processing Agreement

We provide a Data Processing Agreement (DPA) that governs how personal data is handled on behalf of customers. The DPA is available alongside our compliance documentation.

8. Incident Response

If a security incident occurs:

- We take immediate steps to contain and resolve the issue.
- Affected customers are notified without undue delay in accordance with our DPA and applicable law.
- We review incidents internally to identify root causes and improve our controls.

9. Questions

If you have questions about our security practices, please contact:

Email: support@aigonomic.com

Company: aiGonomic GmbH, Ghersburgstraße 4I, 83043 Bad Aibling, Germany