BELINNOV SOLUTIONS

DE EN

TRUST & COMPLIANCE

# Built on security, privacy and responsible delivery.

Belinnov combines structured information-security practices, privacy-aware engineering, contractual safeguards and independently assessed standards to help protect customer data, intellectual property and business-critical systems throughout the delivery lifecycle.

Talk to Our Team

Download Trust Overview



### ISO 27001:2022 Certified

Information-security practices supported by an independently assessed management framework.

### Privacy & GDPR Ready

Processes designed to support privacy-aware and GDPR-aligned customer engagements.

### Client IP & Confidentiality

Contractual and operational safeguards for customer source code, documentation, data and proprietary information.

### Global Delivery with Strong Safeguards

Structured controls designed to support secure collaboration across locations and delivery teams.

BELINNOV SOLUTIONS

DE EN

# 1. Data Protection & GDPR Readiness

We incorporate privacy-by-design principles and appropriate technical and organisational measures to support the protection of personal data in line with applicable data-protection requirements.

### Our Role

Depending on the engagement, Belinnov may act as a controller for information collected for its own business purposes, or as a processor or sub-processor when handling personal data on behalf of a customer. The respective roles, responsibilities and processing instructions are defined through the applicable agreement.

### Lawful and Purpose-Limited Processing

Personal data is processed only for defined, legitimate and agreed purposes. Where Belinnov acts as a processor, personal data is handled according to documented customer instructions and the terms of the applicable Data Processing Agreement.

### Data-Subject Rights

Where applicable to our role, we support customers in responding to requests relating to these rights. Requests are handled in accordance with applicable legal, contractual and operational requirements.

- Access
- Correction
- Deletion
- Restriction
- Portability
- Objection

### International Data Transfers

Because Belinnov delivers from India, personal data processed for EEA-based customers may be transferred to a country outside the EEA. For such transfers, Belinnov uses the EU Standard Contractual Clauses (SCCs) as its standard transfer mechanism, supported by appropriate technical and organisational measures and any engagement-specific data-protection obligations.

BELINNOV SOLUTIONS

DE EN

In practice, Belinnov already delivers for an EU-based customer under a GDPR-aligned Master Services Agreement, with EU Standard Contractual Clauses in

### Data Hosting and Residency

Where a customer requires personal data to be hosted and processed within the EU, Belinnov can design the solution to use EU-region cloud infrastructure. Default hosting arrangements and data residency are agreed for each engagement.

### Data Retention and Deletion

Personal data is retained only for as long as required for the agreed purpose, applicable legal obligations or legitimate operational requirements. At the end of the applicable retention period, information is returned, anonymised or securely deleted in accordance with contractual and legal requirements.

### Data Processing Agreements

Belinnov can enter into an appropriate Data Processing Agreement covering areas such as:

- Nature and purpose of processing
- Categories of personal data
- Security and confidentiality measures
- Sub-processor requirements
- Incident notification
- Assistance with data-subject requests
- Return or deletion of information
- Audit and assurance provisions, where agreed

BELINNOV SOLUTIONS

DE EN

# 2. Client Intellectual Property & Confidentiality

We recognise that customer source code, product knowledge, business processes, technical documentation, datasets and commercial information are critical business assets. Our approach is designed to protect these assets throughout the engagement lifecycle.

### Confidentiality by Contract

Customer engagements can be governed by appropriate confidentiality agreements, non-disclosure agreements and contractual confidentiality obligations. Employees, contractors and authorised delivery partners are expected to comply with the confidentiality requirements applicable to their work.

### Client IP and Deliverable Ownership

Ownership and permitted use of project deliverables are clearly defined in the applicable agreement. Customer-specific source code, designs, documentation, configurations and other deliverables are assigned or licensed according to the agreed commercial terms. Pre-existing tools, frameworks, reusable components or third-party materials are identified and treated separately where applicable.

### Controlled Access

Access to customer repositories, cloud environments, technical documentation, credentials and business information is limited to authorised team members based on their delivery responsibilities. Access can be reviewed, restricted or removed when:

- Responsibilities change

### No Unauthorised Reuse or Disclosure

Customer-specific source code, business logic, designs, documents, datasets and proprietary knowledge are not reused for another customer or disclosed to an unauthorised third party. Any permitted use is governed by the applicable customer agreement.

- A team member leaves the engagement
- Access is no longer operationally required
- The customer requests a change
- The engagement concludes



### Secure Handling Throughout Delivery

Confidential information is considered across development, testing, deployment, maintenance and production-support activities. Depending on the engagement, controls may include:

- Approved source-code repositories
- Role-based access
- Multi-factor authentication
- Secure credential handling
- Environment separation
- Restricted production access
- Controlled document sharing
- Access logging and review
- Secure communication channels



### Return, Retention and Secure Disposal

At the end of an engagement, customer information, credentials and access are handled in accordance with agreed contractual requirements. Materials may be:

- Returned to the customer
- Retained for an agreed period
- Archived where legally or contractually necessary
- Securely deleted when no longer required



**AI Tools, Client Data and Intellectual Property:** Customer source code, documents, datasets, credentials or confidential information are not submitted to public AI tools or used for model training without appropriate customer authorisation and agreed safeguards. Where AI-assisted tools are used, their use can be governed by customer requirements relating to:

- Approved tools and platforms
- Information classification
- Data retention
- Model-training restrictions
- Hosting location
- Human review
- Intellectual-property protection
- Confidentiality obligations

# 3. Information Security Practices

Belinnov maintains information-security practices designed to protect the confidentiality, integrity and availability of customer and business information. Depending on the engagement, these measures may include:

- **Access Control:** Role-based access, least-privilege principles, access approval and review, multi-factor authentication where supported, and timely access revocation.
- **Secure Engineering:** Secure software-development practices, source-code review, dependency and vulnerability management, separation of development, testing and production environments, and controlled deployment practices.
- **Data and Infrastructure Protection:** Encryption in transit, encryption at rest where supported, secure cloud configuration, backup and recovery practices, and business-continuity considerations.
- **Monitoring and Incident Management:** Logging and monitoring, security-event review, incident escalation procedures, root-cause analysis where applicable, and corrective and preventive actions.
- **People and Awareness:** Confidentiality obligations, security-awareness practices, role-appropriate access, customer-specific security instructions, and clear responsibility and escalation channels.

# 4. Responsible Use of AI

Belinnov uses AI thoughtfully to improve engineering, automation and operational outcomes while protecting customer information and intellectual property.

### OUR PRINCIPLES

- **Agreed Purpose:** AI is used only for clearly defined and agreed business or delivery purposes.
- **Customer Data Protection:** Customer information is not automatically submitted to public AI tools or external models.
- **Tool and Model Selection:** Model, hosting and integration choices are assessed based on the sensitivity of the information and the requirements of the engagement.
- **Human Oversight:** Appropriate human review is retained for AI-assisted outputs, decisions and workflows.
- **Transparency:** Customers can be informed where AI tools materially contribute to an agreed solution or delivery process.
- **Contractual Clarity:** Data use, retention, training restrictions, ownership and confidentiality requirements can be defined contractually.
- **Responsible Engineering:** AI-generated code, content or recommendations are subject to appropriate technical review before use in customer deliverables.

# 5. Certifications & Standards

Our quality, service-management and information-security practices are supported by independently assessed standards and structured process frameworks.

ISO 27001:2022

### ISO 27001:2022

Information Security Management System

ISO 9001:2015

### ISO 9001:2015

Quality Management System

### ISO 14001:2015

Environmental Management System

ISO 20000-1:2018

### ISO 20000-1:2018

IT Service Management System

CMMI level 3

### CMMI Development – Maturity Level 3

Structured and defined software-development processes

Certificates and relevant supporting documentation can be shared with prospective customers where appropriate.



# 6. Contractual & Delivery Safeguards

Security, confidentiality and compliance requirements are most effective when defined for the specific engagement. Belinnov works with customers to identify relevant requirements during commercial, technical and delivery discussions.

### Early Security Review

Relevant customer security, privacy, hosting and compliance expectations are identified during discovery and project initiation.

### Appropriate Agreements

Depending on the engagement, documentation may include:

- Master Services Agreement
- Statement of Work
- Non-Disclosure Agreement
- Data Processing Agreement
- Intellectual-property provisions
- Information-security obligations
- Service-level requirements

### Sub-Processor and Third-Party Transparency

Third-party services, cloud platforms and sub-processors relevant to customer-data processing can be identified and reviewed where applicable.

### Incident Notification

Incident-reporting and notification responsibilities are defined according to applicable agreements and legal requirements.

### Transparent Communication

Customers receive defined delivery, governance and escalation channels appropriate to the engagement.

DE EN

### Engagement Closure

Access revocation, information return, knowledge transfer and secure disposal requirements are addressed during engagement closure.

## Do you have specific security or compliance requirements?

We are happy to discuss your data-protection, confidentiality, intellectual-property and information-security expectations and determine appropriate safeguards for your engagement.

Discuss Your Requirements

Contact Belinnov

---

### Important Disclaimer

The information presented on this page describes Belinnov's general approach to security, privacy and responsible delivery. Specific controls, responsibilities and contractual commitments depend on the nature, scope and requirements of each engagement.

Nothing on this page should be interpreted as legal advice, an unconditional guarantee of compliance or a representation that every regulatory requirement applies identically to every customer, system or engagement.

BELINNOV SOLUTIONS

DE EN

Founder-led product-engineering and technology-services company established in 2015, delivering software, cloud, data, applied-AI and commerce solutions for global clients.

**Belinnov Solutions Private Limited**

## CAPABILITIES

- Product Engineering
- Cloud & DevOps Platforms
- Data & AI Systems
- Commerce & Transaction Platforms

## COMPANY

- Company
- Company Facts
- Engineering Philosophy

Certifications

Trust & Compliance

Germany / Mittelstand

Careers

DE EN

## CONNECT

Start a Strategic Conversation

Contact Us

## CERTIFICATIONS

ISO 9001 · ISO 14001 · ISO 20000

ISO 27001 · ISO 45001

Startup India Recognition

Microsoft Azure AWS .NET Next.js Secure by Design

© 2026 Belinnov Solutions Private Limited. All rights reserved. Privacy Policy