inbenta™
(https://www.inbenta.com)

COMPLIANCE

Security and Privacy

Technical and Organizational Measures (TOMs)

Overview

At Inbenta, we are committed to safeguarding your data and the personal information of your users. Our technology, infrastructure and processes are continuously being monitored and improved with security being the main focus. We are certified by third-party specialists in Information and Cloud Security and Privacy Information.

Security Partnership	Cloud & network security
Application Security	Product security features
Certifications & memberships	Supplier Relationships
Additional security methodologies	Privacy and PII

Security Partnership

Inbenta has a partnership with Ackcent Cybersecurity (https://ackcent.com/), in order to perform scheduled product and code audits, security audits and penetration testing, and to handle all SOC/SIEM, Intrusion Detection and Prevention.

Cloud & network security

PHYSICAL SECURITY

Physical Security

Inbenta runs on top of AWS in various regions. The supporting infrastructure and systems are hosted at AWS facilities; as a result, physical security controls, on-site security, and Monitoring of the Datacenters are the responsibility of AWS. Application security and Privacy out of AWS scope and the shared responsibility model is handled by Inbenta and covered by being compliant with GDPR, ISO9001, ISO27001 and ISO27017.https://aws.amazon.com/compliance/data-center/controls/ (https://aws.amazon.com/compliance/data-center/controls/)
https://aws.amazon.com/security/ (https://aws.amazon.com/security/)

- ISO 27002 & ISO 27017 controls: A.11.1

NETWORK SECURITY

Dedicated Security Team and SIEM

Our security monitors and alarms (active/passive systems) as well as our external SIEM security partner are fully integrated into our operations, providing 24×7 security and security teams ready to respond to alerts and events.

- ISO 27002 & ISO 27017 controls: A.12.4.1, A.13.1.2, A.16.1.1, CLD.12.4.5

Protection

Our network is protected and isolated by firewalls, NACL (network access control list), secure HTTPS transport over public networks, DMZ monitorization, regular audits, and network Intrusion Detection and/or Prevention technologies (IDS/IPS) which monitor and/or block malicious traffic and network attacks, DDoS active protection and DNS spoofing monitoring.

- ISO 27002 & ISO 27017 controls: A.13.1.1, A.13.1.2, A.13.1.3

Protection

Our network is protected and isolated by firewalls, NACL (network access control list), secure HTTPS transport over public networks, DMZ monitorization, regular audits, and network Intrusion Detection and/or Prevention technologies (IDS/IPS) which monitor and/or block malicious traffic and network attacks, DDoS active protection and DNS spoofing monitoring.

- ISO 27002 & ISO 27017 controls: A.13.1.1, A.13.1.2, A.13.1.3

Architecture

Our network security architecture consists of multiple zones. More sensitive systems, like databases, cache, and NFS servers, are protected in our most private zones fully isolated. Other systems are housed in mid-private zones like webhook processors in private subnets behind an egress-only NAT. Depending on the zone, additional security monitoring and access controls will apply. DMZs are utilized between the Internet or public subnets (Load Balancers only), and internally between the different zones of trust.

- ISO 27002 & ISO 27017 controls: A.13.1.1, A.13.1.3

Firewalls

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

- ISO 27002 & ISO 27017 controls: A.13.1.1, A.13.1.3

Network Vulnerability Scanning

Network security active scanning is actively running on all subnets across all regions for quick identification of out-of-compliance or potentially vulnerable systems. Scheduled passive scans are also executed for all internal or private subnets as well as all DMZ or public subnet facing exposed ports (http/https).

- ISO 27002 & ISO 27017 controls: A.12.6.1, A.12.7.1

Third-Party Penetration Tests

In addition to our extensive internal scanning and testing program, each year Inbenta employs third-party partners (Ackcent Cybersecurity) to perform a broad penetration test across the Inbenta private and public Production Networks, as well as perform products audits on all products on a per quarter basis.

- ISO 27002 & ISO 27017 controls: A.12.6.1, A.12.7.1, A.14.2.8

Security Incident Event Management (SIEM)

Our Security Incident Event Management (SIEM) system gathers extensive logs from important network devices and host systems. The SIEM sends alerts on triggers that notify the Security team based on the correlated events for further investigation and response.

Intrusion Detection and Prevention

Application data flow ingress and egress points are monitored with Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS). This is integrated with SIEM and 24/7 operations.

- ISO 27002 & ISO 27017 controls: A.12.4.1, A.13.1.1

DDoS Mitigation

Inbenta uses real-time network flow monitoring to inspect incoming traffic in all HTTP entry points such as CDN https terminations, https load balancer listeners and all secure WebSockets terminations (wss://) in order to perform automated mitigation of most DDoS techniques on layer 7 (WAF), and protect against all known infrastructure (Layer 3 and 4) attacks.

- ISO 27002 & ISO 27017 controls: A.13.1.1

Logical Access

Inbenta uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Production resources and all administrative actions are recorded and stored for at least 2 years with an immutable checksum in order to prevent audit logs from being modified.
All production resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role. Access to any Inbenta Production administration network or subsystem is restricted by an explicit need-to-know basis as controlled by the ISO27001 and 27017 controls. All is controlled and monitored by our Operations Team with granular and specific roles per employee. Employees accessing the Inbenta Production Network administration are required to use multiple factors of authentication, with both factors having credentials that expire with low TTLs forcing them to be rotated continuously.

- ISO 27002 & ISO 27017 controls: A.9.1, A.9.2, A.9.4

OPERATIONS SECURITY

Change Management

All changes to our operating systems are managed through our change management procedure which ensures that all changes are controlled, impact, and risks are assessed, and there is a formal approval process before they go live.

- ISO 27002 & ISO 27017 controls: A.12.1.2

In the event that the Customer needs to report a security incident to Inbenta, the appropriate channel is Inbenta Support Center (https://support.inbenta.io) or directly to privacy@inbenta.com .

In the event that Inbenta becomes aware of an incident or a major change within Inbenta's platform, affecting the security of the Customer's information, Inbenta will report to the Customer this incident or major change and its impact over the affected information.

Inbenta will share all necessary information for the Customer to alert their users and apply mitigations if possible.

Inbenta will notify the customer through email to the Customer team assigned to Inbenta, or the contacts specified in this contract (Notices section) in their absence, in no more than 48h after Inbenta is aware of the incident or major change.

Inbenta will also publish an incident or major change report in the Support Center (https://support.inbenta.io) and keep this report updated with the latest status until closure.

Capacity Management

Our Capacity Management procedure is aimed to ensure that current and future IT capacity needs are covered, to monitor and control the performance of the IT infrastructure, to develop capacity plans depending on agreed service levels, and to manage and streamline demand for IT services.

System capacity is continuously monitored and in case of a system alert, events are escalated to our 24/7 teams providing Operations, Network Engineering, and Security coverage.

- ISO 27002 & ISO 27017 controls: A.12.1.3

Control Against Malware

Malware control and prevention is performed regularly by the ISMS Team and included in security training and Code of Professional Conduct.

SOC service provided by our partner Ackcent comprises proactive services for the prevention of security incidents, including continuous cybersecurity threat monitoring, continuous monitoring and vulnerability alerts for critical digital assets, real-time monitoring, detection and analysis of incidents, and remote response to incidents based on the coordination of resources and the rapid application of security countermeasures.

- ISO 27002 & ISO 27017 controls: A.12.2.1

Security Incident Response

In case of a system alert, events are escalated to our 24/7 teams providing Operations, Network Engineering, and Security coverage. Employees are trained on security incident response processes as controlled in both ISO9001 and 27001.

- ISO 27002 & ISO 27017 controls: A.16.1

Logging and Monitoring

Our Security Incident Event Management (SIEM) system gathers extensive logs from important network devices and host systems. The SIEM sends alerts on triggers that notify the Security team based on the correlated events for further investigation and response.

- ISO 27002 & ISO 27017 controls: A.12.4.1

Hardening

Inbenta uses hardening as part of the development/deployment cycle. All production environments/images /containers are build and deployed using hardening from stable, up-to-date, and homologated images. New VM/containers/images are always created from previous base template images (containers, AMIs) within a monitored lifecycle (hardening).

Any production change in the images is previously tested in development and pre-production environments.

All base images/containers are re-build and updated on a scheduled basis.

- ISO 27002 & ISO 27017 controls: CLD.9.5.2

ENCRYPTION

Encryption in Transit

Communications between you and Inbenta servers are encrypted via industry best-practices HTTPS using Transport Layer Security (TLS 1.2 and TLS 1.3 for some terminations) protocol over public networks with the latest non-weak cipher suites. Additionally, no SSL protocols are allowed. TLS is also supported for encryption of emails. A more detailed specification can be found on the “Transmission (https://www.inbenta.com/security-and-privacy /#transmission) Security and Integrity (https://www.inbenta.com/en/security/#Transmission)” section of this document.

- ISO 27002 & ISO 27017 controls: A.13.2.3, A.14.1.2

Encryption at Rest

All Inbenta managed data, disk, filesystems, and datastores are encrypted using provider-managed key-management-systems (AWS KMS – AWS CMK) using keys managed and maintained by Inbenta and its rotation program. All data is encrypted using the industry-standard AES-256 algorithm and strongest block ciphers. Inside the AWS-KMS service Inbenta uses 2 types of managed keys:
Encryption with Customer-Provided Keys and Encryption with AWS KMS-Managed Keys.

- ISO 27002 & ISO 27017 controls: A.8.2.3, A.18.1.4

AVAILABILITY & CONTINUITY

Uptime

Inbenta maintains the Status Portal, available for logged in users, which includes system availability details, scheduled maintenance, service incident history, and relevant security events.

- ISO 27002 & ISO 27017 controls: CLD.12.4.5

Redundancy

Redundancy is built into the system infrastructure supporting production services to help ensure that there is no single point of failure, including firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.
Inbenta employs service clustering and network redundancies to eliminate single points of failure.

- ISO 27002 & ISO 27017 controls: A.17.2

Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, the operations Team performs troubleshooting to identify the root cause and then re-run the backup job immediately, if possible, or otherwise as part of the next scheduled backup job. Backup infrastructure is managed by the cloud provider and does not involve physical media handled by Inbenta personnel. The backup

infrastructure resides on long-live datastores behind private networks logically secured from other networks and is AES256 encrypted at rest using the keys management system by the cloud provider (AWS KMS) using Inbenta managed private keys rotated as per scheduled basis.
A scheduled random backup integrity check occurs weekly.
Backups occur, at minimum, every 24 hours for all production data. Depending on the type of the data classification of the backed-up storage a different periodicity is specified in 3 tiers: 1) Point in time recovery for critical data, 2) Every 12h for configuration data and 3) Every 24h for less changing and log data.

- ISO 27002 & ISO 27017 controls: A.12.3

Disaster Recovery and Business Continuity Plan

Our Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) ensure that our services remain available or are easily recoverable in the case of a disaster. This is accomplished through building a robust technical environment, and the set up of a low–value RTO and RPO, determined by
a Business Impact Analysis (BIA). Several disruptive scenarios are considered, covering situations such as personnel and provider unavailability. The Disaster Recovery simulations and tests are executed and audited annually, as required by ISO 27001 and ISO 27017.

- ISO 27002 & ISO 27017 controls: A.17.1

TIME SYNCHRONIZATION AND NTP

Network Time Protocol, clock synchronization and consistency

Inbenta uses NTP protocol and services to keep all clocks synchronized and consistent across all services, modules and OS. We use Public ntp.org (http://ntp.org/) NTP servers (per region) https://support.ntp.org/bin/view/Servers/NTPPoolServers (https://support.ntp.org/bin/view/Servers/NTPPoolServers) for components with internet access, and Amazon Time Sync Service (by AWS) for all private networks or all non-internet access modules. Amazon Time Sync Service, a time synchronization service delivered over Network Time Protocol (NTP) which uses a fleet of redundant satellite-connected and atomic clocks in each region to deliver a highly accurate reference clock.Our Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) ensure that our services remain available or are easily recoverable in the case of a disaster. This is accomplished through building a robust technical environment, and the set up of a low–value RTO and RPO, determined by

a Business Impact Analysis (BIA). Several disruptive scenarios are considered, covering situations such as personnel and provider unavailability. The Disaster Recovery simulations and tests are executed and audited annually, as required by ISO 27001 and ISO 27017.

Application security

SECURE DEVELOPMENT (SDLC)

Security Training

At least twice annually, engineers and developers participate in secure code training and security by design developing best practices, common attack vectors, and Inbenta security controls. This training is provided by internal and external training programs and training suites.

- ISO 27002 & ISO 27017 controls: A.7.2.2

OWASP Security Controls

Inbenta uses all OWASP top security known rules. These include inherent controls that reduce our exposure to Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and SQL Injection (SQLi), among others. Both in static code analysis and dynamic analysis, as well as realtime-active WAF (web application firewall) rules in front of any HTTP listener.

- ISO 27002 & ISO 27017 controls: A.14.2.4

QA

Our QA department reviews and tests our codebase. Several manual and automated tests are performed and integrated with the CI/CD pipelines in order to deploy only tested and secure code. Our QA team participates actively in the end-application security as well as the development process in the release pipeline/flow.

- ISO 27002 & ISO 27017 controls: A.14.2.1, A.14.2.8

Separate Environments

Testing, development, and staging environments for product development are separated physically and logically from the Production environment via network isolation, firewalls, and NACL. No actual production Data is used in the development or test environment, mock and random data may be generated in order to simulate high data volumes.

- ISO 27002 & ISO 27017 controls: A.12.1.4, A.14.2.6, A.14.3.1

APPLICATION VULNERABILITIES

Internal Dynamic Vulnerability Scanning

We employ a number of third-party, qualified security tools to continuously dynamically scan our applications against the OWASP rules. Additionally, all HTTP handlers have an active WAF blocking all known OWASP and known top rules in realtime.

- ISO 27002 & ISO 27017 controls: A.12.6.1, A.14.2.5

External Dynamic Vulnerability Scanning

Inbenta uses an external security partner for the external SOC-SIEM team.
The third-party partner uses industry-standard scanning technologies and a formal methodology specified by Inbenta (all OWASP rules, and many more).
These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as-needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Inbenta system are implemented through the Change Management process.

- ISO 27002 & ISO 27017 controls: A.12.5.1, A.12.6.1, A.12.7.1

Static Code Analysis

The source code repositories for Inbenta Applications, for both our WebGUI and Product APIs, are continuously scanned in the testing and review stages in the CI/CD (continuous integration) Pipelines and Flow, and they are integrated with all QA and release flows blocking any release or deployment of non-compliant or sub-standard code. Additionally, scheduled scans are triggered by our integrated static analysis tooling.

- ISO 27002 & ISO 27017 controls: A.12.6.1, A.14.2.8

Security Penetration Testing

In addition to our extensive internal scanning and testing program, each quarter Inbenta employs third-party security expert partners (external SOC-SIEM and scheduled pen-tests and audits) to perform detailed penetration tests and dynamic code analysis on different applications within our family of products.

- ISO 27002 & ISO 27017 controls: A.12.6.1, A.14.2.8

Product security features

AUTHENTICATION SECURITY

Authentication Options

For all WebGUI applications, we offer Inbenta account sign-in with 2FA or custom SSO (IdP).
For Product APIs and/or client integrations (JS SDK), we offer an authentication flow with API keys, secrets/tokens (and domain keys for JS SDK) based on JWT (JSON Web Token) to authenticate and authorize all API calls and actions with the backend.

- ISO 27002 & ISO 27017 controls: A.9.2.3, A.9.4.1, A.9.4.2, CLD.9.5.1

Single sign-on (SSO)

Single sign-on (SSO) allows you to authenticate users in your own systems without requiring them to enter additional login credentials for your Inbenta user WebGUI and instances.

Security Assertion Markup Language (SAML) is supported.

You can integrate your SSO with Inbenta, since it works as an SP (Service provider) for SAMLv2.

- ISO 27002 & ISO 27017 controls: A.9.4.2

Password Policy

Passwords can only be reset by the end-user with an active email address (username is the same email address). A temporary reset password URL can be generated by the end-user in the login page. Password policies are enforcing the latest best-known minimum requirements and additional anti-bot detection measures are enabled on all user/password management screens. Admins may also configure a password rotation policy per user.

- ISO 27002 & ISO 27017 controls: A.9.4.3

Two-factor authentication (2FA)

If you are using Inbenta sign-in on your Inbenta Support instance, you can turn on 2-factor authentication (2FA) for agents and admins, including apps like Authy and Google Authenticator for generating passcodes OOTP.
2FA provides another layer of security to your Inbenta account, making it more challenging for someone else to sign in as you. If you are using your own SSO IdP (Identity Provider) to force your users to use 2FA, you can integrate your SSO with Inbenta, since it works as an SP (Service provider) for SAMLv2.

- ISO 27002 & ISO 27017 controls: A.9.2.3, A.9.4.2

Secure Credential Storage

Inbenta follows secure credential storage best practices by never storing passwords in human-readable format, and only after a secure, salted, one-way hash over databases filesystem or no-SQL platforms with encryption at rest and all in-transit operations to the backend.

- ISO 27002 & ISO 27017 controls: A.8.2.3, A.9.2.4, A.9.4.2, A.14.1.2

API Security & Authentication

The Inbenta Product APIs are SSL-only, HTTPS full REST-API with the latest cipher suites on the HTTP listeners using TLS. You must have a verified API key and secret/token and to make any product API requests you previously need to make a mandatory call to the auth request flow on the authorization API, an additional layer for all client-side (javascript SDK) integrations are also available in order to check all Origin domain of the SDK integrations. SAML SP (Service provider) authentication is also supported for the SSO frontend of all WebGUI login access different from the APIs (application). Learn more about API security and endpoint terminations at https://developers.inbenta.io/ (https://developers.inbenta.io/)

- ISO 27002 & ISO 27017 controls: A.9.1.2, A.9.4.2, CLD.9.5.1, A.10.1.1

ADDITIONAL PRODUCT SECURITY FEATURES

Access Privileges & Roles

Access to data and products within Inbenta Workspace and CM/Chat is governed by access rights, and can be configured to define granular access privileges. Inbenta has various permission levels for users (owner, admin, agent, end-user, etc.), and a per-group roles granularity. Access to data for the API/SDK is governed by API keys, tokens and secrets as well as many Identification headers in both tiers for authentication and authorization.

- ISO 27002 & ISO 27017 controls: A.9.1.2, A.9.2.3, A.9.4.1

Product High Availability and access

Some Authorization endpoints and URLs are accessed via a CDN (content delivery network) in order to guarantee a low latency and high availability to boost content delivery based on the geographic locations of the end-user. Additionally a regional or latency-based DNS routing for the SDK integrations can be configured as described in: https://developers.inbenta.io/general/authorization/regions-and-endpoints (https://developers.inbenta.io/general/authorization/regions-and-endpoints)

- ISO 27002 & ISO 27017 controls: A.14.1.2, A.14.1.3, A.17.2.1

Private Attachments

In Inbenta Messenger, by default all instances are sandboxed and secured, all assets and attachments are private and a successful login and permission/role are required in order to view ticket attachments or messages. Additionally, all assets and attachments are stored in an encrypted data store and are served to agents with a temporary signed URL that becomes unavailable after several minutes.

- ISO 27002 & ISO 27017 controls: CLD.9.5.1, A.10.1.1, A.13.1.3

Transmissions Security and Integrity

All communications with Inbenta servers (back and forth) are encrypted using industry-standard HTTPS over public networks. This ensures that all traffic between you and Inbenta is secure during transit. A list of SSL/TLS protocols and cipher suites can be found at: Regions and Endpoints – Inbenta developers (https://developers.inbenta.io/api-resources/security/regions-and-endpoints) for all API terminations and endpoints. Additionally, for realtime features such as realtime Chat, Inbenta uses secure WebSockets protocol as a complementary secure and streaming-oriented HTTP alternative.
All SDKs are hosted in a secure and encrypted AES256 datastore and served via a CDN with WAF (cookie/headers check and audit) and all Inbenta SDK integrations use a subresource integrity (sha384 SRI).

- ISO 27002 & ISO 27017 controls: A.13.1.2, A.14.1.2, A.14.1.3

Messenger outgoing Email Signing (DKIM)

Inbenta Messenger Support offers DKIM (Domain Keys Identified Mail) for signing outbound emails from Inbenta Messenger when you have set up an outgoing response email domain on your Inbenta Messenger instance, and SMTP over SSL/TLS (port 465) and STARTTLS (port 587) for the secure sending protocols.

- ISO 27002 & ISO 27017 controls: A.13.2.3

SDK Subresource Integrity

A Subresource Integrity (SRI) check is a security feature that enables browsers to verify that the resources they fetch are delivered without unexpected manipulation. All Inbenta SDKs have this feature available.

- ISO 27002 & ISO 27017 controls: A.14.1.2, A.14.1.3

Compliance certifications and memberships

SECURITY COMPLIANCE

Auditors

AENOR, the auditor supplier, is part of the IQNet ASSOCIATION network in order to see global coverage all of its certifications (worldwide ISOs):
https://www.inbenta.com/compliance/certifications/
(https://www.inbenta.com/compliance/certifications/)http://www.iqnet-certification.com/ (http://www.iqnet-certification.com/)

- ISO 27002 & ISO 27017 controls: A.18.2.1

ISO 9001

Inbenta is ISO 9001 certified.

ISO 27001

Inbenta is ISO 27001 certified.

ISO 27017

Inbenta is ISO 27017 certified.

ISO 27001

Inbenta is ISO 27701 certified.

MEMBERSHIPS

Privacy Certification Program

We've received a certification seal signifying that our privacy statement and practices have been reviewed for compliance to industry standards viewable on their validation page.

https://privacy.truste.com/privacy-seal/validation?rid=9b207c96-c411-409e-93d3-abf615471625 (https://privacy.truste.com/privacy-seal/validation?rid=9b207c96-c411-409e-93d3-abf615471625)

- ISO 27002 & ISO 27017 controls: A.6.1.4, A.18.1.4, A.18.2.1

Data Privacy Framework

Inbenta has certified compliance with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework as set forth by the U.S. Department of Commerce.

- ISO 27002 & ISO 27017 controls: A.18.1.4, A.18.2.1

Privacy Policy

https://www.inbenta.com/compliance/privacy-policy (https://www.inbenta.com/compliance/privacy-policy/)

- ISO 27002 & ISO 27017 controls: A.18.1.4

INDUSTRY BASED COMPLIANCE

Using Inbenta in a PCI Environment

Inbenta is not PCI DSS compliant. Adding a component from a vendor that is not PCI DSS compliant on the credit card checkout page would make the entire payment process not PCI DSS compliant. The alternative is to host that script in the clients' datacenter, and secure the script using Subresource Integrity.

- ISO 27002 & ISO 27017 controls: A.18.2.2

Supplier relationships

POLICIES

Information security policy for supplier relationships

Regarding our services and infrastructure suppliers, we hold a policy of dynamic risk assessment by classifying our risk of non-compliant behavior according to our verification of our vendor's compliance with international standards of security and privacy by verifying their standards' certifications. In case of not providing a valid certification, we asked them for a detailed description of mandatory ISMS records and controls, assessing the risk as higher than those suppliers that are certified. Our policy is to keep non-certified suppliers as few as possible.

- ISO 27002 & ISO 27017 controls: A.15.1.1

The following requirements must be met by contractors in the handling, management, storage and processing of information belonging to Inbenta Holdings Inc:

- Access to information assets and systems will be the minimum necessary to achieve business purposes.
- When the need to access Inbenta Holdings Inc. information, assets and systems ends, all Inbenta Holdings Inc. information must be returned to Inbenta Holdings Inc. when the termination of a contract.
- Inbenta Holdings Inc. may monitor the use of its information, information assets and information systems for lawful business purposes.
- Anyone granted access to Inbenta Holdings Inc. information, information assets and systems must comply with the requirements of Inbenta Holdings Inc.'s ISMS requirements. Failure to comply with these policies and other relevant instructions may constitute a breach of contract and lead to termination or legal action.
- Supplier personnel will only enter Inbenta Holdings Inc. premises with an appropriate security pass issued by Inbenta Holdings Inc. and escorted by our staff. If necessary, they must sign a Non Disclosure Agreement.
- The transmission of information between Inbenta Holdings Inc. and a supplier must be encrypted to a level commensurate with the security classification of the information and to international standards.
  Inbenta Holdings Inc. data and information may not be used for test purposes unless authorised by our COO,

CTO and CISO. In case of being authorised, data and information to be used for test purposes must be anonymized, scrambled or otherwise rendered in such a way that no Inbenta Holdings Inc. data or information can be reconstructed from that used for test purposes.

- Inbenta Holdings Inc. information may not be copied by any supplier other than as far as is necessary for providing an agreed service to Inbenta Holdings Inc..
- Suppliers must have a security incident reporting process in place to a standard and design acceptable to Inbenta Holdings Inc. to ensure that any incidents involving Inbenta Holdings Inc. information are immediately reported to Inbenta Holdings Inc. Suppliers must agree to undertake any remedial action required by Inbenta Holdings Inc. and ensure that this is implemented in an auditable way.
- A supplier holding Inbenta Holdings Inc. data on Inbenta Holdings Inc.'s behalf must have in place processes to ensure that critical Inbenta Holdings Inc. information held by them can be promptly and efficiently recovered following an emergency.
- In the event that a supplier subcontracts to a third party (either in the form of services or collaboration with people), this supplier is obliged to do the following:
    - Acceptance by Inbenta Holdings Inc. of this fact
    - Inform and guarantee that the third party subcontracted complies with the aspects related to the security policy of Inbenta Holdings Inc.
    - Make sure that the third party does not subcontract the services of another.

Addressing security with supplier agreements

Procedures to assess the level of security of our suppliers is based on a dynamic risk assessment by classifying our risk of non-compliant behavior according to our verification of our vendor's compliance with international standards of security and privacy by verifying their standards' certifications. In case of not providing a valid certification, we asked them for a detailed description of mandatory ISMS records and controls, assessing the risk as higher than those suppliers that are certified.

- ISO 27002 & ISO 27017 controls: A.15.1.2

Confidentiality and nondisclosure agreements

All our suppliers must sign confidentiality commitments and nondisclosure agreements (NDA) to protect the secrecy of the information of Inbenta and our customers.

- ISO 27002 & ISO 27017 controls: A.13.2.4

SUPPLIER SERVICE DELIVERY MANAGEMENT

Monitoring and review of supplier services

Inbenta has implemented a supplier evaluation process that involves the periodic review of compliance with the agreed service level guarantees (SLAs) and compliance with the requirements of the established services.

- ISO 27002 & ISO 27017 controls: CLD.12.4.5

Information and communication technology supply chain

Inbenta's policy is to guarantee the continuity of our services through supplier diversification and redundancy. Also, we require our suppliers' guarantees regarding the availability of their services as well as redundancy policies. Cloud service providers should ensure information security levels are maintained or exceeded with regards to those we agreed with our customers.

- ISO 27002 & ISO 27017 controls: A.15.1.3

Processing of PII

Inbenta has personal data processing agreements (DPA) with all providers that provide services that involve the processing of personal data for which Inbenta or our clients are responsible.

- ISO 27002 & ISO 27017 controls: A.18.1.4

Termination of service

Inbenta requires its providers, and especially those that provide cloud services, to delete any information they treat once the termination of service is agreed. This policy applies to all the information that is processed by virtue of the service provided, whether it is owned by Inbenta or our customers.

Inbenta's main providers are ISO-27017 compliant, so they are certified in the removal of cloud services customer assets

- ISO 27002 & ISO 27017 controls: A.11.2.7, CLD.8.1.5

Segregation of environments

Inbenta requires its suppliers, and especially those that provide cloud services, to ensure the segregation of virtual information processing environments. Cloud service providers should enforce appropriate logical segregation of cloud service customer data, virtualized applications, operating systems, storage, and network for the separation of resources used by cloud service customers in multi-tenant environments.

Where the cloud service involves multi-tenancy, the cloud service provider should implement information security controls to ensure appropriate isolation of resources used by different tenants

- ISO 27002 & ISO 27017 controls: CLD.9.5.1

Additional security methodologies

SECURITY AWARENESS

Policies

Inbenta has developed a comprehensive set of security policies covering information security and privacy. These policies are shared with, and made available to, all employees, clients, and contractors with access to Inbenta information assets. You can request a copy of our Integrated Management Policy by writing an email to compliance@inbenta.com (mailto:compliance@inbenta.com).

- ISO 27002 & ISO 27017 controls: A.5.1.1

Training

All employees MUST pass a Security Training which is given upon hire and annually thereafter. All engineers receive annual Secure coding Training, security best practices, and security by design patterns training. The Security team provides additional security awareness updates via email, blog posts, and internal wiki, sharing and updating best

practices as well as providing periodical presentations as internal events.

- ISO 27002 & ISO 27017 controls: A.7.2.2

EMPLOYEE/HR POLICIES

Confidentiality Agreements

All employees are required to sign Non-Disclosure and Confidentiality agreements.

Inbenta's contractual agreement with employees includes accepting the following agreements: intellectual property agreement; information confidentiality agreement; Professional Code of Conduct on Information Security and Privacy.

- ISO 27002 & ISO 27017 controls: A.7.1.2

Privacy and protection of personally identifiable information (PII)

PRINCIPLES

Purpose of processing

Inbenta Holdings, Inc. provides services of online communication and information search based on natural language. This means that the user can access information from the client's knowledge base by writing and submitting text, which is processed by Inbenta to return the best answer.

This processed text might include personally identifiable information (PII) which implies that Inbenta is the processor of these data on behalf of our customers (the controllers).

Also, Inbenta is the controller of the information we collect from our customers and their employees to manage the contracts and services provided to our customers to contact them, respond to their service requests, and administer their accounts.

- ISO 27701 controls: 7.2.1

Lawfulness of processing

Processing of customer's data is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

- ISO 27701 controls: 7.2.2

Privacy by design and privacy by default

Inbenta limits the collection and processing of PII to the minimum that is relevant, proportional and necessary for the identified purposes. This includes limiting the amount of PII that the organization collects indirectly (e.g. through weblogs, system logs, etc.).

Also, Inbenta does not retain PII for longer than is necessary for the purposes for which the PII is processed, just as stated in the retention criteria.

- ISO 27701 controls: 7.4.1, 7.4.2

Retention criteria

Inbenta will retain personal data we process on behalf of our Clients for as long as needed to provide services to our Client. Inbenta will retain this personal information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

Unless a different agreement is specified in the contract between Inbenta and the customer, the logs in our server are kept for a maximum of 100 days and can be removed when the services finalizes, if the client specifies it.

After this retention period, Inbenta permanently deletes the data contained in our databases, except in those circumstances in which legal obligations or duties may arise from the execution of the provision of the service, in which case a copy may be kept, with the data duly blocked, until the cessation of such responsibilities or duties.

- ISO 27701 controls: 7.4.7

ORGANIZATION OR PRIVACY MANAGEMENT

Privacy Information Management System

Inbenta has implemented a privacy information management system that ensures compliance with legal obligations, proper treatment of risks to users' rights and freedoms, and a process of continual review and improvement of applied policies.

- ISO 27701 controls: 5.2.4

Responsibilities

Inbenta has appointed a responsible for personal data protection in charge of monitoring the performance of the privacy information management system. His responsibilities include defining personal data protection policies, verifying compliance with these policies, assessing risks in the processing of personal data, determining the technical and organizational measures necessary to mitigate risks, supervising the performance of the measures involved, and the evaluation of regulatory compliance.

Likewise, all Inbenta staff have committed to comply and enforce the company's privacy policies and regulations.

- ISO 27701 controls: 5.3.3, 6.3.1.1

Data Protection Officer

Inbenta has appointed a Data Protection Officer (DPO) who is in charge of assessing and monitoring an organization-wide governance and privacy program, to ensure compliance with all applicable laws and regulations regarding the processing of PII.

The DPO would ensure effective management of privacy risks, be involved in the management of all issues which relate to the processing of PII, act as a contact point for supervisory authorities, inform top-level management and employees of the organization of their obligations with respect to the processing of PII, and provide advice in respect of privacy impact assessments conducted by the organization.

- ISO 27701 controls: 6.3.1.1

Organization of information and security operations

At the organizational level, our Chief Information Security Officer (CISO) holds the maximum level of access to information and execution of security measures, followed by our System Administrators, the Chief Operation Officer, and the Chief Technology Officer.

We document and record all mandatory ISMS controls and have a Security and Privacy Board formed by our CEO, COO, CTO, QPM, HR and CISO to monitor and assess the security of operations and incidents.

- ISO 27701 controls: 5.3.3, 6.3.1.1

Staff commitment

All Inbenta staff sign a contractual agreement by which they commit to comply with the personal data protection policies and obligations.

Said agreement includes the warning that the breach of said obligations constitutes a serious lack of indiscipline or disobedience at work and, therefore, will be punishable.

- ISO 27701 controls: 6.4.1.2

Competence and awareness

Inbenta has implemented a training program where all Inbenta employees participate in awareness-raising and training sessions on privacy protection.

In this regard, all employees manage information according to their educational and training certifications, roles and responsibilities, and have received training in the classification of information and EU Regulation 2016/679 (EU GDPR), as well as have signed an intellectual property agreement, and a statement of good practices to prevent non-normative behavior and its consequences when processing and transferring information.

- ISO 27701 controls: 6.4.2.2

RESPONSIBILITY OF THE CONTROLLER AND PROCESSOR

Security of processing

Inbenta implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Personal data processing is protected by the same technical measures that apply to all company information in accordance with ISO 27001 and ISO 27017 certification.

In assessing the appropriate level of security account has been taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

- ISO 27701 controls: 5.6.2, 5.6.3

Operations security

All of our data is stored by Amazon Web Services (AWS), which complies with international information security and privacy standards. Our cloud operational regions are located in United States, Europe, Asia Pacific, and South America. AWS certifications are available here: https://aws.amazon.com/compliance/programs/ (https://aws.amazon.com/compliance/programs/) For information at rest, encryption keys are managed by AWS-KMS and uses at least an AES256. For data in transit, all connections are encrypted under TLS > 1.2 protocol in order to provide communications security and privacy. Protocols, certificates, and ciphers can be found here: https://developers.inbenta.io/api-resources/security/regions-and-endpoints (https://developers.inbenta.io/api-resources/security/regions-and-endpoints)

- ISO 27701 controls: 5.6.2, 5.6.3, 6.9

Pseudonymisation and encryption of personal data

Every Inbenta customer has control to pseudonymize personal data coming from end-users by using the Inbenta feature “logs obfuscator,” which pseudonymizes data before storing it. Each customer must first specify what kind of data they want to pseudonymize and activate the option to do so. If the client activates this option, personal data of users enter our server already pseudorandomized. If the client does not activate this option, users’ personal data is stored in our server without any privacy anonymization since Inbenta cannot manipulate this data.

- ISO 27701 controls: 5.6.2, 5.6.3

Processors

Through the clauses for the treatment of our Data Processing Agreement (DPA), Inbenta assumes its responsibility as the data processor who processes data on behalf of our customers which is necessary to provide the contracted services.

Therefore, Inbenta gives guarantees for:

- The permanent confidentiality, integrity, availability, and resilience of the treatment systems and services.
- Restore availability and access to personal data quickly, in the event of a physical or technical incident.
- Verify, evaluate and assess, on a regular basis, the effectiveness of the technical and organizational measures implemented to guarantee the safety of the treatment.

This DPA is complemented with this Security document which details the technical and organizational measures which are implemented to fulfill the provided guarantees.

- ISO 27701 controls: 7.2.6, 8.2.1

Communication and transfer of data

The process and use of personal information by Inbenta is limited to serve our customers' needs, therefore Inbenta does not transfer data to third, non-involved parties, except to:

- Companies that, as data processors, provide us with services related to the ordinary and administrative activity of the company, such as, among others, IT services and infrastructure suppliers, such as Amazon Web Services (AWS).

Given the case, there are DPA with all these companies, providing sufficient guarantees to implement appropriate technical and organizational measures

- as required by law, such as to comply with a subpoena or similar legal process,
- when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to a public bodies requests,
- if Inbenta Holdings Inc. is involved in a merger, acquisition, or sale of all or a portion of its assets, you will be notified via email and/or a prominent notice on our Web site of any change in ownership or uses of your personal information, as well as any choices you may have regarding your personal information,
- to any other third party with your prior consent to do so
- ISO 27701 controls: 7.5, 8.5

Security breach management

We manage security incidents following the procedure from EU GDPR, which dictate that within a maximum period of 72 hours, we must report the Agency and all person and parties affected on the nature, scope, and consequences of the incident.

- ISO 27701 controls: 6.13.1.5

COMPLIANCE

Privacy Policy

This policy includes information on the purposes and legitimacy of the processing activities, the categories of data processed, the criteria for data conservation, possible communications or transfers of data, and the procedure for those interested to exercise their rights.

- ISO 27701 controls: 7.3.2, 7.3.3

Official laws and regulations compliance

Each branch of Inbenta must report to the Agency of Data Protection any data breach incident within 72 hours. Inbenta complies with EU General Data Protection Regulation 2016/679 (GDPR), as well as CCPA (US) and the LGPD (Brazil).

- ISO 27701 controls: 6.15.1, 7.2.2

International data transfer

The provision of our services may involve the processing of personal data by companies located in countries outside the European Economic Area (international data transfers). However, it will only be done with countries that offer an adequate level of protection or have made available to us Standard Contractual Clauses (SCC) in accordance with the decision of the European Commission to Data transfers from controllers in the EU to processors established outside the EU.

Specifically, information we collect from you might be processed in the United States, and by using these services you acknowledge and consent to the processing of your data in the United States.

Inbenta Technologies Inc., located in the US, is responsible for the processing of personal data it receives, under the EU-U.S. and Swiss-U.S. Data Privacy Framework, and UK extension to the EU-U.S. Data Privacy Framework (DPF), and subsequently transfers to a third party acting as an agent on its behalf. We comply with the DPF Principles for all onward transfers of personal data from the EU, Switzerland and the UK, including the onward transfer liability provisions.

With respect to obligations arising from the DPF, Inbenta Technologies Inc. is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, Inbenta Technologies Inc. may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In addition to participating in the DPF, we also use the EU Standard Contractual Clauses as issued by the European Commission as well as the U.K. International Data Transfer Agreement as secondary measures. Where needed based on our data transfer impact assessments, we will implement additional technical and/or organization measures intended to adequately protect your data.

Name of sub-processor, Server's geographical location, and Subscription provided:

Name of sub-processor	Inbenta Service Using Subprocessor	Servers' location	Subscription provided
AWS (Amazon Web Services Inc.)	– Chatbot – Messenger – Knowledge Management – Search	Depending on the location of the data subjects, the data sub-processing takes place at the nearest AWS location: – European Union (Ireland) – USA (Virginia) – Brazil (São Paulo) – Australia (Sydney) – Japan (Tokyo)	IaaS and PaaS services

		Other countries outside EU under international transfer guarantees (https://aws.amazon.com /compliance/gdpr-center/ (https://aws.amazon.com /compliance/gdpr-center/))	Server delivery network housing containing limited access control encrypted data replicas for performance improvement
Gmail (Google LLC)	– Messenger	European Union area (Ireland)	Email receipt
TURBO SMTP (Delivery Tech Corp.)	– Messenger	European Union area (Italy)	Email delivery
SMTP (j2 Global, Inc.)	– Messenger	Canada (considered adequate (https://eur-lex.europa.eu /legal-content/en/ALL /?uri=CELEX:32002D0002) by the European Commission)	Email delivery

- ISO 27701 controls: 7.5.2, 8.5.2

---

inbenta.™