Skan AI

PRIVACY FIRST PROCESS INTELLIGENCE

Empowering Businesses in Compliance-Sensitive Environments

TABLE OF CONTENTS

01 »

EXECUTIVE SUMMARY

Skan powers **Process Intelligence** to boost enterprise productivity and help digital transformation efforts succeed by providing an observation management system that uses the power of AI. By harnessing process and task mining, we offer clear insights that drive innovation and transformative results for digital transformation initiatives.

With Skan, organizations gain valuable business insights from all areas of their operations through the creation of a Digital Twin of Operations. Skan observes how people work and uses AI technologies (details in this document) to create visual representations of processes. In addition, Skan creates analytics dashboards that highlight key performance indicators in various areas such as productivity, workforce utilization and process automation opportunities.

Safeguarding Enterprise Data

Process Intelligence (PI) tools are revolutionizing enterprise operations by offering invaluable insights into workflow efficiency. However, this technological advancement brings forth concerns about data security and employee privacy, especially in verticals with stringent data protection laws and strong worker representation. Skan, with its customer base in highly regulated and sensitive industries, recognizes these challenges and has purposefully designed its PI technology to address them head-on, ensuring both powerful analytics and robust data protection.

Skan's Process Intelligence technology empowers businesses to understand and optimize their business processes while ensuring data security and employee privacy, even in regions with stringent privacy regulations. Our multi-layered security architecture incorporates advanced data anonymization, masking, and encryption techniques, along with robust access controls and infrastructure security measures.

This whitepaper delves into the technical details of our anonymized aggregate data approach, addressing specific concerns regarding work privacy, data masking, security, and transparency. We demonstrate how Skan sets the benchmark for ethical and compliant Process Intelligence across various industry contexts.

Skan Certifications & Compliance

Information Security Management ISO 27001 Certified

SOC 2 TYPE 2 AICPA SOC

TRUSTe International Privacy Verified Powered by TrustArc

GDPR

EU Artificial Intelligence Act

Employee Monitoring (Law 300)

02 »

SECURITY ARCHITECTURE: END-TO-END DATA PROTECTION

Skan's innovative approach to process intelligence is built upon a robust and multi-layered security architecture. This architecture is designed to ensure the highest levels of data protection, privacy, and compliance while delivering unparalleled insights into business processes.

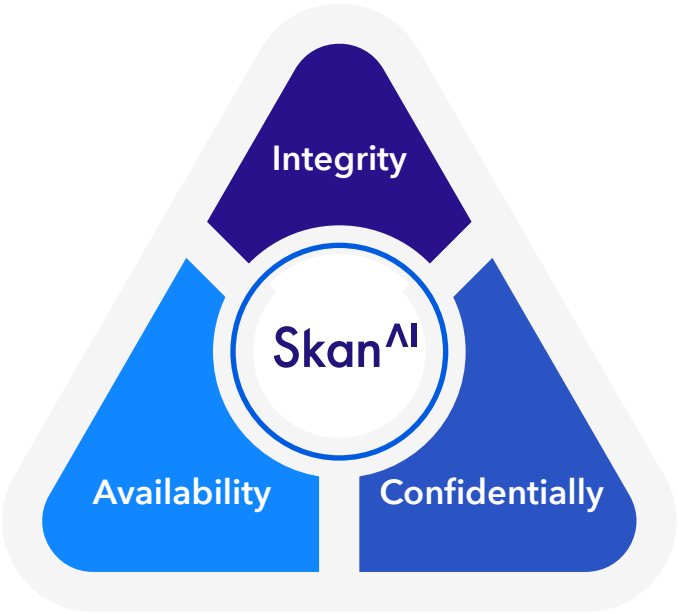
Skan's Triad of Security Platform Design

At its core, Skan's architecture is based on the principles of Integrity, Confidentiality and Availability. These principles are not merely add-ons but are fundamental to how Skan operates, ensuring that security and privacy are built into every aspect of the system.

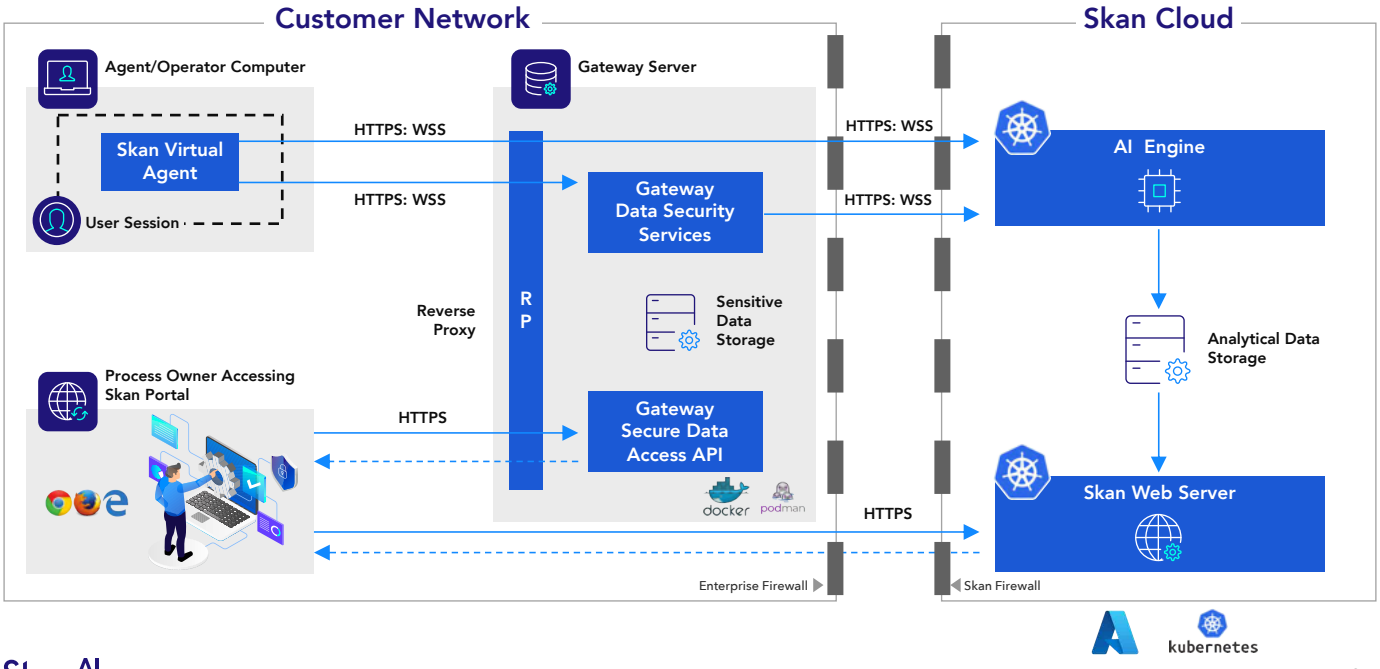
Skan maintains the highest standards of **Integrity** using various checks and balances in development and day-to-day operations.

Skan takes **Confidentiality** seriously, makes privacy a priority, and employs several controls to ensure the protection and privacy of data at all times.

Skan ensures the **Availability** of its systems using measures such as monitoring, BCP and DR.



Key Components of the Skan Platform & Data Processing Flow



Skan's architecture consists of five primary components that work in harmony to provide secure, efficient, and comprehensive process intelligence:

Virtual Assistant:

This is the point of data collection. The Skan Virtual Assistant, installs directly on employees' computers, utilizes advanced computer vision algorithms to capture detailed UI data, producing a comprehensive clickstream of every task observed.

The Virtual Assistant applies selective observation of only those applications approved for observation and applies multiple techniques to extract selected data elements with discretion ensuring privacy. This initial layer of protection begins the process of safeguarding data as sensitive information will not be collected or transmitted.

Centralized control on all VAs for observing and extracting data by selection ensures full control of privacy and follows a principle of observing only what is needed.

This initial layer of protection begins the process of safeguarding sensitive information before any data leaves the user's device.

Gateway Server:

Next, your captured data moves securely from the VA to the Gateway Server. Deployed within your network infrastructure (either on-premises or in a private cloud), the Gateway Server acts as a central hub for data processing and security reinforcement.

The Gateway Server receives protected observational data from multiple VAs across the organization. The Gateway Server further enhances data security by deepening anonymization, reinforcing masks, and extracting valuable metadata for analysis. Importantly, all sensitive data remains within this client-hosted environment, never leaving your organization's control.

Skan Cloud:

Anonymized and aggregated metadata is stored in Microsoft Azure, providing the foundation for your advanced process intelligence insights. Here, 22+ AI/ML algorithms are applied to stitch together the observation data creating end-to-end process views.

Skan's core analytical engine resides here, transforming the sanitized data into actionable insights while maintaining stringent security measures. Advanced algorithms and AI technologies are employed to extract deeper intelligence on processes, enabling optimization and transformation opportunities without compromising data privacy.

Only whitelisted IP addresses for the customer are allowed to access the Skan Cloud.

Use MTLS security for communication between Skan Gateway Server and Skan Cloud.

Firewell:

As your data flows through the Gateway Server and into the Skan Cloud, it passes yet another security checkpoint. The Firewall, in conjunction with other critical security functions such as the Intrusion Prevention System, and malware inspection is an important security barrier between the Gateway Server and the Skan Cloud.

The Firewall implemented in the Client's network ensures that only authorized connection requests on designated ports can pass through. The Skan Gateway connects to the Skan Cloud by opening only an outbound connection through the firewall and thus is crucial in preventing any inbound request to access sensitive data stored on the Gateway Server.

This maintains a strict separation between the client's private information and Skan's analytics platform. This setup allows Client IT Stakeholders to enforce the access policies as per corporate-approved practices.

Skan Portal:

The Skan Portal provides a secure interface where authorized users can interact with anonymized and aggregated process intelligence information and analytics. Employing advanced visualization techniques and strict access controls, including role-based access control (RBAC) and multi-factor authentication (MFA), the portal ensures that sensitive information remains protected while delivering actionable insights tailored to users' specific roles and responsibilities.

Through the portal, users can access interactive process maps, performance metrics, and optimization recommendations derived from the anonymized data. The portal's design prioritizes both security and usability, providing a seamless experience for authorized users to leverage the power of Skan's process intelligence while maintaining the highest standards of data protection.

03 »

DATA PRIVACY SAFEGUARDS

Data Capture and Processing

Skan captures information using software installed directly on the desktop computers for operators/agents called the Virtual Assistant (VA). This powerful tool serves as both observer and protector, capturing valuable process data while simultaneously implementing robust security measures.

The VA's primary function is to provide non-intrusive process discovery and optimization. It achieves this through advanced Computer Vision algorithms that:

- Meticulously analyze and document granular steps within digital processes
- Observe user interactions on the computer screen only for whitelisted and approved applications

From the moment data is captured, the VA implements security measures designed to protect sensitive information at the source.

Security Safeguard #1: You Approve Applications to Observe

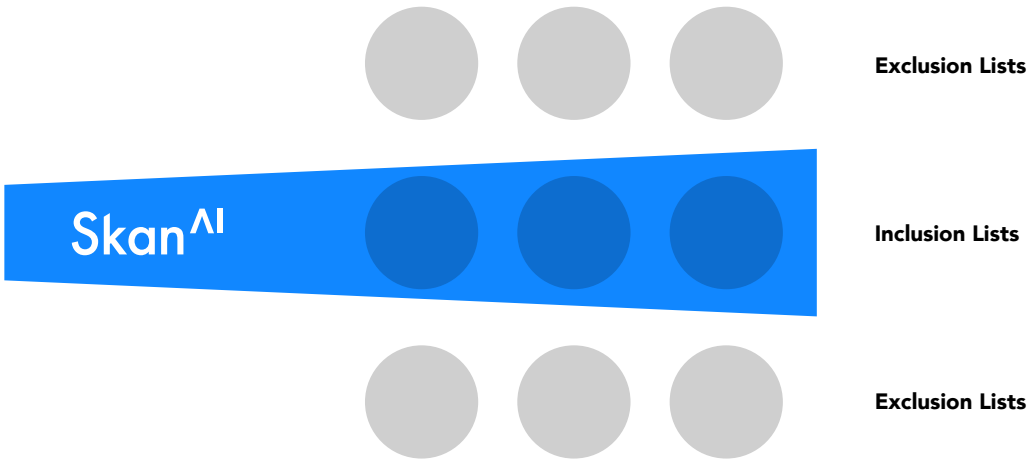
At Skan, we believe that true data security starts with putting control in the hands of our clients. Skan's customers whitelist and approve applications within the observation scope of the VAs to meet the specific requirements each customer outlines at the beginning of any engagement with Skan.

By default, the VA's no applications are selected for observation until approved. This approach ensures that your sensitive data remains private unless you explicitly choose to include it in the process analysis.

Key aspects of this privacy-first approach include:

Precision targeting:	Strict adherence to boundaries:	Respect for privacy:
Create both inclusion and exclusion lists to fine-tune the VA's focus, ensuring it only observes the processes most relevant to your goals.	The VA only captures digital actions within client-approved applications, associating them exclusively with the specific process and iterations being studied.	When a user engages with an application on the exclusion list, the VA not only disregards this activity but also omits it from learning models, categorizing such time simply as "non-process" usage.

This granular level of control allows organizations to harness the power of process intelligence while maintaining stringent data protection standards. It's not just about analyzing processes; it's about doing so on your terms, with your unique process optimization goals at the forefront.



* This is an opt-in feature; by default, no applications are selected for observation.

Security Safeguard #2: Data Masking & Anonymization

As the VA captures data, it simultaneously employs best-in-class masking techniques to protect Personally Identifiable Information (PII):

> **Employee Anonymization:**

Names are replaced with anonymous identifiers throughout the system

> **Non-Reversible Masking:**

A proprietary region masking algorithm utilizes altered pixel intensity values to ensure that masked areas cannot be reversed

> **Application Image Protection:**

Sensitive fields or entire screens can be masked where applicable

> **Customizable Anonymization:**

Configurable options allow clients to replace sensitive data fields with generic identifiers in the reporting phase, tailored to organizational needs

> Skan's robust data segregation and metadata transfer approach gave us the confidence to implement process intelligence across our sensitive financial operations. Their commitment to keeping our data within our own network is a game-changer.
>
> - VP Of Operations, Fortune 500 Financial Services Company

Data Transfer and Processing

Once the VA captures data and information from a given desktop, the data is sent to the Gateway Server. The Gateway Server acts as a sophisticated checkpoint, enhancing both security and privacy as data travels through the Gateway Server and into the Skan Cloud for analysis.

Security Safeguard #3: Flexible Deployment Options with Layered Security

At Skan, we understand that every organization has unique security needs and infrastructure preferences. That's why we've designed our Gateway to be adaptable to various deployment scenarios, always maintaining stringent security measures:

- **On-premises deployment:** The Gateway Server is installed behind your own firewall, providing maximum control over your data environment.
- **Private cloud deployment:** The Gateway can be hosted in a private cloud environment managed by your organization, offering flexibility while maintaining full control.
- **Skan-hosted cloud deployment:** For organizations preferring a fully managed solution, Skan can host the Gateway in a secure cloud environment.

Regardless of the deployment option, the Gateway Server is always protected by a firewall, ensuring that sensitive data remains secure. This versatility allows you to seamlessly integrate Skan's architecture with your existing security protocols, ensuring that your data remains within environments you trust and control.

Security Safeguard #4: Robust Data Encryption, Segmentation, & Transfer

As data passes through the Gateway Server and into the cloud, it undergoes a series of rigorous security processes. The following details the layers of protection that safeguard your information:

Data Transport Encryption: A Shield for Data in Motion

Data is transmitted through secure, encrypted channels using industry-standard encryption protocols. Even in the event of interception, the data remains inaccessible without proper decryption keys. The Gateway Server provides:

- **Secured protocols:** Customized to your specific security requirements
- **End-to-end protection:** Shield data from unauthorized access or interception throughout its journey

Data Segregation and Metadata Transfer: Minimizing Exposure

A cornerstone of Skan's privacy-first architecture is our comprehensive approach to data handling. This allows only the most essential, non-sensitive information to pass through:

Screenshot Retention: All visual data captured during process observation stays securely within your network

Metadata Only: Only abstracted metadata – the essence of the process without the sensitive details – is transferred to Skan's servers

Limited Data Exposure: External access to the Skan portal never reveals actual screenshot images to maintain a strict barrier around your sensitive information.

Clients maintain full access and control of the data stored in the Gateway, which is protected by a firewall, ensuring that no sensitive or unmasked data ever reaches the Skan Cloud.

This careful segregation of data significantly reduces the risk of sensitive information exposure while still enabling Skan to provide powerful process intelligence insights.

As data completes its journey through the Gateway, it emerges ready for analysis, having undergone multiple layers of security processing. The result is a dataset that maintains the highest standards of privacy and confidentiality while still holding the key to valuable operational insights your organization needs to drive real transformation.

Next, we'll explore how the metadata is securely transferred to the Skan Cloud for analysis, maintaining our commitment to data protection.

> The level of granular control Skan offers over data security and access rights addressed significant compliance concerns. It's rare to find a solution that balances deep process insights with such stringent privacy measures.
>
> - Director of Compliance, Global Insurance Firm

Skan's Intermediary Firewall

Before data reaches the Skan Cloud, it must pass through one final checkpoint - a firewall between the Gateway Server and the Skan Cloud.

The firewall works in conjunction with Intrusion Prevention and other critical security functionalities with layer 4 to 7 inspection:

01

Rigorous packet inspection:

Every data packet is scrutinized for potential security threats

02

Strict access control:

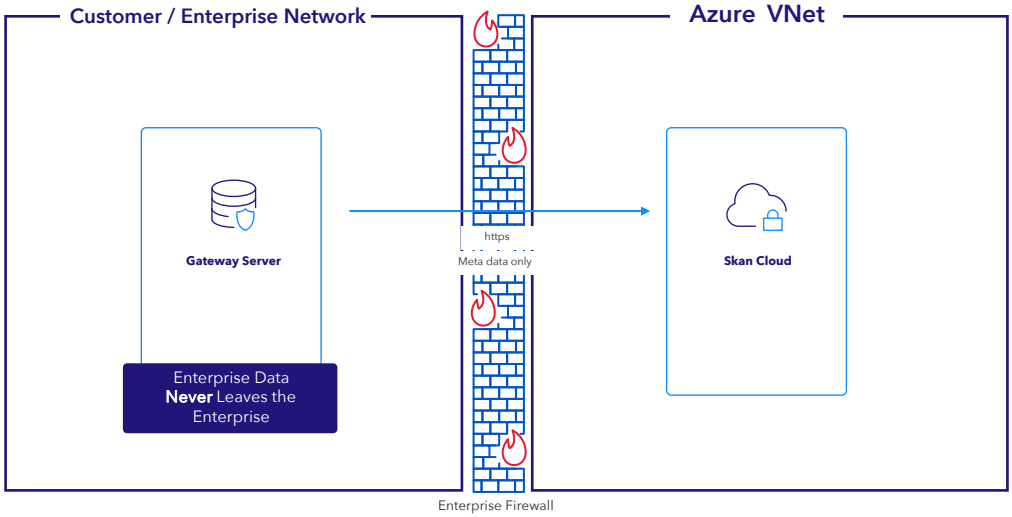
Only authorized, encrypted metadata is allowed to pass through

03

Continuous monitoring:

The firewall is always monitoring data, adapting to emerging threats in real-time

This critical component adds an extra layer of defense, ensuring that only the most essential, thoroughly vetted information reaches our Cloud analytical engine. It double-checks that all our previous safeguards have done their job effectively.



By implementing this powerful firewall, we create a clear delineation between your internal network and our cloud environment. This separation provides an additional buffer of security, further minimizing the risk of unauthorized data access or potential cyber threats.

This final security check ensures that we protect your sensitive information as metadata is sent to the Skan Cloud for analysis.

The Skan Cloud: Processing and Analysis

Skan Cloud is the analytical powerhouse where metadata is transformed into actionable insights. Here, advanced technologies converge to process the metadata from the Gateway while upholding the highest standards of security and privacy.

01

Skan Cloud Hosting

Skan has set up its cloud infrastructure on Microsoft Azure's Cloud which is composed of a globally distributed, ISO27001, SOC1, and SOC2 and FedRAMP compliant datacenter infrastructure, supporting thousands of online services and spanning more than 100 highly secure facilities with worldwide physical security standards, employing strict access controls, surveillance, and environmental safeguards. For more information on Microsoft Azure security: https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security.

02

Hosting Location

Based on the customer's location, the required compute and storage services will be deployed to an Azure location in the customer's region. This option ensures that customers have ultimate control over data storage location.

03

Azure Security Services in Use

Skan also makes use of several security services available in Azure such as strong authentication, role-based access, Azure Key Vaults, data encryption, Azure DevOps, data redundancy, etc., as part of its Cloud Security strategy. Details are in subsequent sections.

Security Safeguard #5: Skan Cloud 3rd Party Technology for Analytics Purposes

Skan Cloud works like a high-tech command center where streams of metadata converge and transform into meaningful process intelligence. This powerful hub is built on a foundation of cutting-edge technologies:

> **MongoDB and Databricks:**

Provides robust, scalable data storage and processing capabilities

> **Docker and Kubernetes:**

Ensures efficient service management and seamless scalability

> **Proprietary Analytical Service:**

Interprets data and generating valuable process insights

> **Power BI Integration:**

Delivering powerful data visualization and reporting tools

This advanced infrastructure design keeps security at its core, ensuring that customer data remains protected throughout the analysis phase. It acts as a knowledge repository, where a customer's valuable process intelligence insights are not only generated but also safeguarded to provide security and privacy.

Security Safeguard #6: Encryption at Rest

Keeping customer data protected is the most important priority. In the Skan Cloud, customer data remains protected whether it is in motion or at rest:

> **Best-in-class encryption:**

All data stored in the Skan Cloud is encrypted using industry-leading standards

> **Secure credential management:**

Salted user password hashes are stored using advanced cryptographic techniques

> **Stringent cloud access policies:**

Strong password enforcement with MFA, Segregation of Duties and regular policy updates maintain a robust security posture

This approach ensures that even if someone were to gain unauthorized access to our storage systems, your data would remain indecipherable and secure.

Security Safeguard #7: Strict Data Isolation

On Skan Cloud, customer data is stored separately and secure from other clients' information:

> **Multi-tenant architecture:**

Allows efficient resource use while maintaining strict data boundaries

> **Industry-best practices:**

Our approach adheres to and often exceeds standard data isolation protocols

> **Metadata-driven separation:**

Customer data and configuration information are kept distinct using advanced isolation techniques

This separation ensures that the customer's process intelligence insights remain exclusively yours, with no risk of cross-contamination between clients.

Security Safeguard #8: Responsible Data Lifecycle Management

We understand that responsible data handling extends beyond analysis to include retention and deletion. Our flexible approach includes:

> **Customized retention policies:**

Aligned with individual customer agreements and regulatory requirements

> **Secure deletion protocols:**

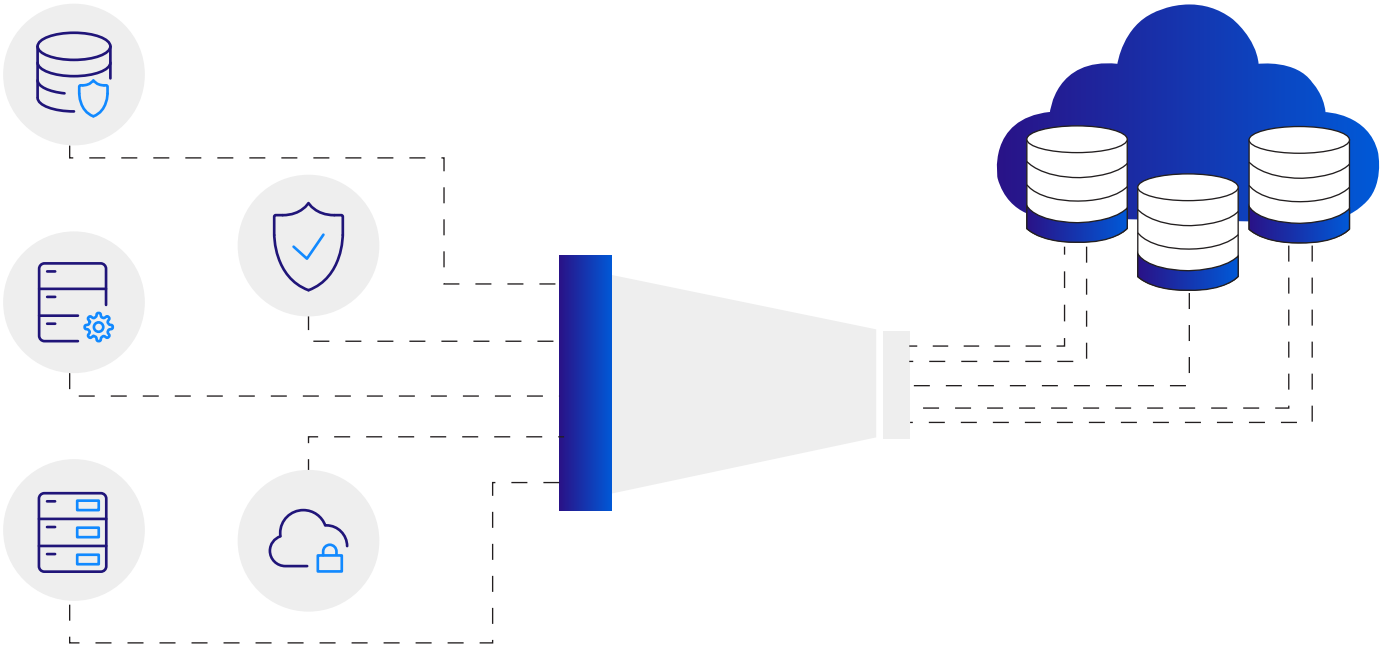
Each data deletion request is carefully logged and authorized

> **Default safeguards:**

A 60-day retention period post-subscription ensures data isn't held longer than necessary

> **Data return options:**

We provide secure methods for returning your data upon request



As your data completes its journey through the Skan system, it emerges as valuable, actionable intelligence, having been protected at every step by our comprehensive security measures. This combination of advanced analytics and unwavering data protection demonstrates that with Skan, you don't have to choose between powerful process intelligence and ironclad security - you can have both.

> Skan's clear and flexible data retention policies gave us peace of mind. As a healthcare payer, ensuring our members' sensitive data is handled in compliance with strict regulatory requirements was crucial in our decision to partner with Skan.
>
> - **Senior Manager of Claims Processing, Leading Health Insurance Company**

The Skan Portal: Secure Insights Delivery

As we reach the final destination in our data journey, we arrive at the Skan Portal - the secure interface where authorized users access and interact with the valuable process intelligence insights generated from your data. This portal serves as the bridge between the powerful analytics of the Skan Cloud and the decision-makers in your organization, all while maintaining the highest standards of data protection.

Security Safeguard #9: Role-Based Access Control (RBAC) and Authentication

On Skan Cloud, role-based access control (RBAC) policies have been designed with need-to-know and segregation principles:

- **Custom-tailored roles:**
  Users are assigned specific roles based on their job functions
- **Granular permissions:**
  Each role is granted carefully defined rights to Skan resources
- **Need-to-know basis:**
  Ensures sensitive data and functionalities are accessible only to authorized personnel
- **Multi-Factor Authentication (MFA):**
  Adds an extra layer of security beyond traditional passwords
- **Single Sign-On (SSO) Integration:**
  Allows seamless integration with your existing authentication systems

This multi-layered approach creates a secure environment where data access is not just restricted, but intelligently managed, ensuring that your process intelligence insights are accessible only to authorized personnel.

Security Safeguard #10: Encrypted Data Transmission

Skan employs secure protocols to protect all network traffic using:

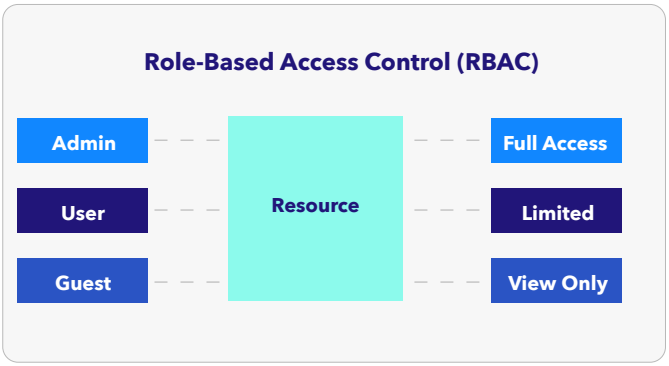
- **TLS 1.3 (or higher) Encryption:**
  Ensures all data in transit between the Skan Cloud and the portal is encrypted
- **Secure API Endpoints:**
  For organizations integrating Skan insights into their own systems
- **Regular Security Audits:**
  To verify the continued efficacy of our encryption measures

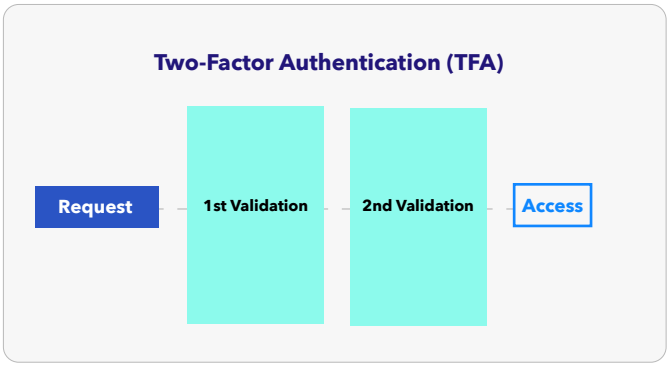
Security Safeguard #11: Privacy-Preserving Visualizations

Process-level insights are provided without exposing individual user details through privacy-preserving visualizations.

- **Aggregate Data Display:** Insights are presented at a process level, without revealing individual employee information
- **Dynamic Data Masking:** Any potentially sensitive information is automatically obscured in reports and dashboards
- **Customizable Anonymization:** Allows you to set specific rules for how data is displayed, ensuring compliance with your privacy policies

These techniques ensure that users can gain valuable insights into process performance and optimization opportunities without compromising individual privacy.

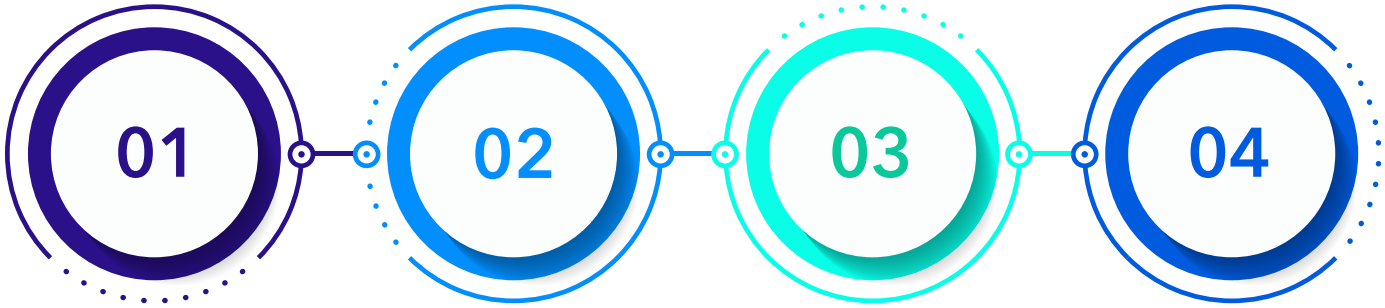




04 »

ACCESS, COMPLIANCE, AND TRUST

This section provides details on how Skan systematically approaches security, privacy, and compliance:



Infrastructure integrity

The responsible use of AI

Client trust

Adherence to international standards

Infrastructure and Operational Security

At Skan, we understand that true security isn't just about protecting digital data; it's about creating an ecosystem where every component is fortified against potential threats, both physical and digital. Our holistic approach ensures the integrity, reliability, and resilience of our process intelligence platform from the ground up.

Security Safeguard #12: DevSecOps Practices

Security measures in cloud-based operations are critical to the services Skan offers and help extend protections to each data transfer step and storage. Our DevSecOps approach ensures that security considerations are addressed at every stage:

> **From concept to deployment:**

Security checks are integrated from the initial requirements gathering to the final code deployment

> **Continuous vigilance**

Even after deployment, we maintain ongoing security monitoring and updates

This proactive stance means we're not just reacting to threats but anticipating and preventing them before they become issues.

Security Safeguard #13: Monitoring and Alerting Mechanisms

Monitoring systems continuously track network and system activities to detect and respond to potential security incidents, employing industry-leading protection mechanisms.

> **NextGen Firewalls:**

Every incoming request is scrutinized through a NextGen firewall with layer 4 to 7 packet inspection, threat prevention, malware prevention, DNS security, etc.,

> **Network-level protection:**

Our firewalls and zoning ensure only whitelisted IP addresses can interact with our systems

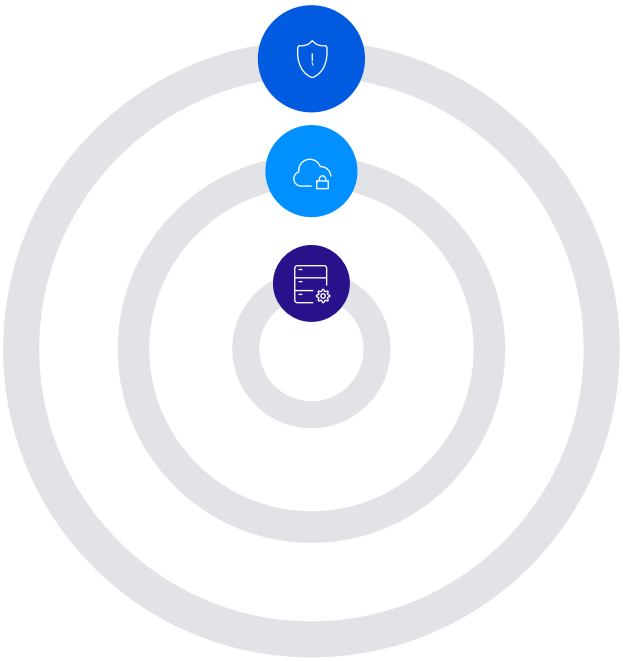
> **Comprehensive logging:**

All system activities are recorded and analyzed, providing a clear audit trail

Physical Infrastructure Protection

DevSecOps Practices

Monitoring and Alerting Mechanisms



Transparency and Communication

While cutting-edge technology forms the backbone of our security framework, we recognize that true data trust is built on openness and clear communication. At Skan, we believe that transparency isn't just a buzzword – it's a fundamental component of our comprehensive data protection strategy.

Security Safeguard #17: Fostering a Culture of Data Trust

We've cultivated an environment where open dialogue about data usage is not just encouraged but essential:

> **Education is key:**

We provide detailed documentation and training on our data collection, anonymization, and analysis methods

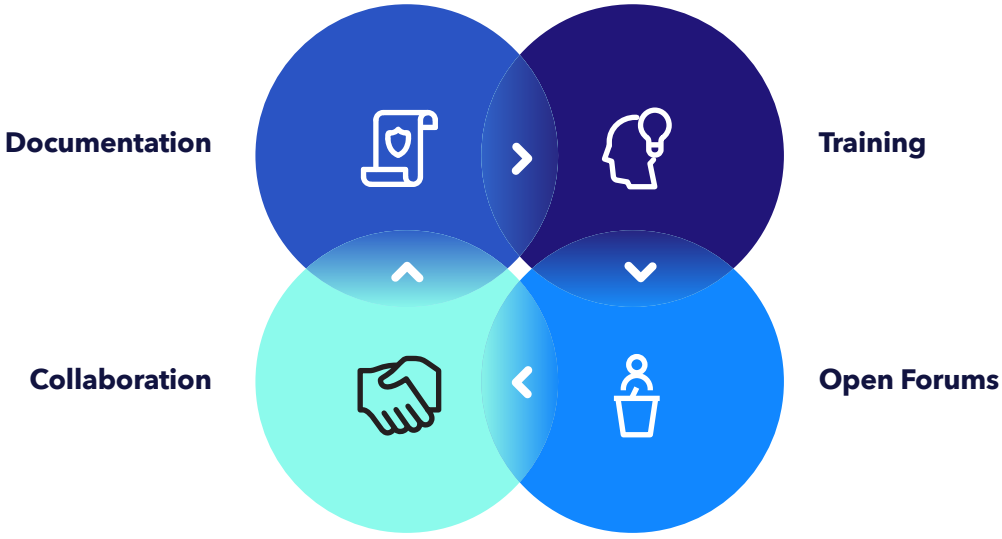
> **Open forum policy:**

Regular Q&A sessions create a space for addressing concerns and answering questions

> **Collaborative approach:**

We work with our customers to ensure observation only includes the applications necessary for process improvement initiatives

This commitment to transparency extends beyond mere compliance; it's about building lasting trust with all stakeholders involved in the process intelligence journey.



> Skan's transparency in communication and willingness to collaborate with our workers' council was impressive. Their approach to ethical AI and data handling aligns perfectly with our corporate values.
>
> - Senior Information Systems Manager, Multinational Banking Corporation

05 »

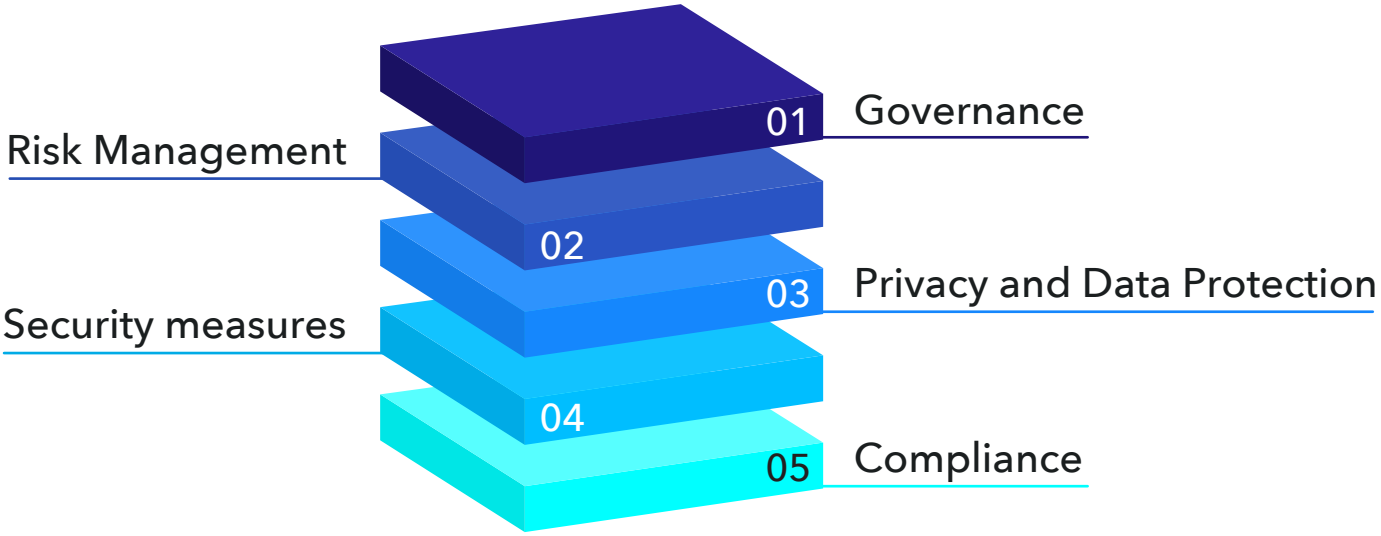
SECURITY PROCEDURES

Skan employs a comprehensive, multi-layered security approach that addresses several key areas:

- Governance
- Risk Management
- Security measures
- Privacy and Data Protection
- Compliance

Security measures cover several areas in line with Skan's Information Security Management System, such as:

This multi-faceted strategy ensures that security is maintained at every level of the system, from data handling and masking to user access and beyond. Skan maintains an Information Security Management System (ISMS) (Created in 2021) and invests significantly each year in the Security & Privacy programs. Skan sets up independent verification mechanisms. Skan regularly reviews, evaluates, and updates security policies and procedures



Additional details about each of the 12 areas are following:

Personnel / HR Security

- Personnel security policies covering
- Non-Disclosure and employment agreements
- Background verifications
- Staff orientation programs including security awareness
- Role-based training programs
- Timely onboarding and offboarding processes
- Various employee engagement initiatives

Identity & Access Management

- Unique identification
- Multi-factor authentication by default to access any resource on Azure Cloud
- Role-based privileges and authorization per Azure service or resources
- Quarterly review of user IDs and account privileges
- Timely deactivation of IDs
- Continuous monitoring of user access controls
- Secure remote access over TLS 1.3, MFA and VPN
- Endpoint security policies
- Secure email and Internet access
- Use anti-phishing, anti-spam, DKIM, SPF, URL restriction policies

End-Point Security Controls

- Strong data security using full disk encryption
- Cloud-based enforcement of end point security protection software
  - Anti-malware
  - Prevention of access to certain categories of websites
  - Data Loss Prevention
  - Periodic security and OS updates
  - Secure management of passwords
- Multi-Factor authentication
- Restrictions for unwanted software
- Restrictions for Admin access
- Enforcement of security policies through MDM tools
- Continuous monitoring of end point security controls

Cloud Security

Azure Network Infrastructure:

- Subscription level segregation between Dev and Prod environments
- Subscription level security protection using firewall with IPS, VPN, URL filtering, DoS protection, etc.,
- Virtual network level separation using virtual firewalls
- Whitelisting of source IP addresses
- Restrictions on remote console access
- Prevention of root logins
- Remote console access through VPN

Skan manages cloud security using the following:

- Monitors Azure's Security Compliance and Posture
- Strong access controls and with RBAC
- Multi-layered network segmentation and security
- Security logging and monitoring
- Infrastructure redundancy with multi-availability zones
- Segregation of duties in application development, infrastructure management, etc.,

Cloud Operational Security

- Apply patches and security updates of virtual resources
- Continuous assessment of security vulnerabilities and remediation
- Configuration management to maintain security baselines
- Control over changes to infrastructure through Terraform
- Security assessments of Skan platform images and remediation
- Monitoring of cloud security posture

Data Classification, Retention and Disposal

- Skan relies on classifying data appropriately
- Data classification policy is enforced through Office365 for all Office documents and email
- Endpoints and cloud access monitored using Data Loss Prevention tools
- Data encryption at rest on Skan Cloud
- Data retention as per contractual terms
- Secure data disposa

Data Security

Data security measures include:

- Policies for data classification, retention and disposal
- Periodic monitoring of security controls
- Certificate-based authentication among Skan Platform components
- Database logging
- Encryption of all network traffic using TLS 1.3
- Encryption of all data at rest using AES
- Secure management of secrets, keys and passwords using exclusive key vaults with access controls
- Daily, weekly, & monthly data back-up
- Back-up restoration and disaster recovery testing
- Segregation among developers and production support teams

Within the Skan Platform

- Observe only those applications that are explicitly allowed
- Secure and retain observed customer data within customer premises
  - In the case on-premise deployment
- Access observed process images available only to customers
  - Even Skan staff cannot access process images in any deployment model
- Anonymize personal information
  - PII and data from applications
- Mask process information
- Transfer only non-personal metadata to Skan Cloud
- Environment and data segregation from other customers
- SSO Integration with strong user authentication to UI Portal
- Granular access control including RBAC restrictions enforced within UI Portal

Secure Software Development Practices (SDLC)

- Strong segmented access control with MFA
- Role-based access and permissions
- Restricted administrative access
- Security policies for reviewers and approvers of pull requests
- Restricted release control for every deployment
- Continuous application code scanning during software development lifecycle
- Continuous security scanning of application code for vulnerability

Security Testing

Various testing occurs throughout each year:

- Platform is tested twice a year by a 3rd party vendor for application security
- Cloud infrastructure undergoes security penetration testing by a vendor
- Each software release undergoes testing by the internal QA team. Includes security testing.
- Platform images are tested for security vulnerabilities, internally
- Application code is tested for security vulnerabilities, internally
- Tabletop exercises for disaster recovery and incident management

Business Continuity & Disaster Recovery

BCP and DR plans include:

- Skan Cloud infrastructure offers resilience through multiple available zones
- Uses geographically redundant storage for data
- Infrastructure configured to scale automatically
- Alert communications through dedicated, customer-specific channels
- Monitor and response from Skan support staff across time zones
- Data back-up program
- Periodic recovery testing

Security Logging & Monitoring

- Uses a centralized log collection and correlation system
- Collects security audit logs from critical environments
- Analyses and alerts in case of security incidents
- Has security incident management policy and plan for specific events
- Conduct incident response tabletop testing

3rd Party Vendor Security

Skan uses Azure Cloud, Okta (Auth0) and Elastic Cloud to deliver services through Skan Cloud

For other vendors:

- Skan evaluates vendor security measures and compliance periodically
- Maintains vendor inventory and security posture-related details
- Detailed security evaluations before onboarding new vendors
- Place data protection agreements in place for all vendors

Additional 3rd Party Tools in Use

- **Azure Cloud Tools:** infrastructure security
  - Key Vault, Network Security Groups, Defender, Threat and Vulnerability Monitoring
- **Sophos Intercept:** end points protection
- **Office 365:** email security, DLP and threat intelligence
- **Drata:** continuous monitoring
- **Rapid Fort:** security vulnerability assessment of Platform images
- **Sonar Cloud:** code scanning and security hotspots
- **Jamf:** secure management of Mac endpoints
- **Intune:** secure management of Windows endpoints
- **Azure DevOps:** secure and reliable infrastructure management and application development
- **Manage Engine:** patch and vulnerability management
- **Terraform:** controlling changes to infrastructure
- **Usecure:** user security awareness management
- **Palo Alto VM-300:** Firewall Software

Responsible AI: Security and Governance

Beyond technical excellence and data security, Skan is committed to the ethical development and deployment of AI. This section explores how we ensure our AI-driven process intelligence solutions not only deliver powerful insights but also adhere to the highest standards of responsible technology use.

Model Validation

We implement rigorous testing and validation protocols for our AI models to ensure they perform accurately and reliably in real-world scenarios. Our process includes:

- **Regular retraining of models** with new data to maintain their effectiveness and relevance
- **Comprehensive testing** across diverse datasets to ensure consistent performance
- **Continuous monitoring of model outputs** to detect and address any anomalies

Bias Mitigation

We are committed to identifying and mitigating biases in our AI models.
Our approach includes:

- **Using diverse datasets** that represent a wide range of industries, processes, and user groups
- **Conducting regular fairness assessments** to ensure equitable treatment across different demographics
- **Implementing bias detection algorithms** to identify and address potential biases in model outputs

Transparency

We believe in demystifying AI decision-making processes. To this end, we:

> **Provide clear explanations**

of how our AI models analyze processes and generate insights

> **Develop user-friendly documentation**

that allows stakeholders to understand the logic behind AI-generated recommendations

> **Offer detailed model cards**

that outline the capabilities, limitations, and intended use cases of our AI systems

Purpose Limitation

We are committed to using AI technologies strictly for their intended and stated purposes. This means:

> **Clearly defining and communicating**

the scope and objectives of our AI-driven process intelligence solutions

> **Implementing safeguards**

to prevent the deployment of our AI systems in ways that could potentially harm individuals or organizations

> **Regularly reviewing and updating**

our AI use cases to ensure alignment with ethical guidelines and customer expectations

Human Oversight

While our AI systems are highly advanced, we believe in maintaining appropriate human oversight. Our approach includes:

- **Establishing clear protocols** for human review of critical AI-generated insights and recommendations
- **Providing intuitive interfaces** that allow users to easily validate and, if necessary, override AI-generated process optimizations
- **Maintaining a team of human experts** who continuously monitor and evaluate the performance of our AI systems

Continuous Improvement

We foster a culture of continuous learning and improvement in our AI development and deployment. This involves:

- **Staying updated with the latest advancements** in AI ethics and incorporating best practices into our operations
- **Actively participating in industry forums** and collaborations to contribute to the development of ethical AI standards
- **Regularly soliciting feedback** from our users and incorporating their insights into our AI development process

By adhering to these principles of responsible AI, Skan ensures that our process intelligence solutions not only drive innovation and efficiency but also uphold the highest standards of ethical technology use.

06 »

RESPONSIBLE AI: SECURITY AND GOVERNANCE

AI Security

Skan takes AI security seriously. As a result, Skan maintains an AI governance framework that includes:

- Secure and compliant use of open-source AI tools in its platform
  - E.g. for image feature extraction and anonymization
- Maintaining an inventory of AI tools and purpose of use
- Maintains extensive documentation on all the use cases
- AI use cases are assessed for security, privacy, and compliance risks and mitigation
- Functionalities of AI tools are restricted to a single customer deployment
- AI tools used other than OCR train dynamically on observed data per customer
- Does not take user inputs or any inputs or information from any external sources
- No risk of training on one customer's data and using it for another customer
- No risk of copyright or left violations

AI Governance

Transparency on Use of AI & AI Systems

By disclosing to individuals that AI is used in the system, individuals will become aware and can make an informed choice of whether to use of AI-enabled system

1. General Disclosure

Inform its users that they are interacting with an AI-powered feature

Understanding how an AI model reaches a decision.	Ensuring safety and resilience of AI system.	Ensuring quality of data and outcome	Ensuring proper human oversight of AI system
This allows individuals to know the factors contributing to the AI model's output	Ensuring that the AI system will not cause harm, is reliable and will perform according to intended purpose even when encountering unecxpected inputs.	Ensuring that the AI system does not unintentionally discriminate.	Ensuring human accountability and control
2. Explainability The system provides explanation of system's process for generating the output. **3. Logging & Traceability** For an Investigation into how the model was functioning or why a particular prediction was made. **4. Model registry** Store and manage models for versioning, refuse and auditing. **5. Model config/data** Prompt examples,...	**6. Privacy** Consumer privacy is respected and customer data is not used beyond its intended and state use **7. Security** Detecting and mitigagting system vulnerabilities. **8. Repeatability/Reproducibility** The ability to consistently perform an action or make a decision, given the same scenario. **9. Robustness** AI system will not cause harm, is reliable and will perform according to intended purpose even when encountering unexpected inputs.	**10. Data Provenance** Allows an organisation to ascertain the quality of the data based on where the data originally came from, how it was collected, curated and moved. **11. Data Bias & Fairness** Ensure that the training data and generated content is fair unbaised **12. Gold Feature storage** Store the gold standard of features that have been painstakingly curated and prepped.	**13. Responsible/Accountability** • Monitor Model Performance • End user feedback **14. Human Agency & Oversight** • Human in the loop • Human over the loop • Human out of the loop

AI Services and Use Cases

Nos.	Service Type	Model Name(S)	Service Detail	Description	Required	Remarks
1.	**Natural Language Processing**	NLP, Hidden Markov Models, Pattern Mining	Feature Extraction, Anonymization, Activity Discovery and Naming	Part of speech tagging, named entity recognition, compound word segregation , instance data pruning	Required	Feature extraction and anonymization services reside on the gateway while the activity discovery service resides on Skan cloud. Anonymization service uses NLP models such as named-entity recognition and part of speech tagging in addition to proprietary algorithms. The public models used are Stanford's NER tagger and Spacy models. These models are deployed inhouse (gateway) and are purely used for inferencing. No fine-tuning or training is performed on these models.
2.	**Ensemble**	Unsupervised Skan.ai Proprietary Model	Browser model training	Distinguishing the different activities within web applications	Required	This service resides on Skan cloud and is a proprietary model. Classic graph simplification algorithms are adopted.
3.	**Ensemble**	Unsupervised Skan.ai Proprietary Model	Case Discovery/ Contextual Disambiguation	Predicting the case ids for events where they are not present	Required	This service resides on Skan cloud and is a proprietary model. Classic conditional probability based techniques are adopted. If the processes and applications considered have the case_id in most of the screens, we can have this service optional
4.	**Computer Vision**	Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM)	OCR/Attribute Extraction	Extract text from images for attributes	May be required	This service resides on the gateway and uses public OCR engines/models viz., tesseract and paddle. The models are deployed inhouse and used purely for inference and no data is fed to the models for training. This engine maybe required for handling special applications
5.	**Computer Vision**	Deep Learning	Masking	Blur out (mask) sensitive information	Nice to Have	There are different flavors of masking supported ranging from full image masking to fixed section masking (e.g., title bar) and field level masking. Each of these variants can be turned on/off. For fixed section masking, we use public model of SAM (Segment Anything Model) and variants of it. For field level masking we use public OCR engines (tesseract/paddle). This service resides on the gateway, is deployed inhouse, and is purely used for inferencing purposes. No data is sent/fed into the model for training.

AI Services and Use Cases

Nos.	Service Type	Model Name(S)	Service Detail	Description	Required	Remarks
6.	**Computer Vision**	Visual Pattern Matching	Disambiguation Service	Classify screens	Nice to Have	This service resides on the gateway and is a proprietary model.
7.	**Natural Language Processing**	Language Modeling with N-Grams	Variant Discovery, Trace Alignment	Discovering process variants and backbone of the process executions	Nice to Have	This service resides on Skan cloud and is a proprietary model.
8.	**Ensemble**	Unsupervised Skan.ai Proprietary Model, Multi Modal Learning	Widget and Attribute Extraction	Be able to disambiguate the different widgets of the application and identify the different manifestations of the label across multiple screens of an application	Nice to Have	This service resides on the gateway and is a proprietary model.
9.	**Ensemble**	Random Forests, Decision Trees, Association Rule Mining	Variant Explanation, Driver Analysis	Be able to find signature patterns to explain variations in the processes, find driver attributes that influence KPIs	Nice to Have	This service resides on the Skan Cloud and is a proprietary model
10.	**Deep Learning**	Sequence Mining, Generative Pre-trained transformers	Task Discovery	Contextual transformation of low-level event data to high level tasks	Nice to Have	This service resides on the Skan cloud and is a proprietary model.

07 »

NAVIGATING GLOBAL DATA SECURITY, PRIVACY, AND LABOR LAWS

Regulatory Landscape:

In today's data-driven economy, businesses must adhere to a complex patchwork of regulations around privacy, data retention, worker monitoring, and AI use. Legal frameworks such as the EU's GDPR, the AI Act, and national laws like the Workers' Statute (Art. 4 Law 300/1970 in Italy) present significant challenges. Skan's technology, which allows for selective application monitoring and ensures de-identified, on-premise data processing, provides a compliant solution to these global challenges.

Key Compliance Challenges:

Worker Monitoring and Privacy:

Regulations like the Workers' Statute in Italy restrict employers from intrusive monitoring of individual employees. Skan's ability to whitelist applications ensures that only relevant activities are observed, mitigating concerns about excessive surveillance.

GDPR and Data Privacy:

The General Data Protection Regulation (GDPR) sets stringent guidelines for processing personal data, mandating safeguards like anonymization and limited retention.

AI Accountability and Transparency:

The EU's AI Act imposes strict requirements around transparency, fairness, and the responsible use of AI in decision-making processes.

(US) Call Center Labor Union

Skan's selective monitoring approach, combined with its group-level analysis, ensures that US labor unions' demands for privacy and transparency are fully respected.

> **Aggregated data analysis**

Focusing on trends and patterns across groups, not individual call recordings or interactions.

> **No personally identifiable information (PII)**

Excluding names, addresses, and other PII from data analysis.

> **Data security measures**

Implementing robust security protocols to protect all data from unauthorized access or misuse.

> **Transparency and collaboration**

Engaging with unions to ensure their concerns are addressed and data is used responsibly

A. Group-Centric Analysis to Align with Global Regulations

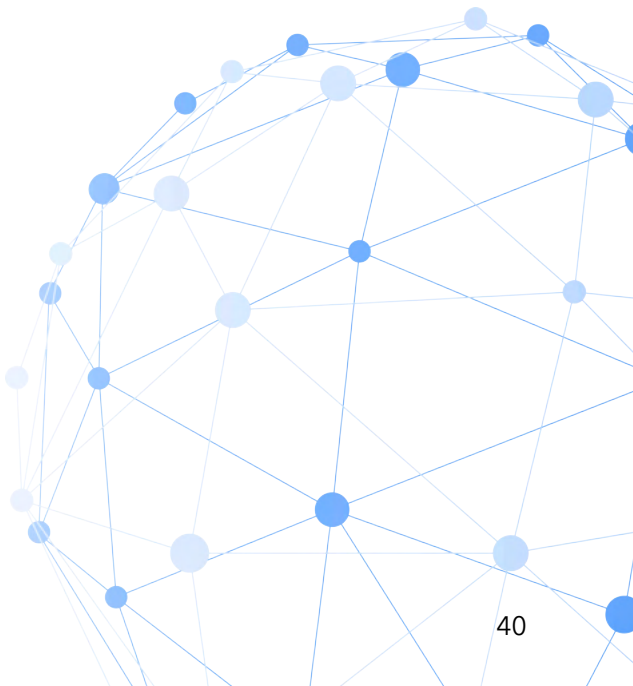
(EU) GDPR (Reg. 2016/679) Compliance

Skan's platform complies with GDPR. Skan acts as a Data Processor and its Enterprise Customers are the Data Controllers.

Key compliance measures include:

1. On-premise behind the firewall Gateway Server deployment.
2. Skan processes only de-identified data, meaning that no personally identifiable information (PII) is stored or analyzed.
3. Skan Cloud deployment within the EU based on the customer's location
4. Customizable retention policies
5. Skan Cloud uses data encryption at rest and in-transit
6. Minimal data collection
7. Customers create inclusion/exclusion application lists before any data is collected
8. Eliminates access to sensitive process images
9. Processes non-personal business application data
10. Retains data only for the period required
11. Keeps data in the same region as that of the customer
12. Secure data disposal practices
13. Ensures AI uses are segregated from other customer environments
14. Maintain procedures to comply with Article 17 of GPR "Right to Erasure"

Example: For a financial services client in Germany, Skan enabled GDPR-compliant data retention policies, ensuring workflow data was stored only for the minimum necessary duration before purging, in line with data minimization principles.



(EU) Working Towards Compliance with the AI Act (EU Reg. 1689/2024)

The EU AI Act sets out strict guidelines for ensuring that AI systems are transparent, non-discriminatory, and ethically used in business processes. Organizations such as Skan have 24 months to comply from August 1, 2024. Skan is working towards compliance by currently employing principles such as :

> **Risk-based approach:**

Skan continually evaluates it AI use cases and takes risk-based actions to sustain secure and compliant handling of AI technologies.

> **Bias Detection and Mitigation:**

The platform includes built-in safeguards to detect and mitigate bias in AI-driven decision-making, ensuring that workflows and business insights are fair and non-discriminatory.

> **AI Transparency:**

Skan provides full transparency into how its algorithms operate, ensuring that businesses can explain AI-driven insights, as required by the AI Act.

> **Human Oversight:**

While Skan provides insight/process intelligence on process exceptions, nuances, and process performance, human operators retain the ability to review or override AI-generated insights, aligning with the AI Act's human-in-the-loop requirements.

Example: For a manufacturing client, Skan provided explainable reports to ensure that any insights related to process optimization were transparent and could be easily audited, fully complying with the AI Act's mandates.

(EU) Worker Monitoring Provisions (Art. 4 Law 300/1970)

The Workers' Statute in Italy restricts how employers can monitor workers, particularly in remote and digital environments. Article 4 mandates that worker monitoring must be limited, consented to, and not infringe on individual privacy.

Compliance: With its application whitelisting feature, Skan ensures compliance with the Workers' Statute by only observing and recording work-related activities, while personal applications and irrelevant actions are excluded. Additionally, Skan's use of de-identified data further safeguards individual privacy, ensuring no personal or sensitive data is collected or stored.

> **Limited Monitoring Scope:**

Only predefined business applications are monitored.

> **Consent Management:**

Skan facilitates transparent communication with worker councils, ensuring that any monitoring aligns with the legal consent frameworks.

> **Anonymized aggregated Insights:**

The system aggregates data at the group level, providing insights into process efficiencies without tracking individuals, fully complying with Italy's monitoring restrictions.

(EU) Worker's Council

The Skan platform was designed to be endorsed by Work Councils in Europe based on the following key components of the Skan platform:

> **Employee data protection:**

Minimal data collection, masking, redaction, anonymization, and white labeling of applications.

> **Job security and workload:**

Furthermore, the implementation of the Skan platform in the EU country restricts analysis and visibility to cohorts rather than individuals. The VA does not interfere with the daily work of the employees and the outcomes are used to improve the Employee Experience and workload.

> **Benefits for Employees:**

The utilization of Process Intelligence helps identify gaps in training, inefficient or ineffective processes, application rationalization, and employees' well-being.

> **Data sovereignty:**

Data stays in the European Union as Skan stores data in the same Microsoft Azure region as the customer.

Consultation, Consent, and Worker Involvement

Skan enables businesses to involve worker councils and unions in the deployment process, ensuring that monitoring is transparent and consensual. The ability to whitelist applications means that workers and unions can agree on what activities are monitored, fostering trust and compliance.

Example: During deployment in Europe, Skan worked with worker representatives to ensure that only relevant business applications were whitelisted, and personal data was de-identified before any analysis occurred, ensuring full compliance with local labor laws.

08 »

CONCLUSION: DRIVING INNOVATION WITH CONFIDENCE

By implementing comprehensive security and privacy measures, Skan provides process intelligence solutions with a focus on security, risk mitigation, and compliance with stringent data protection regulations. This approach ensures transparent security practices and compliance within organizations.

The combination of robust technical safeguards and open communication makes Skan a leader in secure and ethical process intelligence. Our integration of privacy measures with cutting-edge process intelligence demonstrates that operational excellence and data protection can coexist harmoniously. As privacy regulations and concerns evolve, our team remains committed to advancing secure and ethical Process Intelligence.

We invite organizations to harness Skan's technology, confident that their process optimization efforts are supported by stringent privacy safeguards, enabling them to optimize operations without compromising on data security or employee privacy.

Skan AI

LEARN MORE AT

www.skan.ai