GoodData

GoodData Corporation

# Security White Paper

# July 2020

# Table of Contents

This whitepaper is organized into three sections, starting with the executive overview. After the overview, the section titled "GoodData platform security" explains the security measures applied to the GoodData platform and provides guidance for GoodData customers on the security concepts and techniques they should use to ensure security in the cloud.

The section titled "GoodData security overview" is intended for our customers' security, compliance, and risk personnel. This section provides an overview of GoodData's information security management system-built on the ISO 27001 standard-and explains our compliance against the 14 domains of the standard.

# Executive Overview

The GoodData Enterprise Insights platform is designed to help enterprises and independent software vendors (ISVs) securely transform their data into actionable insights and deliver them to business users, customers, and partners at their point of work to drive better business outcomes. GoodData realizes that helping to protect our customer's data, ensure proper security regulations are followed, and mitigate any potential risk is essential to building trust and delivering a high level of service. GoodData takes a risk-based approach to security, and this paper details the measures and technologies in place to protect our customers. It also outlines our internal security compliance standards, so that our customers may be assured about the diligence and robustness of our information security management system.

We adhere to the following certifications, frameworks, and best practices, demonstrating our commitment to data security and privacy:

- SOC 2® - SOC for service organizations: Trust Services Criteria. Since 2013, we have obtained a Type II audit report on an annual basis
- Compliance with the ISO 27001:2013 international standard for information security management systems, adherence to best practices documented in ISO 27002
- HIPAA compliance
- GDPR compliance
- Registered participant in the EU-US and Swiss-US Privacy Shield Frameworks
- A licensee of the TRUSTe® Privacy Program

# Defense in Depth

As you'll see from any best-in-class SaaS provider, there is no single layer that protects customer data. Rather, it is a well-architected solution that considers every layer from the physical security measures at the data center all the way through the access privileges that determine what data an individual user can access. GoodData, as a best-in-class analytics provider, uses this approach to protect customer data.

# Scalable Security Compliance

Security is incorporated into all aspects of GoodData. Our customers and prospects can rely on our Security Shield-an industry standard security compliance package-and request our compliance documentation, such as SOC 2 Type II audit report, ISO 27001.

Statement of Applicability, reports from our third party penetration tests as well as Cloud Security Alliance Consensus Assessment Initiative Questionnaire (CAIQ) for their review.

We offer Enterprise Shield for enterprise customers who require above-standard due diligence or integration of our security compliance KPIs into their processes, for ISVs who have enterprise companies amongst their clients, and for customers who have sensitive data that require robust assurance on the implementation level and a full audit trail to all access to data. This service offering is built on the top of Security Shield and includes all these aforementioned capabilities.

For customers who require HIPAA compliance or processing of special categories of data under GDPR Article 9, we offer add-ons to Enterprise Shield that ensure full compliance as well as execution of the applicable contractual addendums.

## Regional Deployments

Data sovereignty is a complex issue that ranges from the technical to the regulatory to sometimes even the political arena. Understanding the complexities of this issue, GoodData operates data centers in the United States to serve the US and most other North American companies, in Canada to serve those who require storing their data in the Canadian area, and in the United Kingdom to support customers in the European Union.

# GoodData Platform Security

## Application Security

The GoodData platform doesn't just provide customers with the ability to access their reports, dashboards, and data, but it also enables integration of the Enterprise Insights platform directly with our customers' other software so they can provide their clients with a seamless experience. The GoodData application employs many security measures to enable the secure flow of data from when it is loaded into the Enterprise Insights platform through to delivery to workspaces for end-user consumption.

**Integration and APIs**
Any integration with the GoodData application programmatic interface (API) leverages HTTPS/TLS encryption. The user security model is enforced at the API level, providing that data retrieved with the API is still subject to user authentication and access privileges (see user security section below).

**Agile Data Warehousing Service**
Agile data warehousing service, or ADS (also known as "data Warehouse"), is a fully managed, columnar data warehousing service for the GoodData platform. GoodData customers' administrators may access the warehouse using a customized, secure JDBC interface.

Data stored in ADS is encrypted at rest, leveraging either AES-256 or proprietary FIPS-certified HPE Secure Encryption™.

**Workspaces**
Users added to the GoodData Enterprise Insights platform are not given broad access to the network but to an explicit workspace that is assigned to a "consumer" site. This ensures that users only have access to the workspaces appropriate for them.

Data in the data mart databases supporting the workspace is stored on file systems that are encrypted at rest, leveraging either AES-256 or proprietary FIPS-certified HPE Secure Encryption™. All customer workspaces are backed up on a daily basis and maintained in line with progressive backup retention policy.

**User access**
End users may access the data only through the application layer. Whether this access is through the user interfaces or through the publicly available API, it enforces user access controls to limit access to customer data only to authorized users and personnel.

As such, GoodData does not provide end users with direct access to any database. This approach prevents unauthorized services or systems from accidentally or maliciously retrieving or modifying customer data.

## User Security

User security is enforced via a variety of security measures that allow authorized users to view only the strictly defined set of objects and data that enable the user to access to the analytics they need to perform their job.

### Authentication

GoodData's architecture relies on a centralized authentication and authorization security framework to control access to services. The security framework enables the enforcement of security policies by requiring password strength, algorithms to set minimum password length and complexity, and progressive timeout on the login API to mitigate the risks related to password-guessing attacks. Customers may also choose to implement single-sign-on (SSO) with their own access policies (e.g., whitelisting, multi factor, etc.) to integrate and enforce user authentication within their own identity management system (e.g., active directory).

### Role-based access control (RBAC)

The GoodData Enterprise Insights platform supports enterprises and ISVs as they define the user roles that control which objects and capabilities within the Enterprise Insights platform a user will have access to.

> For example, if a customer has implemented a loan insights solution, an account manager may be granted a role that allows access to a client health dashboard, while a regional sales VP may be granted a role that allows access to both the client health dashboard and a loan pipeline dashboard.

### IP whitelisting

IP whitelisting is an additional security measure. This feature should be used to limit and control access based on a list of defined IP addresses or address ranges from which users can access the customer's GoodData domains.

Some scenarios under which customers might benefit from IP whitelisting include:

- Ensuring that administrative access, including access to the ADS, is restricted only to a trusted company network
- Enforcing change control to all changes to ETLs by allowing deployment of ETLs only to a trusted deployment system
- Implementing a custom access control policy that prevents end users from accessing data from non-trusted networks

### User session expiration

User session expiration allows you to specify a period of inactivity after which user sessions are terminated and users are automatically logged out of the GoodData platform. We recommend aligning the user session expiration with the session expirations for the rest of the customer solution in which the GoodData platform is integrated. Session expiration should be also customized to match customer access control policies in all deployments using Enterprise Shield or containing sensitive data.

### Platform event auditing

Customers with the Enterprise Shield package may use the platform event auditing API, which provides a real-time feed of platform security events such as user log-in attempts, user profile changes, and data access. All of this is delivered in an industry-standard form that is easy to integrate into a customer's SIEM for security monitoring and alerts sent to their users in GoodData platform.

# Data Security

Data security is that final layer of security that limits access to the GoodData Enterprise Insights platform based on permissions that each user has. GoodData employs several redundant layers of data security for the safety of our customer's data.

**Data-based access control (DBAC)**

The GoodData Enterprise Insights platform supports enterprises and ISVs by restricting query results based on a user's pre-defined permissions.

> For example, a customer may implement data-based access controls on a sales insights solution for individual sales reps and sales managers. On a quarterly sales recommendations view, sales managers' queries will be unrestricted so they can assess quarterly sales across their business, but the same dashboard for individual sales reps will only query data rows specific to their personal sales results..

**Segmented/isolated data mart**

The GoodData Enterprise Insights platform, as the name suggests, is intended to securely deliver insights from a publisher to one or more enterprise sites, each site having one or more users.

To organize each site and its users so that each has access to only the data intended for that subset, the data is distributed to a dedicated and isolated data mart to support the workspace for that consumer site. This physical security measure is in addition to the logical RBAC and DBAC security measures.

# GoodData security overview

## Information security policies

GoodData has established a comprehensive set of information security policies, processes, and standards. Our information security management system is based on the international standard ISO 27001:2013, and we are building our security procedures and standards upon the National Institute of Standards and Technology's (NIST's) Special Publication (SP) 800 series.

Our policies are owned and approved by appropriate senior management owners, communicated to affected internal and external personnel, and reviewed on an annual basis or ad hoc in case of a significant business change to ensure ongoing suitability, adequacy, and effectiveness.

# Organization of information security

GoodData has appointed a dedicated information security organization led by the chief information security officer (CISO), who has the executive responsibility for information security across the corporation and leads the security and compliance department.

The CISO also chairs the GoodData Security Council, a cross-functional group established for ongoing oversight of the GoodData information security program, both from a design and an effectiveness point of view.

The council's senior roles bring together a wide range of perspectives, ensure efficiency of the security program, and, last but not least, reinforce that information security is a business issue with involvement across the corporation, not only an isolated issue of for engineering and IT. The council meets on a monthly basis to review security events and issues, discuss open and emerging security risks, and to otherwise ensure ongoing alignment between security and business objectives.

All new features and capabilities, from the development of a simple pluggable visualization to the building of a new data center, are managed as projects with the input of a security architect to maintain the integrity of security measures across all components. To ensure that security is built into all aspects of the GoodData platform, the GoodData engineering team follows DevSecOps methodology. Our software engineers and operations staff are trained on secure development practices and use a wide range of technical means, which are built directly into the continuous integration infrastructure, to address risks related to code flaws and vulnerabilities as well as to prevent promotion of changes without proper review and approval.

GoodData's security and compliance department, together with the internal legal team, monitors the global regulatory landscape to identify emerging data security and privacy-related laws, standards, and regulations and ensure customer data is protected accordingly.

## Human resources security

All new employees around the world are subject to an industry standard background check. GoodData has established three levels of a security clearance; the highest level, which has the most demanding background check requirements and which has to be regularly renewed, is mandatory for all key security-related roles as well as for personnel with the highest level of administrative access to the GoodData platform and critical internal systems.

Contractual agreements include confidentiality clauses as well as the responsibilities for information security and ensure that the relevant employee responsibilities (including the non-disclosure clauses) remain valid after job termination.

Management is responsible for security compliance in their areas of business. Documented job descriptions further outline specific security-related rights and responsibilities for all roles.

All internal and external employees must complete security awareness training as part of their onboarding and then on an annual basis. There is additional role-specific mandatory training for employees who need to access data that is subject to regulatory protection such as HIPAA or GDPR.

GoodData has an established disciplinary process. Management reviews all compliance violations, and sanctions are taken in the event of high-risk violations. All employees have to sign an acknowledgment of the possible consequences of policy violations, which include loss of access, employment termination, and/or criminal prosecution.

## Asset management

GoodData maintains inventories of relevant IT assets and has established responsibilities and assigned ownership. Our internal data classification policy defines five levels of data classification as well as mandatory data protection requirements on systems that process particularly classified data.

Customer data has the two highest levels of protection and are classified as either "restricted" or, in the case of data subject to strict regulatory requirements such as ePHI under HIPAA or special categories of data under GDPR, as "highly restricted."

All internal systems, as well as GoodData platform components, are labeled in line with data classification rules to ensure enforcement of adequate data protection.

Procedures for handling of restricted and highly restricted customer data are documented, communicated to all personnel with access to such data, and strictly enforced. GoodData personnel never access customer data without proper business justification and procedures, and technical safeguards ensure that customer data is never stored outside of the GoodData platform. GoodData does not use customer data for development purposes, and if there is a strong need to use production data for testing purposes, then a dedicated production-like environment with strong security safeguards, strict access control, and formal change management rules is available. As a policy rule, customer data is never loaded to removable media.

Following the end of a customer contract, GoodData implements a documented procedure to ensure that all customer data is properly removed and, if applicable, the media sanitized and/or securely disposed of. Upon written request, the GoodData security team will provide written attestation of data deletion.

GoodData employee laptops and BYODs follow strict security rules; centralized monitoring is established to ensure ongoing compliance. All MacOS- and Windows-based laptops are equipped with centrally managed antivirus protection. All laptops are protected by firewall, and hard drives are fully encrypted. Acceptable use rules are documented and communicated to all employees.

Upon termination of employment, laptops are collected and wiped before reuse, and BYODs are de-authorized from company systems. Whenever possible, remote wipe is enabled and triggered upon the report of a lost or stolen device.

## Access Control

GoodData has implemented access control policy and enforcing mechanisms which comply with industry best practices. The rules are applied across all internal systems and the GoodData platform to ensure that only authorized users with proper business justification have access to internal and customer data. We enforce the principle of least privilege for all systems with data classified as confidential, restricted, or highly restricted.

We apply industry standard password policies, and, whenever possible, we use single sign-on for access to internal company systems. Two-factor authentication is enforced for administrative access to the GoodData platform and key internal systems. We review access entitlements across all company systems on an annual basis at minimum.

Before being granted privileged access, employees must complete the security training as well as role-specific training related to their access. Based on the sensitivity of access, security clearance level 2 or 3 is mandated (security clearance level 1 is mandatory for all employees). The CISO reviews and approves all requests for privileged access, and we monitor ongoing business justification and review all privileged access entitlement and usage on a quarterly basis.

For details around end user access control, please refer to GoodData platform security.

## Encryption and Cryptography

GoodData uses state-of-the-art cryptography technology to achieve protection of data in transit and at rest and has documented cryptographic policy and standards.

All traffic outside of our data center is encrypted; we use TLS 1.2 and AES-256 by default. While we support some of the legacy protocols and cipher suites for compatibility reasons, we systematically deprecate older versions and disable those that have known weaknesses. Our servers enforce HSTS and offer forward secrecy as well as a strong key exchange.

The entire platform infrastructure is encrypted at rest on the file system level. Depending on the environment and underlying hardware, we use either AES-256 or proprietary FIPS-certified HPE Secure Encryption™.

Backups stored outside of our primary data center are encrypted using AES-256-based symmetric cryptography on the client side before being stored in the off-site, encrypted at-rest file system.

For passwords, we use glibc crypt(3) SHA-2-based scheme with an increased number of rounds to mitigate offline password cracking attacks. Administrative sessions are protected via SSH protocol.

## Physical and Environmental Security

Best-in-class providers host GoodData data centers. Rackspace, Inc. operates our US and EU datacenters, and Zayo, Inc. operates the datacenter in Canada in a facility provided by Equinix.

We also use some services provided by AWS, Inc., including S3 storage (off-site data backups and data exchange), EC2 (disaster recovery), and Spark (machine learning) for business continuity and disaster recovery purposes as well as a simple common data exchange platform and for some data transformation scenarios.

The data center providers have obtained a wide range of security certifications and compliance standards, including ISO 27001:2013, SOC 2 Type II, PCI-DSS, HIPAA, and GDPR. GoodData personnel review their audit reports and certificates on an annual basis to ensure ongoing compliance with GoodData physical security requirements.

These data centers also feature at least N+1 redundant HVAC and UPS, diesel-powered generators, and multiple internet connections by independent Tier-1 providers. The physical security adheres to the best practices in the industry and include:

- Keycard protocols, biometric scanning protocols, and round-the-clock interior and exterior surveillance
- Access limited to authorized data center personnel-no one can enter the production area without prior clearance and appropriate escort
- Assurance that every data center employee undergoes thorough background security checks

All infrastructure used by GoodData is under full control of our operations personnel; the vendor provides hardware maintenance only. All devices behind our edge router are used solely by GoodData and are not shared with other customers of the hosting provider. We require that all decommissioned hardware be securely disposed of and that industry standard media wiping procedures are applied in line with NIST SP 800-88 requirements.

Even though we are a cloud company and do not host any data internally, GoodData protects its offices by industry standard means including keycards and CCTVs; all visitors must sign an NDA and must be accompanied by GoodData personnel at all times. We implemented a clean desk and clear screen policy to address risks related to undesired exposure of sensitive information to external parties, and we train our employees on security while working remotely or during travel.

# Operations Security

A formal change control process minimizes the risk associated with system changes. The process enables tracking of changes made to the systems and verifies that risks have been assessed, interdependencies explored, and necessary policies and procedures considered and applied before any change is authorized.

The production environment may be accessed only by authorized personnel and when adequately justified by business needs. Operations personnel have administrative access only to the subcluster they are responsible for, and all access is fully logged. Access to the infrastructure is controlled via a separate network which is physically isolated from the GoodData corporate network. This ensures that only personnel authorized to access the data center may do so.

A limited number of key personnel have "super admin" access to the entire platform, which they may use in emergencies. Such access triggers an alert for immediate independent review. Privileged session logs are subject to periodic internal audit.

Development, testing, and production environments are strictly separated both on the logical access level and on the network level to reduce risks related to unauthorized or unexpected changes to the production environment.

The GoodData platform is protected both internally and externally by firewalls and security groups. GoodData deploys host-based intrusion detection systems as well as a variety of network-level controls to detect attempts for unauthorized access or circumvention of security controls. We use industry standard hardening procedures including installation of only the minimum software necessary, changing default system passwords or disabling implicitly created accounts, and making sure that firewalls let through only explicitly allowed traffic.

We apply infrastructure-as-a-code and configuration-as-a-code principles to ensure consistent application of our security standards as well as for in-time monitoring and alerts in case of unintended or unauthorized changes.

The entire production infrastructure, as well as all platform components, is monitored, and alerts are addressed by operations personnel 24x7x365. The platform team is responsible for capacity monitoring and planning to ensure the timely provision of new hardware as our customers' usage of the platform grows.

The log management system is set up in line with NIST SP 800-92 recommendations. Logs are securely transferred to the centralized log management system and protected from unauthorized access. All systems have synchronized clocks via NTP. Logs are available for 90 days in a SIEM and then for a year in secure offline storage.

We have established an industry standard patch and vulnerability management procedures. Our operations personnel monitor relevant security groups, upstream software providers, as well as hardware vendors for patch and vulnerability notices, and we have defined SLAs for remediation. Critical patches are handled via incident management procedures. Compliance with SLAs is monitored by the service delivery function and is reviewed by management on a monthly basis.

# Network Security

GoodData platform servers are allocated to the respective security groups, characterized by specific security settings (TCP/IP level), and supplemented by individual instance-level stateful firewalls. Separate VLANs are used to split production, testing, and development environments, as well as to segregate end-user and administrative traffic.

All network access to the virtual hosts is protected by a multi-layered firewall operating in a deny-all mode. Internet access is only permitted on explicitly opened ports for only a subset of specified virtual hosts. A separate set of firewall rules manage access to database instances within the internal environment.

GoodData employs a three-tier security model:

- Web servers at the frontline
- Application servers in the demilitarized zone
- Database servers behind an additional firewall

Consistent with our DevSecOps approach, we maintain a configuration-as-a-code approach for network security and firewall rules and have alerts for any discrepancies between the approved configuration and production settings.

## System Development, Maintenance, and Acquisition

We follow industry standard secure development life cycle practices. A formal change control process minimizes the risks associated with system changes. The process enables tracking of changes made to the systems and verifies that risks have been assessed, interdependencies explored, and necessary policies and procedures considered and applied before any code change is formally authorized. We have integrated static and dynamic security testing in our CI/CD infrastructure, and peer code review includes secure development considerations.

Development of new platform features follows agile project management principles. Security architecture considerations are part of all architecture design and reviews. Before we roll-out new platform features to production, we review the implementation against design, and for new or significantly modified components, we also execute external penetration tests.

## Vendor management

All vendors with access to the GoodData platform are rigorously reviewed for security and compliance practices, and we have contractual arrangements in place to ensure their ongoing compliance with our security requirements. We review the contractual performance of all vendors annually.

## Security Incident Management

GoodData has established an industry standard security incident response plan. We train our staff to ensure all potential security incidents are identified and reported in a timely manner. Our security operations team is on call 24x7x365, and we have defined protocols and escalation trees for the handling of security incidents and, when required by the nature of the incident and applicable contractual commitments and regulatory requirements, for the notification of the affected parties as well as the authorities. Procedures for collection of evidence ensure chain of custody.

Following the resolution of a security incident, the GoodData security team conducts root cause analysis and, if applicable, implements changes to its technology and procedures to prevent regressions.

# Business Continuity and Disaster Recovery

To achieve the committed platform availability SLA and reduce the impact of failures, GoodData applies high-availability architecture principles on the software and hardware level and ensures its data center providers have adequate redundancies in the infrastructure.

We store all customer workspace backups on a daily basis and move them regularly to a secure, highly available, and durable off-site storage. Our disaster recovery plan addresses major disruptions to GoodData facilities, key internal systems, and the GoodData platform, and we can restore production operations in the public cloud or at another company data center. We test our disaster recovery plan on an annual basis.

# Compliance

GoodData complies with a variety of data protection standards. We have obtained SOC 2 Type II audit report, maintain compliance with the ISO 27000 standards family, and build our security practices upon industry standards, including applicable NIST, OWASP, and Cloud Security Alliance standards and recommendations.

We have policies and procedures to ensure appropriate protection of PII and personal data both in the platform and as part of our business operations. Our platform allows for processing of ePHI under HIPAA, we comply with GDPR, and we offer signing data processing agreements with our customers.

We monitor the emerging legislation and standards to maintain compliance and achieve best-in-class security of our platform.

We continuously monitor and regularly review and audit our security compliance. We do this on the policy and on the technical level both internally and by using external penetration and vulnerability testing providers and auditors.

On an annual basis, external reputable penetration testers conduct a comprehensive penetration test of the complete GoodData platform API set. The entire GoodData infrastructure (including GoodData's office network) is subject to quarterly "weakest link" penetration tests and vulnerability scans. We partner with two different penetration and vulnerability test providers who alternate on the different test types to achieve above-standard coverage and depth of testing.

# Conclusion

Here at GoodData, we pride ourselves on the vigilance we employ to protect our customers' data assets, and we continually stress that a mature security organization requires coordinated dedication across technology, policy, procedures, and people. This dedication is underscored by the risk-based approach laid out in this document to demonstrate strength at every layer of security, minimizing any potential vulnerability or weakness.

We want our customers to know their data is adequately protected by this approach, and we welcome the opportunity to discuss these practices and approaches further.

We also encourage customers to consider the criticality and sensitivity of their usage of the GoodData platform and, in line with the recommendations provided in this whitepaper, to implement adequate technical and administrative safeguards to achieve the desired level of security. The GoodData security team is looking forward to assisting with the implementation.