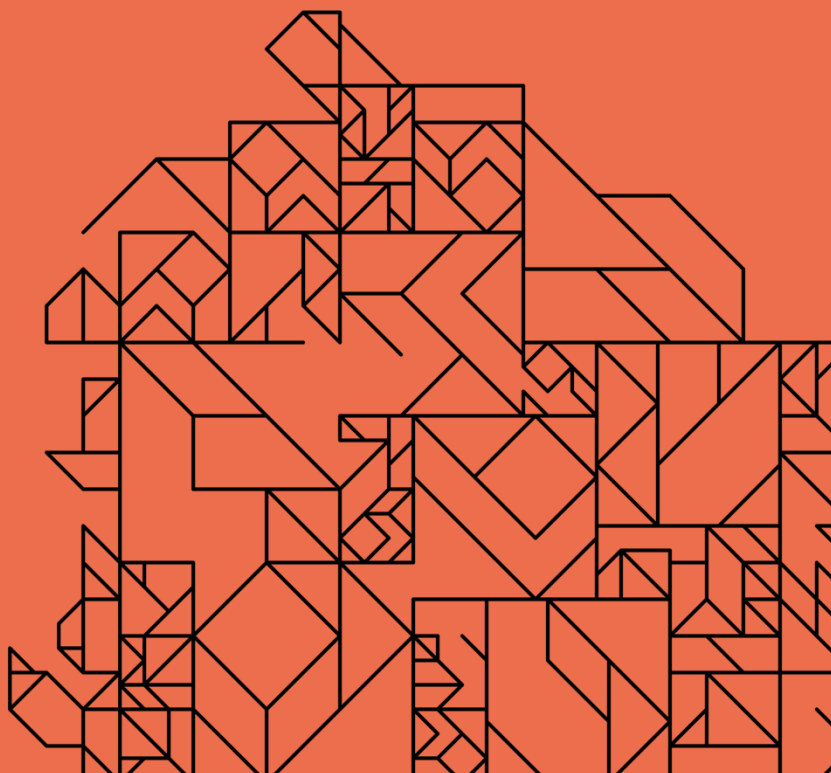
DataTako

Security & Trust Overview



DataTako

V2.1 – May 13th, 2025

Introduction

Datatako is a SaaS platform enabling users to **share Power BI reports securely** with external stakeholders without requiring individual Power BI Pro licenses. We recognize that protecting customer data and mitigating risks is essential for building trust. Security isn't an afterthought for Datatako—it's built into our product and operations from day one. We follow a multi-layered "defense-in-depth" approach, considering every layer from physical data center security to user access privileges. Notably, Datatako's architecture stores only report metadata and access permissions**,** never the report data itself**.** This data minimization significantly reduces our attack surface and compliance burden. Technical decision-makers (CIOs, CTOs, CISOs) will find that Datatako's security program aligns with industry best practices and is designed to meet the stringent requirements of enterprises and regulated industries.

Key Security Features at a Glance:

- **SSO & 2FA:** Single Sign-On with Microsoft Azure AD accounts, with configurable mandatory two-factor authentication for all user logins (meeting the needs of finance, healthcare, government sectors that require 2FA).
- **Data Minimization: No customer report content or source data is stored** on our servers – only metadata and user access info are retained. Your sensitive data remains in your Microsoft Power BI environment, which is secured and compliant with standards like **ISO 27001, ISO 27018, HIPAA, and EU Model Clauses** under Microsoft's Trust Center.
- **Encryption Everywhere:** All sensitive data is encrypted **at rest and in transit**. Datatako uses strong encryption (AES-256 for data at rest, TLS 1.2+ for data in transit) to protect customer information.
- **Granular Access Control:** Robust role-based access controls and the **principle of least privilege** ensure users (and Datatako staff) have only the minimum access required. Fine-grained controls (including support for Power BI's Row-Level Security) guarantee that report viewers see **only the data they are authorized** to see.
- **Operational Security:** Strict internal security policies – background checks and security training for all employees, administrative access tightly restricted and **protected by MFA**. Continuous monitoring, alerting, and incident response processes are in place to rapidly detect and respond to threats.
- **Future Compliance & Certification:** We are committed to formalizing our security program with certifications like **ISO 27001** (planned) and **SOC 2**. We already comply with **GDPR** and are prepared to support **HIPAA** requirements via Business Associate Agreements, leveraging the compliance of Microsoft Azure/Power BI. (See the *Compliance & Certifications* section below for details.)

Platform Architecture & Data Handling

App-Owns-Data Model: Datatako leverages Microsoft's **Power BI Embedded (App Owns Data) (**https://learn.microsoft.com/en-us/javascript/api/overview/powerbi/embedding-solutions**)** architecture to deliver reports. In this model, Datatako's service authenticates to Power BI through a secure Azure App Registration and retrieves an **embed token** for the

report. This design means that **the underlying data and visuals remain within Microsoft's Power BI service** – Datatako does not cache or store the report's data. All report queries and rendering are executed by the Power BI service in real-time when a viewer accesses a report. The embed tokens we use are **encrypted and signed by Power BI**, and they encode precise security policies (per-report access rights, row-level security filters, etc.). End users' browsers receive these tokens and content directly from Power BI; they cannot modify the tokens or access data beyond what the token permits. This architecture ensures that your data never leaves the trusted Microsoft cloud environment during report viewing.

Data Isolation & Row-Level Security: For multi-tenant scenarios, Datatako supports **strict separation of each customer's data**. Depending on your implementation, we can either use **Power BI's dynamic Row-Level Security (RLS)** to filter data per viewer or isolate data by using separate Power BI workspaces for each client organization. RLS enforcement means each user only sees the rows of data they're entitled to, even if using a shared dataset. In cases of enterprise deployments, each client's reports and metadata can reside in distinct workspaces, ensuring no cross-tenant data leakage. All access policies defined in Power BI (including any Object-Level Security on sensitive columns or tables) remain in full effect when reports are viewed through Datatako.

Minimal Data Storage: By design, Datatako **stores only minimal metadata** – e.g. report IDs, titles, and the mapping of which users have access to which reports. **No actual report data or query results are persisted** on our side. This minimalistic data handling greatly reduces the risk and compliance scope for our customers. In essence, Datatako acts as a secure conduit to Power BI, not a data repository. Your data remains under Microsoft's robust security controls (Power BI is certified for **ISO 27001, ISO 27018, HIPAA BAA, UK G-Cloud, etc.** as per Microsoft's Trust Center).

Data Security & Encryption

We employ strong encryption and data protection measures to safeguard the information entrusted to Datatako (however limited it may be). Our data security controls align with industry best practices and regulatory expectations:

- **Encryption at Rest:** All sensitive data managed by Datatako (such as stored metadata, user information, API keys or embed tokens) is **encrypted at rest** using advanced ciphers (AES-256 or better). We use FIPS 140-2 validated cryptographic modules to ensure compliance with government-grade standards. This means that even if physical storage media were accessed, the data would be unintelligible without the proper decryption keys. Encryption keys are securely managed (utilizing cloud key management services with tight access controls and regular key rotation policies).
- **Encryption in Transit: All network communication** between users, Datatako, and Microsoft's Power BI service is protected via **TLS 1.2+** encryption. We force HTTPS for all interactions – there are no insecure HTTP endpoints. This TLS encryption (with modern ciphers) guards against eavesdropping or man-in-the-middle attacks, ensuring that report data, embed tokens, and user credentials cannot be intercepted in transit. Our TLS configuration follows industry recommendations (SSL Labs A+ standards) and is updated as new security protocols become available.

- **Isolated Data Storage:** The limited data that Datatako does store (account metadata and access permissions) is segregated per tenant in our databases. We leverage logical separation mechanisms so that one customer's metadata is never accessible to another. Each customer organization has its own context within our multi-tenant database, enforced by application logic and strict authorization checks. This approach is similar to how leading SaaS platforms allocate a dedicated environment or schema for each tenant. In addition, our production database is accessible only to the application and a few tightly controlled admin accounts – direct queries or cross-tenant access are not permitted.
- **Backups & Retention:** We perform regular backups of critical metadata (e.g., daily encrypted backups of our database) to guard against data loss. Backup files are encrypted and stored in secure, access-controlled locations. We retain data only as long as necessary to provide the service; if a customer leaves the platform, we can purge their metadata upon request in accordance with our data retention policy. This ensures we are not holding data longer than needed, which aligns with privacy principles.
- **Data Center & Cloud Security:** Datatako is hosted on a reputable cloud platform (built on Microsoft Azure), inheriting the physical and environmental security of Microsoft's data centers. These facilities feature 24/7 guarded premises, biometric access controls, redundant power and cooling, and certified processes (ISO 27001, SOC 1/2/3). Our infrastructure is contained within a **virtual private cloud/network**, with strict network security groups and firewall rules controlling inbound and outbound traffic. Only the necessary ports/protocols are open to the internet (e.g., HTTPS), and internal components communicate over private, encrypted channels. This isolation helps prevent any unauthorized network access to databases or servers holding customer metadata.

Identity & Access Management

Proper authentication and authorization are cornerstones of Datatako's security, ensuring that only the right individuals can access reports and that they only see what they're permitted to. Our identity and access management practices include:

- **Single Sign-On (SSO) via Azure AD:** Datatako integrates with **Microsoft Azure Active Directory** for user authentication. Users sign in with their existing Microsoft 365 (Work or School) accounts – no separate Datatako-specific password is required. This SSO approach centralizes identity management and lets organizations enforce their own security policies (like password complexity, account lifecycle, and MFA) through Azure AD.
- **Mandatory Two-Factor Authentication: Two-factor authentication (2FA)** is **required** for all logins to Datatako. When users authenticate via Azure AD, they must pass a second verification step (e.g., an Authenticator app push or SMS/Call as configured in their Microsoft account). This dramatically improves account security by adding an extra layer beyond just a password. Notably, 2FA is considered essential in high-risk industries; sectors like finance, healthcare, and government *require or strongly encourage* 2FA for system access. By enforcing 2FA platform-wide, Datatako aligns with these best practices and compliance requirements.

- **Role-Based Access Control (RBAC):** Datatako employs RBAC to ensure users only have the permissions necessary for their role. Within the Datatako application, roles might include (for example) **Administrators**, who can configure connections and manage users, versus **Report Viewers** who can only view assigned reports. Each role's capabilities are clearly defined, and we default to the **least privilege principle**: users are given the lowest level of access that allows them to perform their work. For instance, an external report viewer would have no ability to see or modify another organization's data or settings. Permissions to share or administer reports are limited to authorized roles. All access requests within the app are checked server-side to prevent privilege escalation.
- **Power BI Security Integration:** Because Datatako leverages Power BI, we also honor any security controls set at the Power BI level. If your reports utilize **Row-Level Security (RLS)** or define specific audience access within Power BI, those restrictions carry through to Datatako's embedded view. A user who is not granted access to a particular report (or particular data within a report) in Power BI will not be able to access it via Datatako either. In effect, Datatako acts as an extension of your existing Power BI access model, not a bypass of it. This integration gives you confidence that **no one can see data in Datatako that they couldn't see in your direct Power BI service**.
- **Session Management & Device Security:** We implement secure session management – user sessions are tied to tokens with short lifetimes and are invalidated on logout. We use HTTP-only, secure cookies for session tokens when applicable, and tokens are scoped to the minimal privileges (OAuth scopes) necessary. Administrators can review active user sessions and force logouts if a device is lost or compromised. Azure AD Conditional Access policies (if configured in your tenant) can also be applied, for example requiring login only from managed devices or certain IP ranges – these policies will apply to Datatako since login is via Azure AD.
- **Administrative Access Controls:** On the backend, **only a very limited number of Datatako engineers/admins have access to production systems** or customer metadata, and even then, only for legitimate operational needs. All staff access to sensitive systems requires MFA and is logged. We have separate roles for our support personnel (who may assist customers but have no access to change core security settings) vs. system administrators. Administrative actions (like granting user access or changing system configurations) are tracked via audit logs, and we review these logs to ensure no unauthorized access is occurring. Our internal access policies ensure that **no single individual** can unilaterally make privilege changes without oversight.

Application & Infrastructure Security

Datatako's platform is built following secure software development practices and is deployed on hardened infrastructure. Key aspects of our application and infrastructure security include:

- **Secure SDLC & Code Quality:** We integrate security into our Software Development Life Cycle. Developers are trained in secure coding (avoiding common vulnerabilities like SQL injection, XSS, etc.), and we employ **code reviews** and automated **static analysis** to catch security issues before deployment. Dependencies and libraries are kept up-to-date to patch known vulnerabilities promptly. We periodically run **dynamic**

application security testing (DAST) on our running application to simulate attacks and ensure resilience against the OWASP Top 10 risks. Any vulnerability identified is tracked to closure with high priority.

- **Cloud Infrastructure Hardening:** Our cloud environment (in Azure) is configured according to industry benchmarks. We use hardened virtual machine images, restrict administrative ports, and apply the principle of least privilege at the infrastructure level as well. For example, our application servers run under least-privilege service accounts; they only have access to the specific resources (databases, storage) needed. We utilize Azure Security Center recommendations for continuous hardening. All secrets (API keys, database credentials) are stored in **Azure Key Vault** or an equivalent secret management service, never in plain text in code or config. Keys and certificates are rotated regularly.
- **Network Security & Firewalls:** We deploy multiple layers of network defense. A web application firewall (WAF) fronts the Datatako application, filtering malicious traffic (e.g., SQL injection attempts or DDoS patterns) before it reaches our servers. Internal communication between components is on a private network segment – our database is not exposed to the internet at all. We also implement **intrusion detection and prevention systems (IDS/IPS)** that monitor network traffic in real time, alert on suspicious activity, and can actively block attacks. These systems, combined with continuous log monitoring, allow us to detect anomalies such as brute-force attempts or unusual data access patterns.
- **Endpoint Security:** The devices and endpoints used by Datatako's engineering team to manage the service are secured. We enforce security configurations on employee laptops/servers: full-disk encryption, antivirus/EDR solutions, and strict access controls. Administrative consoles can only be accessed through secure, authenticated channels – for instance, developers must use a VPN or privileged access workstation to reach production, ensuring that even if a device were compromised, an attacker cannot directly access Datatako's infrastructure.
- **High Availability & Continuity:** Although availability is not security per se, it's a critical part of trust. Datatako's architecture is designed for high uptime and resilience. We deploy across redundant servers and availability zones to avoid single points of failure. Our data storage has point-in-time recovery and backups (as noted in *Data Security* above). In the event of any incident (security or otherwise), we have a **disaster recovery plan** to restore services quickly. This ensures that even under adverse events, your ability to access your reports is protected.

By following these practices, we minimize vulnerabilities in our application and ensure that the infrastructure running Datatako is robust against attacks.

Operational Security & Employee Practices

Security is not only about technology – it's also about the people and processes behind the platform. Datatako maintains strict operational security controls to prevent insider threats or human error, which is especially important when working with enterprise and regulated customers. Here are some of the measures in place:

- **Employee Vetting & Training:** Every Datatako employee undergoes a thorough **background check** as part of our hiring process. We verify candidates' employment history and perform criminal background screenings in accordance with local laws. This helps ensure we hire trustworthy individuals. Once on board, all employees receive comprehensive **security awareness training** covering topics such as data privacy, secure handling of customer information, phishing prevention, and our internal security policies. New hires must agree to our Code of Conduct and security policies, affirming their responsibility to protect customer data. We also conduct regular refresher training so that our team stays vigilant against emerging threats.
- **Least Privilege for Staff:** Datatako enforces strict **access controls for internal systems**. Staff are given access only to the systems and data needed for their role – no more. For example, a support engineer may have the ability to view diagnostic logs for troubleshooting, but not the ability to query or export customer metadata. Administrative privileges are highly restricted to a small ops team. Even within that team, we segregate duties (the principle of segregation of duties) so that no one individual can make critical changes alone. **No one at Datatako (except the few authorized admins) can access customer report content**, because that content resides in Power BI, not in our environment. And those admins who can access our systems must use individualized accounts with MFA, and all their actions are logged for review. This tight control is aligned with the principle that *no one should have more access than necessary*.
- **Monitoring of Internal Access:** We log and monitor all access to sensitive systems. Anytime an administrator accesses the production environment or views/modifies sensitive data, an audit log entry is generated. We employ automated alerts – for instance, if an admin account were used at an unusual time or from an unusual location, or if it attempted to perform a disallowed action, our security team would be notified immediately. Regular access reviews are performed: each quarter we review all admin accounts and permissions to ensure they are up-to-date and that no permissions exist beyond what's needed. Dormant accounts or unnecessary privileges are removed promptly.
- **Vendor and Third-Party Risk Management:** Datatako carefully manages any third-party services we use. All critical service providers (for hosting, monitoring, etc.) are vetted to ensure they meet stringent security standards comparable to our own. We maintain a list of sub-processors and ensure they uphold commitments like data encryption and confidentiality. For example, any payment processing (for subscription billing) is handled by a **PCI DSS-certified** payment provider – we do not store credit card info on our systems. We also require that any vendors we use have GDPR-compliant data handling and, if applicable, sign Data Processing Agreements. This way, our supply chain of services does not become a weak link.
- **Incident Response Preparedness:** Our team has defined procedures for responding to security incidents. We have an Incident Response Plan that outlines steps for triage, containment, eradication, recovery, and communication. Key personnel are trained on these procedures. We also run periodic incident response drills (simulated breach scenarios) to ensure we can react quickly and effectively in a real event. If an incident were to impact customers' data or services, we are prepared to notify affected customers promptly and transparently, in line with regulatory requirements (e.g.,

GDPR's 72-hour breach notification rule). Our goal is to prevent incidents, but also to be ready to minimize damage and inform stakeholders should one occur.

Our operational security measures ensure that trustworthy people and well-defined processes form a strong last line of defense. By minimizing human-factor risks, we build additional confidence for customers in highly regulated fields where insider threats and process lapses are a major concern.

Monitoring, Auditing & Incident Response

Datatako employs robust monitoring and auditing across our systems to detect issues early and provide accountability. In addition, we have a well-defined incident response strategy. This ensures that if something goes wrong, we know about it quickly and can respond decisively. Key facets include:

- **Security Monitoring & Alerting:** We maintain 24/7 monitoring of our production environment. Logs from servers, authentication systems, firewalls, and applications are aggregated in real time to a centralized logging system. We utilize a Security Information and Event Management (SIEM) platform that correlates events and raises alerts on suspicious patterns. For example, multiple failed login attempts, unusual admin activities, or anomalies in data access all trigger alerts. We also employ **intrusion detection systems** that watch network traffic and host behavior for signs of compromise. If any **suspicious activity** is detected – such as an unrecognized device trying to access the backend, or an unusual spike in data export – our on-call security staff are notified immediately (we have personnel available around the clock to respond). This continuous monitoring means we're poised to catch and stop malicious activity early.
- **Audit Logging:** Nearly every important action in Datatako is recorded in audit logs. This includes user activities (logins, report access, sharing actions) and administrative actions (permission changes, configuration updates). These logs are immutable and are regularly reviewed. We provide customers the ability to get audit logs of their own users' activities (so you can integrate it into your own SIEM or monitoring processes if desired). Internally, audit logs are a cornerstone of our oversight; they allow us to forensicly reconstruct events if needed and ensure that all access to data is traceable. For example, if a customer ever had a question about "who accessed this report and when," we could provide a reliable audit trail.
- **Automated Compliance Checks:** We run automated scripts and tools to ensure our systems remain in a secure state. This includes daily configuration checks (to verify that security groups, firewall rules, IAM roles, etc., match our approved baseline). If a discrepancy is found (say a port was opened or a setting changed outside of the change management process), it's flagged for investigation. We also continuously scan for known vulnerabilities in our systems (as mentioned under penetration testing). These proactive checks help maintain compliance with our security standards and policies at all times.
- **Incident Response Process:** In the unlikely event of a security incident, Datatako has a defined **Incident Response Plan**. Our team will execute a sequence of steps: **Identify** (detect and confirm the incident), **Contain** (isolate affected systems or

accounts to prevent spread), **Eradicate** (remove the threat, e.g., apply patches, disable accounts), **Recover** (restore systems to normal operation from clean backups if needed), and **Review** (conduct a post-mortem analysis). We also have customer communication templates ready, so we can inform you promptly of any breach affecting your data, detailing what happened and what we are doing about it. We practice a policy of transparency and will work closely with customers and possibly authorities if a significant incident occurs. Additionally, after any incident, we will update our processes to address any gaps and prevent future occurrences.

- **Business Continuity:** Our monitoring extends to performance and availability as well – we have uptime monitors and can respond to outages (whether caused by security events or not). Regular drills for disaster recovery (like restoring from backups, simulating data center outages) are part of our practice. This operational readiness ensures that even in worst-case scenarios, we can maintain or quickly resume service, which is crucial for organizations that rely on Datatako for sharing critical reports.

By combining vigilant monitoring with a practiced incident response plan, Datatako strives to not only prevent security incidents but also to minimize impact and communicate clearly if one does occur. This level of preparedness is often required by enterprise risk management standards and is part of how we build trust with customers who have their own oversight responsibilities.

Compliance & Certifications

Datatako understands that formal compliance attestation and alignment with regulatory standards are key for working with enterprises and regulated industries. We are committed to meeting these requirements and providing assurance to our customers through both our current practices and future certifications. Below is an overview of our compliance posture and roadmap:

- **GDPR and Data Privacy:** Datatako is fully **GDPR compliant**. Although we store very little personal data (primarily user login info and names/emails), we uphold all obligations regarding EU personal data. We offer a **Data Processing Addendum (DPA)** for customers, outlining how we process and protect personal data on your behalf. We honor data subject rights (access, deletion, etc.) and will assist customers in fulfilling GDPR requests. Our data is primarily processed in the region agreed with customers (we can host in EU data centers for European clients to address data residency concerns). We also align with other privacy laws like CCPA (California Consumer Privacy Act) as applicable, ensuring transparency in data handling.
- **ISO 27001 (Planned):** We are in the process of implementing an Information Security Management System (ISMS) aligned with **ISO/IEC 27001:2013** standards. Our security policies and controls are mapped to ISO 27002 best practices, and our goal is to achieve ISO 27001 certification in the near future. This certification will provide independent validation that Datatako adheres to internationally recognized security management processes. Even prior to certification, we internally follow ISO 27001's control framework (e.g., risk assessments, asset management, access control, cryptography, physical security, supplier security, incident management, business

continuity, compliance, etc.). Customers can expect that our environment and procedures are built on this solid foundation.

- **SOC 2 Type II (Future Goal):** As we grow our enterprise customer base, we plan to undergo a **SOC 2 Type II** audit by an independent auditor. A SOC 2 report will attest to our controls in areas of Security, Availability, Confidentiality (and Privacy/Processing Integrity, if in scope). Many companies ask vendors for a SOC 2 report or similar; we recognize this and are laying the groundwork for SOC 2 compliance. Many of our existing controls mirror the **AICPA Trust Services Criteria** – for example, access controls, change management, logical security, and monitoring are already in place as described above. Our target is to have a SOC 2 report available once we have sufficient operational history to satisfy the audit requirements. In the meantime, we are happy to answer security questionnaires and provide details of our controls to give you assurance.
- **Industry-Specific Regulations:** Datatako's design makes it suitable for use even in regulated industries:
    - *Healthcare (HIPAA):* We **do not store Protected Health Information (PHI)** on our systems, as all report data stays in your Power BI tenant. This greatly limits our role with respect to HIPAA. If required, Datatako is prepared to sign a **Business Associate Agreement (BAA)**, and we ensure that our platform uses HIPAA-compliant services. (Notably, Microsoft Power BI is covered under Microsoft's HIPAA BAA, meaning the underlying report hosting environment meets HIPAA requirements.) We also employ the necessary safeguards (encryption, access controls, audit trails) that align with the HIPAA Security Rule. Thus, healthcare organizations can confidently use Datatako to share reports containing PHI, with the understanding that PHI remains in the HIPAA-compliant Microsoft environment during visualization.
    - *Finance (PCI-DSS, SOX, etc.):* Datatako itself does not process credit card payments or financial transactions – any payments for our service go through PCI-certified third-party processors (Stripe). Therefore, PCI-DSS is not directly applicable to our platform (no cardholder data stored). However, for financial institutions concerned with SOX or other regulations, our strong access controls, audit logging, and forthcoming SOC 2 report will address those needs. We can assist customers in their SOX compliance by providing evidence of controls and audit logs on request.
    - *Government (FedRAMP, FISMA):* Government clients often require FedRAMP compliance for cloud services. While Datatako is not yet FedRAMP-authorized, it is built on Azure, and Azure Government could be an option in the future if demand arises. Many of our controls overlap with FedRAMP moderate requirements. We are monitoring this and other government compliance frameworks and will pursue them as needed.
- **Microsoft Compliance Inheritance:** Since Datatako relies on Microsoft Power BI for core report rendering and data storage, our customers benefit from Microsoft's extensive compliance certifications. Power BI (as part of Microsoft 365/Azure) is certified or compliant with **ISO 27001, ISO 27018 (cloud privacy), SOC 1/2/3, FedRAMP, GDPR, HIPAA, and more**. This means the environment where your data actually resides and is processed meets high standards audited by third parties. Datatako adds a secure layer around that environment without compromising those

compliance attributes. We are essentially extending a trusted, compliant platform (Power BI) to your external users in a secure manner. For regulated customers, this is a key point: **Datatako does not introduce a new unvetted data store – it keeps your data within the certified Microsoft cloud while enforcing additional sharing controls**.

To summarize our compliance status and commitments, the table below highlights key frameworks and Datatako's stance:

Standard / Framework	Datatako Status & Commitment
ISO/IEC 27001 (Information Security)	*In Progress:* Implementing controls aligned to ISO 27001/27002; pursuing certification. Demonstrates commitment to a holistic ISMS.
SOC 2 Type II (Security, Availability, Confidentiality)	*Planned:* Will undergo independent SOC 2 audit as customer base grows. Current controls mapped to Trust Services Criteria; no report available yet.
GDPR (EU General Data Protection Regulation)	*Compliant:* Minimal personal data collected; offers DPA. Supports EU data residency. Upholds data subject rights and breach notification within 72 hours.
HIPAA (Health Insurance Portability and Accountability Act)	*Ready:* No PHI stored on Datatako; can sign BAA if needed. Underlying Microsoft services are HIPAA-compliant. All ePHI safeguards (encryption, access control, audit logs) in place for data in transit.
PCI-DSS (Payment Card Industry Data Security Standard)	*Not Applicable:* Datatako does not process or store payment card data. Any billing uses PCI-certified vendors.
FedRAMP (Federal Risk and Authorization Mgmt Program)	*Not Yet:* Not FedRAMP authorized at this time. Datatako can potentially deploy in Azure Gov cloud if required. Many FedRAMP controls (encryption, logging, access control) are already implemented as part of our standard operations.
Other Regulations (CCPA, SOX, etc.)	*Compliant/Supported:* Adheres to applicable privacy laws (e.g., CCPA for user data). Provides audit logs and internal control evidence to assist with SOX, internal audits, and other oversight as needed.

Datatako's focus is to **continually improve our security and compliance posture**. We will update customers and this security whitepaper/page as we achieve new certifications or make significant enhancements. Our roadmap includes not only certifications but also participating in third-party security assessments and possibly the **Cloud Security Alliance CAIQ** registry for transparency. We speak the language of enterprise security and are committed to earning and keeping your trust through verifiable actions.

Conclusion

Security is a shared responsibility, and Datatako is your proactive partner in secure analytics sharing. We combine a highly secure architecture (that keeps your data in a trusted environment) with rigorous operational practices and a dedication to meeting top-tier security standards. This security sheet has outlined how Datatako protects your data through multiple layers: strong encryption, robust authentication and access control, secure software and infrastructure, vigilant monitoring, and compliance with the frameworks that matter to you. We use a *"secure-by-default"* philosophy, similar to other best-in-class providers, to ensure that security is not optional but ingrained in every aspect of our service.

For technical leaders evaluating Datatako, the key assurances we offer are: **your data remains safe, private, and under your control**, and our platform meets the security expectations of modern enterprises. Whether you're an SMB or a large regulated institution, our measures – from 2FA enforcement to planned ISO 27001 certification – are designed to **gain your confidence** and help you satisfy your own security due diligence. We welcome any questions and can provide further details (such as policy documents or audit results) under appropriate non-disclosure, so you can verify that Datatako will be a trusted custodian for extending your Power BI reports to a wider audience.

By choosing Datatako, you enable greater collaboration and insight-sharing powered by Power BI **without compromising on security**. We remain committed to safeguarding your data as fiercely as if it were our own, and to continuously adapting our security program to meet the evolving threat landscape and compliance requirements.

Feel free to contact our team for any additional information or to discuss how Datatako can meet your organization's specific security needs. Your trust is our highest priority, and this document demonstrates the lengths we go to earn and maintain it.