DATA PROTECTION FRAMEWORK

JANUARY 2020

SEEKIFY.COM/SECURITY

Document Control

Version	Version Notes	Prepared	Approved	Effective Date
1.0	Initial Release	Ajeet Kushwaha	Arihant Jain	Jan 1, 2020

Seekify's Promise

The Seekify platform is poised to converts agents into super humans to deliver the perfect Customer Experience. How do we do that - We act as the management viewfinder to focus on the elements that matter the most. Our Insights engine dissects your business data to draw timely and actionable Insights that lets your agents stay on top of their game always.

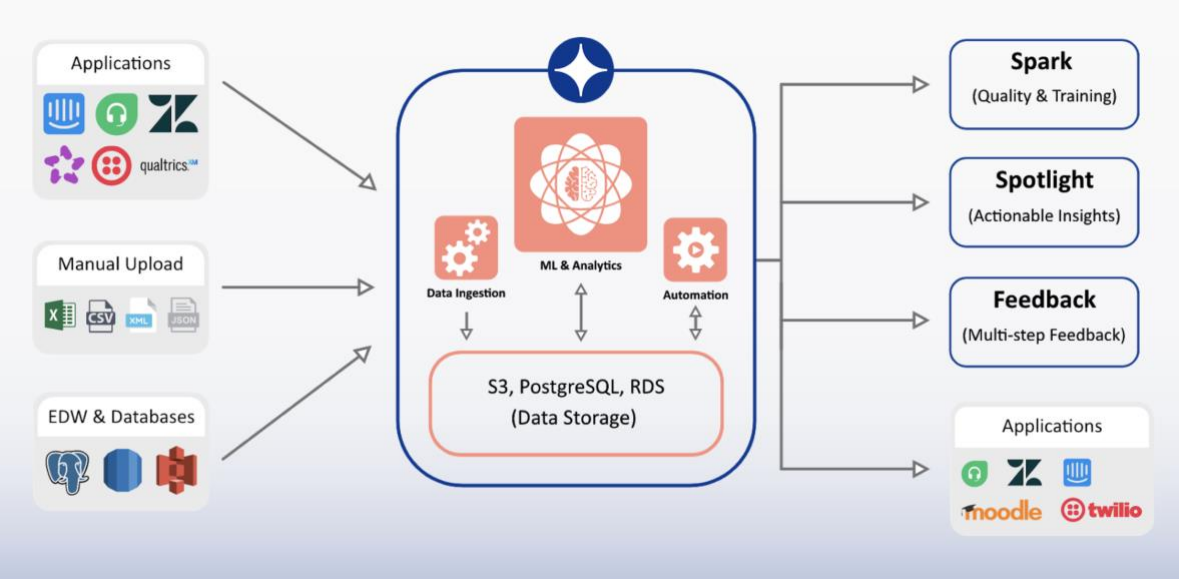
While we deliver these Insights, we respect the sensitivity of business data and privacy of individuals identified in the data. We operate within the following principles:

Transparent Processing	Data minimization	Data protection
Customers determine the target data and systems from which Insights are drawn	Processing limited to essentials determined by the client and data is purged thereafter	The platform and the data are guarded to assure its security, integrity and resiliency

In this document, "Data Protection Framework", Seekify sets out its intent, philosophy, and approach to secure Customer data. This document is intended to provide to customers an overview of Seekify's ways of working when it comes to protecting their data. This Data Protection Framework supplements the security terms in Seekify's Customer Terms of Use (seekify.com/terms) ("Terms") and in case of any conflict between the Data Protection Framework and the Terms, the provisions in the Terms will prevail.

Index

1. Technology Overview



Following is a sneak peek into the critical components of our tech stack. The entire stack is hosted on AWS.

- **PostgresSQL:** It is an open-source Relational Database Management System (RDBMS) emphasizing extensibility and technical standards compliance. It is designed to handle a range of workloads including data warehouses or Web services with many concurrent users.

- **Java Spring Boot:** Ensures comprehensive infrastructure support for developing micro services and enables us to develop enterprise ready applications.

- **Thymeleaf:** It is a modern server-side Java template engine for both web and standalone environments. Thymeleaf's main goal is to bring elegant *natural templates* to the development workflow — HTML that

can be correctly displayed in browsers and also work as static prototypes, allowing for stronger collaboration in development teams.

- **ReactJS:** It is a JavaScript library for building user interfaces as it is optimal for fetching rapidly changing data that needs to be recorded.

- **AWS DynamoDB:** It is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-region, multi-master, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications.

- **Apache Airflow:** A platform to programmatically author, schedule, and monitor workflows

These apart, we also use MySQL and Python coding.

1.1. Sub-Processors

- Amazon Web Services (AWS) are our only sub-processers that are involved in our service design as all our services are hosted and delivered from AWS.
- Seekify Technologies Pvt. Ltd as the product development, support and maintenance are performed from India.

1.2. Data Residency

Our services are hosted within the AWS datacenters in the following locations:

- Mumbai, India
- N. Virginia, US (Q1-2020)

Seekify will sign the model contractual clauses with customers to cover data transfer if the data processed originates from the European Economic Area. Customer data will be processed by the sub-processors mentioned below.

1.3. Data Processing

- **Base Data:** Seekify draws insights from the data that the customer shares with its systems. Customers may share their data through an API over a scheduled system action for data transfer, or customers may transfer their data as CSV files. This is the raw data with which Seekify draws insights.
- **Processed Data:** Seekify converts the Base Data to a format that is compatible for its engine to draw insights.

Once the Base data is converted into Processed Data, the Base data is deleted.

- **Insights Data:** Seekify's System of Actionable Insights draws specific actionable insights from the Processed Data. Once the Insights Data is extracted, the Processed Data is deleted. Retention of the Insights Data on the Seekify's platform will be as per the retention specifications in the Terms.

2. Risk Management

The CEO and Co-founders of Seekify has defined a risk management framework and its appetite for risk tolerance. Accordingly, Seekify performs a cyber security and information security risk assessment on a yearly basis. Guided by this risk assessment, Seekify implements appropriate safeguards to secure its technology platform and data.

The objective of the risk management is to ensure that

- risks that threaten the confidentiality and integrity of Data is addressed.
- Risks that threaten the continuous availability of its Data and technology platform are addressed.

Broadly, Seekify considers the following as part of its Risk Assessment

- Regulatory and legal considerations on the data
- Business sensitivity of the data and the systems
- Any major changes to its business model and technology landscape
- Inherent threats to the underlying technology

- Any pertinent security incidents that is reported within Seekify or in the industry at large
- Any findings from its internal audit

3. Security Policy

Seekify is committed to design, implement and operate system and procedural safeguards that assures to maintain the

- Confidentiality and integrity of Data
- Non-repudiation of critical system activities
- Continuous availability of its Data and technology platform.

The Information Security safeguards of Seekify are regularly calibrated to be aligned with its risk environment and thereby Seekify ensures continuous adaption and improvement of its security posture.

The Security policy of Seekify applies to all of its employees and business vendors. As part of the employment contract, all employees provide an affirmation of having read and understood the intent and specifics of Seekify's Data Protection Framework. The policy is also cascaded to its business vendors as part of their service contracts.

Any employee or vendor not adhering to the Data Protection Framework will be considered as a Security incident and appropriate corrective and preventive actions, as recommended by the CEO and Co-founders will be taken.

4. Acceptable Use Policy

The Data and the information systems used by Seekify are subject to various regulatory and contractual obligations. It could also provide or deny competitive business advantages to its customers and/or Seekify. Hence all the employees and business vendors are obliged to adhere to the Seekify's Data Protection framework and specifically adhere to the following:

- Maintain the confidentiality and integrity of Data.
- Maintain and process Customer Data[1] only within the Production environment. This data is not to be used for any other purposes than providing services to the customers as stated in its Terms of Service.
- Use only authorized systems and services for business communications.
- Do not share any Customer or Seekify confidential information on public communication channels (such as Facebook, LinkedIn, Twitter, etc.)
- In the event of any actual or suspect system anomaly that threatens its data and systems, inform the CEO and Co-founder.

In order to deliver on its security obligations, Seekify reserves the right to monitor and review the system utilization and activities performed by its employees.

[1] Customer Data includes both Base data and Insights data.

5. Security Baseline

The production environment is hardened to ensure that the services, communications, and data are secured.

- Access to the production environment shall be routed through a bastion host.
- Two-factor authentication shall be implemented in the IAM.
- Security groups shall be hardened to permit only authorized ingress and egress network traffic.
- Servers shall be hardened to allow only legitimate services.
- Anti-malware services shall be implemented in the servers.
- Security patches on the servers and software components shall be implemented within the defined timelines as determined by its severity.

6. Access Management

The objective of Seekify's Access management policy is to ensure that access to information resources and data are restricted to authorized users only. Accordingly, Seekify takes the following measures to maintain the sanctity of data and information systems:

- The level of access to information resources are commensurate to the role and processing requirements of the user
- While planning the access entitlements, conflict of interests is to be avoided or managed through suitable compensating controls
- Systems are built with adequate identification and authentication measures prior to granting access

- Adequate system logs are maintained for information access to ensure non-repudiation
- Access to information resources and data are to be reviewed and recertified on a half-yearly basis

7. Change Management

Changes to Seekify's information systems, including its technology landscape is to be managed such that

- the changes do not adversely impact the existing system functionalities, or
- the changes do not introduce newer system vulnerabilities, or
- cause service downtime or performance degradation.

Seekify shall maintain separate environments for system development, testing, and production. The product source code shall be maintained in a version-controlled repository. Access to the source code shall be limited to only authorized employees. All modifications or changes to the source code shall be approved by designated individuals.

Changes to the technology infrastructure shall be implemented after a thorough assessment of its impact and based on an adequate roll-back mechanism.

Change also include implementation of any patches to the application and infrastructure. Seekify shall monitor the patches that are applicable for its technology environment. The patches are reviewed for its applicability, and impact, and are

accordingly implemented as part of the Change Management process.

Any major changes that require downtime to the platform shall be communicated to the customers at least 15 days in advance.

System record of all changes made to the information systems and the corresponding approvals shall be maintained within Seekify. Release notes of newer changes shall be made available to customers through product release notes, that are accessible from the product.

8. Data Encryption

All Customer Data in transit are encrypted using TLS through. All data at rest are encrypted and that includes the underlying storage for DB instances, its automated backups, Read Replicas, and snapshots.

Amazon RDS encrypted DB instances use the industry standard AES-256 encryption algorithm to encrypt the data on the server that hosts the Amazon RDS DB instances. After the data is encrypted, Amazon RDS handles authentication of access and decryption of the data transparently with a minimal impact on performance. The data that is in transit between the source and the Read Replicas is encrypted, even when replicating across AWS Regions.

The encryption keys are managed using AWS Key Management Service (KMS) that provides secure, highly available hardware and software to provide a key management system. The master keys that are created in AWS KMS are protected by hardware

security modules (HSMs) that validated by the FIPS 140-2 Cryptographic Module Validation Program.

9. Incident Management

The Site Reliability Engineering (SRE) team at Seekify monitors the key system metrics through AWS CloudWatch to ensure that the operational health of the systems is maintained in terms of latency, resource availability, and security. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing the team with a unified view of resources, applications, and services that run on the production landscape. Thereby anomalous behavior could be detected and addressed through automated actions or manual troubleshooting.

In the event of any technical glitches or anomaly or incident faced by the customers, it may be notified to support@seekify.com.

Support requests from customers are categorized as follows:

Incident category	**Containment SLA**	**Resolution SLA**
FYI – Lead indicators to a possible incident	24 hours	Next Product Release
Glitch – Minor service degradation	8 hours	48 hours
Anomaly – Malfunctioning of	6 hours	24 hours

certain critical functionalities		
OMG – Entire platform being unavailable for customers	2 hours	8 hours

Some of these incidents may have a potential or actual impact on the confidentiality or integrity of Customer Data. These are called as Security Incidents and are classified as "OMG". The CEO or Co-founder are notified about the Security Incidents to oversee the situation and provide suitable directions.

While dealing with Security Incidents, the Infra team ensures that the system state is preserved for forensic investigations. The incidents are first contained and later, controlled based on its root cause analysis. If there is an actual or a suspected impact on any personally identifiable information, the same is communicated to the Legal and Privacy counsel for reviewing any contractual or regulatory impact and managing communication to the customers and regulators.

10. Backup and Retention

Database is backed up in real time through the deployment of Multiple Availability Zone (AZ) redundancy. In addition, Seekify runs an hourly schedule for data backups. The backup snapshots are retained for seven (7) days.

Data retention requirements are configured automatically as per the specifications defined in the Terms of Service.

11. Disaster Recovery

Seekify infrastructure is hosted using AWS Multi-Availability Zone (AZ) service. Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.

In a Multi-AZ deployment, the database is automatically maintained in a synchronous standby replica in a different AZ. The primary DB instance is synchronously replicated across AZ to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability enhances availability during planned system maintenance, and help protect the databases against DB instance failure and AZ disruption.

In the event of a planned or unplanned outage of the DB instance, Amazon RDS automatically switches to a standby replica in another AZ. While the time it takes for the failover to complete depends on the database activity and other conditions at the time the primary DB instance became unavailable, the failover times are typically in the range of 60-120 seconds. Essentially, our Recovery Point Objective is no data loss in the event of a technology disruption and our Recovery Time Objective to come back-up is two (2) hours.