# Privacy Policy

| | | |
|---|---|---|
| Koan Analytics | **Privacy Policy** | Document Owner<br>Aditya Gabrani |
| Effective Date<br>July 22, 2022 | Version 1.1 | Document Approver<br>Robert Wood |

# 01 OVERVIEW AND SCOPE

## 01.01 Overview

This policy and applicable supporting procedures are designed to provide Koan Analytics with a documented and formalized process for protecting individuals' privacy. Respect for the privacy of personal and other information is fundamental to us. This privacy policy describes our collection of personally identifiable information from users of our Web site ("Website" or "Site"), our Platform, as well as all related applications, widgets, software, tools, and other services provided by us and on which a link to this Policy is displayed (collectively, together with the Website, our "Service"). This Policy also describes our use and disclosure of such information. By using our Service, you consent to the collection and use of personally identifiable information in accordance with this policy.

In accordance with mandated organizational security requirements set forth and approved by management, Koan Analytics has established a formal privacy policy and procedures. This comprehensive Policy document is implemented immediately, along with all relevant and applicable procedures.

The Policy Owner owns this Policy and is responsible for reviewing the Policy on an annual basis and following any major changes to Koan Analytics's sensitive data environment, to ensure that it continues to meet its organizational goals. The Policy Owner is also responsible for ensuring that the Privacy Procedure is reviewed and updated on an annual basis and following any major changes.

## 01.02 Purpose

This Policy along with supporting procedures are designed to provide Koan Analytics with a formalized information security policy to comply with various regulatory and business requirements. Compliance with the stated policy along with supporting procedures help ensure the safety and security of all Koan Analytics's system components within the sensitive data environment as well as any other environments deemed applicable.

## 01.03 Scope

This policy and supporting procedures cover the privacy of all data collected by Koan Analytics in its interaction with individuals in its business operations.

This Policy along with supporting procedures cover all system components within the sensitive data environment owned, operated, maintained, and controlled by Koan Analytics. This Policy along with supporting procedures cover all other system components (both internally and externally) that interact with these systems and all other relevant systems.

This Policy along with supporting procedures cover all employees, interns, volunteers, and contractors. All of these individuals will be referred to as 'employees' throughout these policies/procedures, unless otherwise noted. Both policies & procedures will be made available to employees and they will be required to sign an acknowledgement they read these policies/procedures and agree to abide by them.

## 01.04 Monitoring and Enforcement

Koan Analytics periodically monitors adherence to this Policy to help ensure compliance with applicable laws, requirements, and contractual agreements applying to Client and Consumer Data.

Penalties for failing to comply with Koan Analytics's Policies and Procedures could lead to disciplinary and/or enforcement actions against individuals and lead to sanctions brought against Koan Analytics. Enforcement actions could include civil and/or criminal charges brought against violators depending on the seriousness of the offense.

*[Note: If the organization is a covered entity, there are specific requirements related to Privacy Notices. There are specific headers and content requirements for a covered entity. A sample from the Department of Health and Human Services can be found here: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html ]*

# 02 ROLES AND RESPONSIBILITIES

The following roles and responsibilities are to be developed and subsequently assigned to authorized personnel within Koan Analytics regarding privacy practices:

- **Chief Privacy Officer:** Responsibilities include providing overall direction, guidance, leadership, and support on methods and tools for the implementation of a security and privacy-related program. The Chief Privacy Officer will conduct resource and investment planning to implement the management, operational, technical, and privacy requirements of the program.

- **Privacy Committee:** Responsibilities include approving and monitoring adherence to this policy, analyzing the organization's environment, and the legal requirements with which it must comply. Additional responsibilities include:
    - Execute the privacy operations of the firm, including monitoring the system used to solicit, evaluate, and respond to individual privacy complaints and problems.
    - Evaluate implemented privacy controls;
    - Assessing existing policies and procedures that address privacy areas;
    - Working with appropriate departments to ensure compliance with privacy policies and procedures;
    - Recommending and monitoring, in conjunction with the relevant departments, the development of internal systems and controls to carry out the organization's privacy objectives;
    - Report to the Chief Privacy Officer on the effectiveness of the privacy controls/program in meeting applicable regulatory requirements and standards.

The organization must formally document and make privacy policies readily available to data subjects, internal personnel, and third parties who need them. Privacy policies will be documented to include security practices for privacy as well as all areas covered below.

Management will review and approve privacy policy on an annual basis.

# 03 Authority to Process Personally Identifiable Information

The organization will determine and document the authority permitting the organization to process personally identifiable information. The organization will restrict processing of personally identifiable information not authorized. Where possible, the organization will attach data tags containing authorized processing to elements of personally identifiable information. The organization will enforce the authorized processing of personally identifiable information using restrictive data policy definitions and identity provider permission sets. .

# 04 Personally Identifiable Information Processing Purposes

The organization will identify and document the purposes for processing personally identifiable information. The purpose of processing will be described in the public privacy notices and related privacy procedures. The organization will restrict processing of personally identifiable information to only that which is compatible with the identified purposes. If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the organization will document the new purpose, notify the data subject, and obtain implicit or explicit consent prior to such new use or purpose.

The organization will monitor changes in processing personally identifiable information and implement mechanisms to ensure that any changes are made in accordance with defined requirements.

Where possible, the organization will attach data tags containing purposes to elements of personally identifiable information for defined processing purposes.

The organization will track processing purposes of personally identifiable information using CloudWatch logging and alert mechanisms..

## 04.01 Collection

The organization will limit the collection of personally identifiable information to what is necessary to meet the organization's objectives. The methods of collecting personally identifiable information will be reviewed by management prior to implementation to confirm personally identifiable information is obtained fairly and without intimidation or deception as well as lawful, adhering to all relevant rules of law.

The organization will inform data subjects if the organization develops or acquires additional information about them for the organization's use.

## 04.02 Use and Retention

The organization uses personally identifiable information only as is authorized and only at the minimum necessary level required by the organization to meet service level obligations, contractual obligations, or regulatory requirements.

The organization will retain personally identifiable information for only as long as required or according to the organization's retention schedule as may be required by regulatory or contractual obligations.

## 04.03 Access

The organization permits data subjects to determine whether the organization maintains personally identifiable information about them and upon request, the data subject may obtain access to their personally identifiable information. The organization will verify and authenticate the identity of data subjects who request access to their personally identifiable information before they are given access to the information.

The organization will provide personally identifiable information to the data subject in an understandable form, in a reasonable timeframe, and at a reasonable cost.

The organization may deny a data subject access to or a request to change their personally identifiable information based on regulatory requirements and will inform the data subject of the denial along with the reason for the denial in a timely manner, unless prohibited by regulations.

## 04.04 Disclosure

The organization will disclose personally identifiable information to third parties only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject, unless a law or regulation specifically requires otherwise.

The organization will track and log authorized and reported unauthorized disclosures.

## 04.05 Correction and Update

The organization will permit data subjects to update or correct personally identifiable information held by the organization. The organization will provide such updates or corrected information to third parties that were previously provided with the data subject's personally identifiable information consistent with the organization's objectives related to privacy.

The organization may deny a data subject access to or a request to change their personally identifiable information based on regulatory requirements and will inform the data subject of the denial along with the reason for the denial in a timely manner, unless prohibited by regulations.

## 04.06 Deletion

The organization will capture requests for deletion of personally identifiable information and information related to requests will be identified/flagged for destruction to meet the organization's objectives related to privacy.

# 05 Choice and Consent

The organization informs data subjects about the choices available to them with respect to the collection, use, and disclosure of their personally identifiable information. The organization must

require implicit or explicit consent to collect, use, and disclose personally identifiable information. The organization will obtain and document implicit or explicit consent from data subjects at or before the time personally identifiable information is collected (or soon thereafter). The individual will confirm and implement the individual's preferences expressed in their consent. The organization obtains consent before personally identifiable information is transferred to or from an individual's computer or other similar device.

The organization will implement tools or mechanisms for individuals to consent to the processing of their personally identifiable information prior to its collection facilitating individuals' informed decision-making. Where possible, the organization will provide mechanisms to allow individuals to tailor processing permissions to selected elements of personally identifiable information. The organization will present consent mechanisms to individuals at the time of processing. The organization will implement a mechanism for individuals to revoke consent to processing.

# 06 Privacy Notice

The organization must make the organization's latest privacy policy publicly available on the organization's website.

The organization will also provide notice to individuals about the processing of personally identifiable information that:

- Is available to individuals upon first interacting with an organization, and subsequently upon changes in the notice;
- Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;
- Identifies the authority that authorizes the processing of personally identifiable information;
- Identifies the purposes for which personally identifiable information is to be processed; and
- Includes specific information related to the organization's regulatory or contractual obligations.

The organization will present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or annually if or when the notice changes.

The organization will include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

# 07 System of Records Notice

For systems that process information that will be maintained in a Privacy Act system of records, the organization will:

1. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;
2. Publish system of records notices in the Federal Register; and
3. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

The organization will review all routine uses published in the system of records notice annually to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.

The organization will review all Privacy Act exemptions claimed for the system of records annually to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.

# 08 Specific Categories of Personally Identifiable Information

The organization will apply special conditions for specific categories of personally identifiable information as required by law.

When a system processes Social Security numbers, the organization will:

- Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;
- Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and
- Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

The organization will prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

# 09 Quality and Computer Matching Requirements

When a system or organization processes information for the purpose of conducting a matching program, the organization will:

- Obtain approval from the Data Integrity Board to conduct the matching program;
- Develop and enter into a computer matching agreement;
- Publish a matching notice in the Federal Register;
- Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and
- Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

# Related Documents

- Privacy Procedures
- System Integrity Policy

# CHANGE CONTROL

| Date | Version | Change(s) | Reason for Change(s) | Change(s) Made By |
|---|---|---|---|---|
| | | | | |