TRUSTPOINT.ONE WHITEPAPER

Data Mapping & Analysis:

The Foundation for Effective Information Governance Policy.

Introduction

Data mapping is a common colloquial word for a "data inventory," and is the first step an organization takes towards developing a privacy program. Using tools and answering a series of questions, an organization can uncover what data it has, where it is located, how it is being used, and who has access to it. Once the data mapping exercise is complete, the end result show how data is collected, whether or not there is personal or sensitive information in the data flows, and highlight possible risks in using that information.

Trustpoint Cyber Services offers a comprehensive and holistic approach to data mapping. Combining our software and privacy expertise, the Trustpoint Cyber Services client report lays out data mapping information in an understandable manner and possible next steps to achieve the client organization's overall privacy goals and requirements.

Why is it so important?

Organizations are increasingly required by data privacy laws and regulations to protect data they hold with personal and sensitive information. Completing a comprehensive data mapping exercise allows an organization to understand what type of data they hold, where it is located, and how it is currently used. Without this knowledge, an organization cannot timely or accurately respond to actions mandated by emerging privacy laws and regulations, such as the Right to Erasure or a Data Subject Access Request. Also for organizations subject to these emerging privacy laws and regulations, these laws may permit individuals to bring suit under a Private Right of Action with possible statutory damages; i.e., allow an individual to sue for failure to comply with their data requests or to otherwise comply with the privacy laws.

Data mapping also allows organizations to analyze their data from a macro perspective and assess vulnerabilities and areas of risk regarding personal and sensitive information they hold. If an organization does not understand the type of data it has and where it is located, it cannot mitigate its risk and the data may be vulnerable to unauthorized access. These weak spots are prime targets for a threat actor to maliciously access organization data and create a regulatory and public relations nightmare for the organization. Once vulnerabilities and risks are identified, an organization should follow up with additional steps to further their privacy program, including additional risk assessments and creating a privacy policy regarding each collection or area of concern with regards to handling of the data.

Beyond the initial need to complete a data mapping exercise to establish a privacy program coupled with government and consumer pressure to continually protect personal and sensitive information, it is a best practice for an organization to regularly complete data mapping actives to ensure that there are no material changes. If any material changes are identified in follow up data mapping assessments, also as a best practice, an organization should run through the privacy lifecycle to ensure data protection is a top priority.

Privacy Risk Assessments

Any time there is a collection of personal or sensitive information, an organization will face a risk in storing and/or processing this information.

LEARN MORE

What is involved?

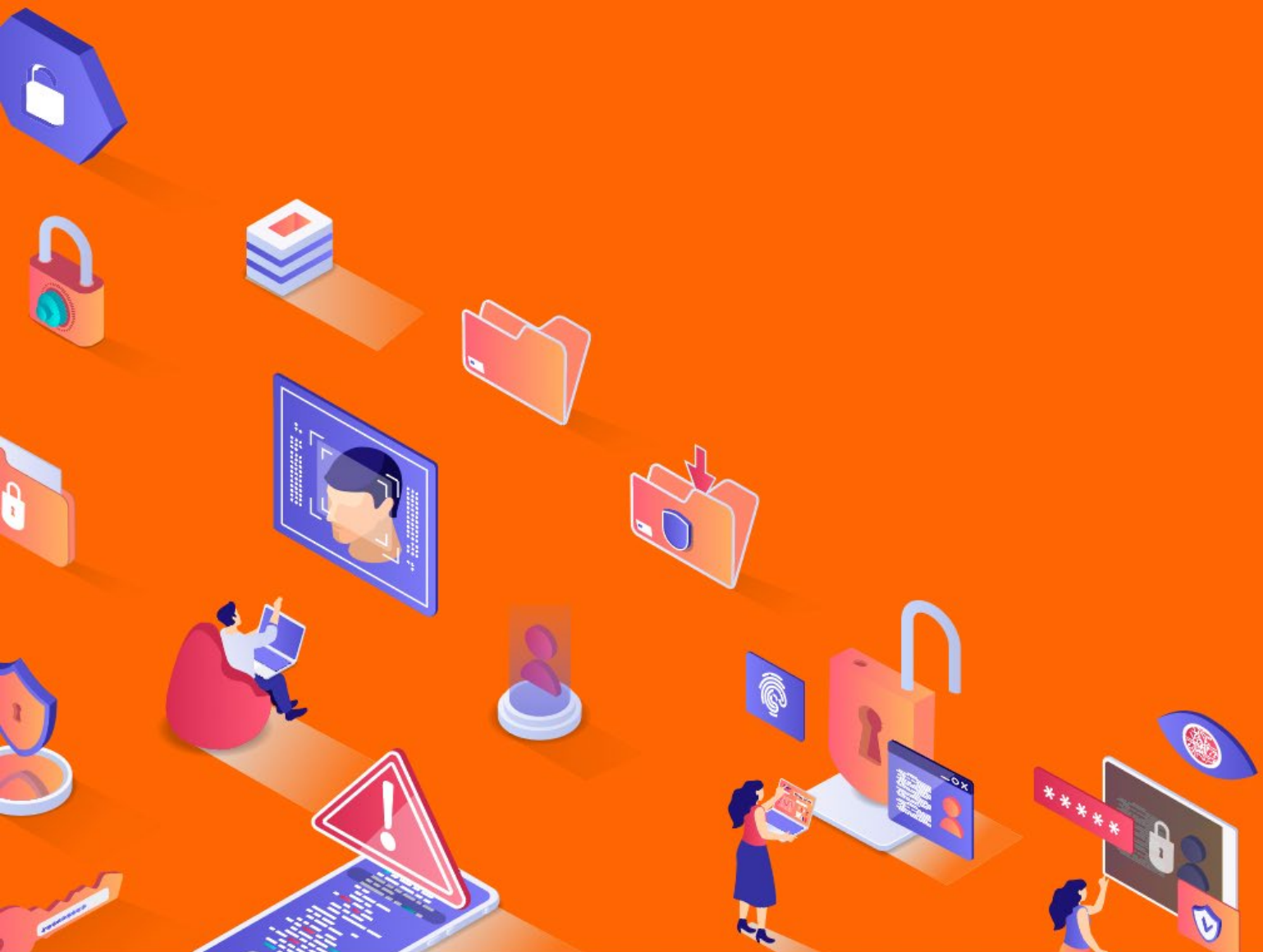
Trustpoint Cyber Services may deploy a couple of options, depending on the needs of the client:

1) - Software - Trustpoint Cyber Services may install and use third-party software to process a client organization's databases and loose files, often referred to as "Data Discovery." This information is then used by Trustpoint Cyber Services to identify and create a data inventory.

2) - Questions - Some organizations do not have collected data, or their data processing is simple enough to not warrant software based data discovery. Our privacy experts will walk through the data inventory exercise by asking certain questions and taking a holistic view of the client's information.

"Overcollection of data is the number one mistake we see every day. Many firms are just collecting and storing way more information than they need, not realizing it poses a risk. That's one major reason Data Mapping is so important, as it often reveals potential risk a firm had no idea it was holding."

DAN ROGERS,
Trustpoint.One Cyber Services



Using data discovery software is not always required in order to perform a data mapping exercise in all cases, and sometimes is unnecessary. Through a series of client-answered questions in combination with the information from data discovery, our privacy experts will conduct our analysis and create a report containing the pertinent information for the client.

Examples of Questions We Commonly Ask:

Describe the activity (collection) the client organization is pursuing.

Examples include: Recruiting activities, compensation, background checks, etc.

Is your organization conducting the activity on behalf of another organization?

Who are the key participants in this activity?

Examples include: HR, Legal, Sales

What information is collected about the customer?

Examples include: Name, Address, Driver's License#, Social Security Number

Where is the database physically stored?

Are you storing this information in multiple locations?

Examples include: Salesforce, Third Party Billing software, Local Server

The data involved relates to which type of individuals?

Examples include: Customers, Employees, Contractors

Is there a retention policy (data set for deletion after certain amount of time)?

Is the data subject provided an opportunity to consent to the data collection prior to data collection?

Notable items to look out for in a data mapping exercise:

Look out for oversimplification

Databases may contain multiple tables and connectors to other databases, all presenting possible risk for the data stored.

Multiple Departments

Keep in mind that each department may run a separate process and require its own data map. For example, the operations department of a company versus the billing department. Both may be dealing with the same data, but their functions are different and therefore each requires its own data map.

Jurisdiction

The definitions of personal information and sensitive information vary by jurisdiction, but an initial data map should look at the information broadly to help ensure a regulation is not triggered without an organization's knowledge.

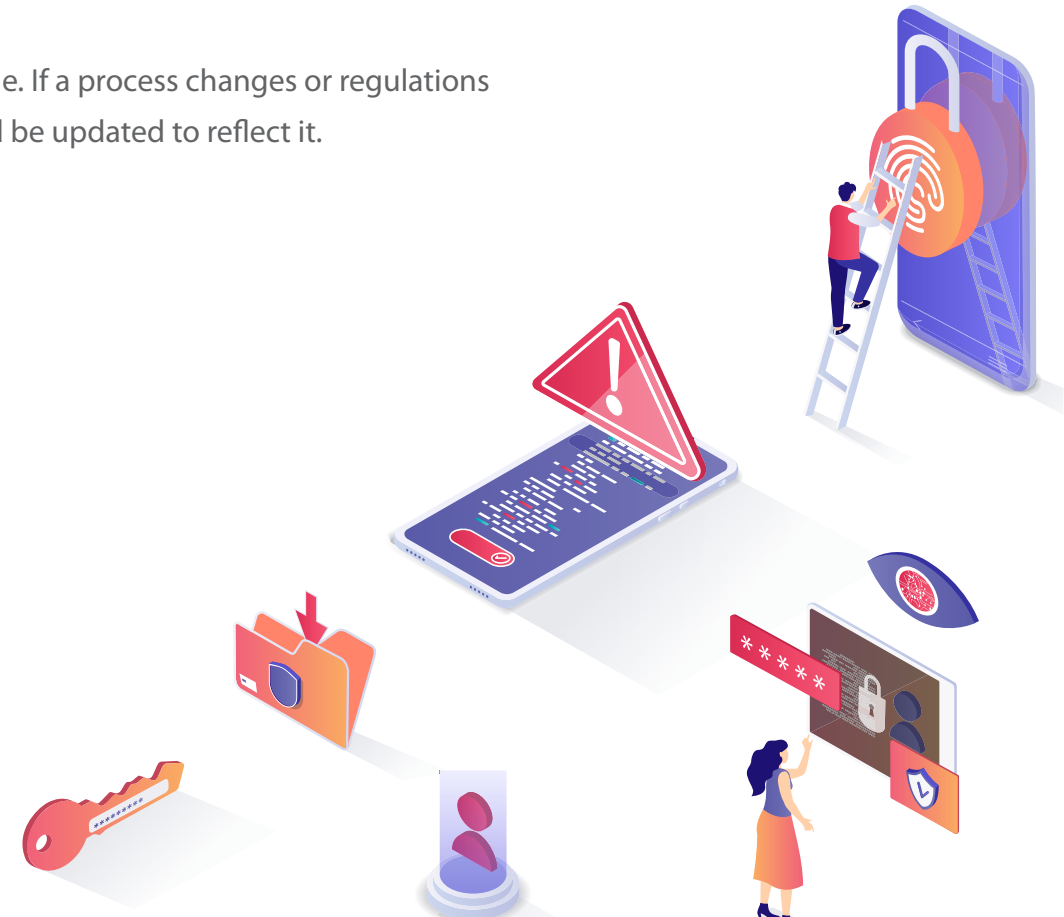
Process Changes

Data maps are a snapshot in time. If a process changes or regulations change, then a data map should be updated to reflect it.

Data Mapping Do's and Don'ts

To learn more about what to look for when performing data map, read our article on the do's and don'ts.

LEARN MORE



Difference between a data mapping exercise and a risk assessment:

Data mapping may be used to help a more thorough risk assessment, but it is different in regards to what information it provides. Data mapping looks at the *where and what*, while a risk assessment generally goes more into the *how and why* data is being used.

A privacy assessment is typically used to look at the overall data privacy practices of an organization. These assessments typically consist of a series of questions, interviews, and surveys of the appropriate stakeholders of an organization. This could include a chief legal officer, a chief information technological officer, or a chief information security officer, but it's not exclusive to any one individual or role, it's driven by the actual action of the organization.

If a risk is identified, an organization should use an alternative method or reduce the collection of personal and sensitive information. Once this process is down, it should be implemented into the organization's privacy policies and employees should be trained on any change in processes that will affect their work. Moreover, organizations should continually audit their privacy program to ensure they are mitigating the risks found from the assessments. Risk assessments may only be part of the privacy lifecycle, but will affect all other parts of the lifecycle.

Risk Questionnaire

Get our no-cost risk questionnaire to assess your infrastructure capabilities and security needs.

LEARN MORE

Jerry McIver,
Director Trustpoint Cyber Services

www.trustpoint.one