



Building a Data Inventory

Creating a **data inventory offers key benefits**, including understanding data flows, classifying and assessing the sensitivity of personal data, providing essential information for risk assessment, enabling the implementation of security controls, and **ensuring compliance with privacy regulations** like GDPR and CCPA.



Here are the four steps to building a comprehensive data inventory:

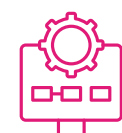
STEP 1



Stop and Plan

- **Define goals:** Are you addressing data privacy needs or broader IT/IS requirements?
- **Assess current state:** What is the current state of maintaining personal data?
- **Leverage existing processes:** Can existing processes be used, or will new ones need to be created?
- **Determine data ownership:** Who owns the data, and who is responsible for maintaining it?
- **Sustainability:** How will the organization keep the data inventory current? Is it sustainable?

STEP 2



Build Out

Once the planning is complete, start building out the data inventory:

- **Identify business activities:** Recognize internal and external activities that process personal data.
- **Engage data owners and SMEs:** Identify and collaborate with data owners or subject matter experts (SMEs).
- **Transparency and commitment:** Be clear about time commitments and expectations with SMEs and their leadership.
- **Collect data:**
 - Conduct interviews.
 - Distribute surveys.
 - Use automated data discovery and scanning tools.
- **Review and approve:** Ensure the completeness of business activities and personal data processing.
- **Validate and map:** Validate content and develop optional data flow maps to visualize processing activities.

STEP 3



Assess Risk and Remediate

With the data inventory in place, the next step is to assess the risk:

- **Risk assessment:**
 - Identify high-risk business processes.
 - Determine if personal data crosses international borders.
 - Check for automated scoring or AI use.
 - Identify special categories of data (e.g., ethnicity, religion, etc.).
 - Assess medical data, including biometrics.
- **Sort by risk:**
 - Sort business processes by high to low risk using a risk-based model.
 - Further assess high and medium-risk activities to reduce inherent risk and establish target residual risk.
- **Complete PIAs:**
 - Conduct Privacy Impact Assessments (PIAs) with SMEs and data owners.
 - Identify compliance gaps and minimize risk areas.
 - Document assessment activities and results for potential requests by authorities.

STEP 4



Publish and Demonstrate

The final stage is to publish your data inventory:

- **Collate findings:** Compile the inventory so it can be used organization-wide.
- **Software tools:** For larger data inventories or dynamic data processing, consider leveraging software such as TrustArc's [Data Mapping & Risk Manager](#) to automate data mapping, risk analysis, compliance reporting and remediation.
- **Maintain accuracy:** Ensure SMEs or business activity owners keep the content current and accurate.

Automate your manual workflows with data maps & ROPAs?

When it comes to your data and vendor management for compliance, it is important to continuously assess and monitor for privacy risks. Use TrustArc's [Data Mapping & Risk Manager](#) to automate data mapping and risk management. Out-of-the box templates and automated workflows help you continuously govern and generate ROPAs and Assessments to minimize your risk.

[REQUEST A DEMO](#)