TrustArc

Guide to

Data Inventory and Mapping

for GDPR & CCPA Compliance

Please note that this whitepaper is intended as a general overview of the subject and cannot be regarded as legal advice.

Why Build a Data Inventory and Data Flow Maps

One of the most important steps to design and build a data privacy program is to create a data inventory of all of the business processes within an organization. If an organization does not know the type of data they collect and how it's shared, processed and stored, or the data inflows and outflows, it is difficult to meet regulatory requirements, mitigate organization risks, and efficiently respond to data subject access requests.

As privacy regulations become broader in scope, requiring organizations to demonstrate how they reduce and manage risk, the importance of building and maintaining a data inventory is increasing. The EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are two examples of regulations which rely heavily on a comprehensive data inventory to support risk management, compliance reporting and responding to individual rights and data subject access rights requests.

An example of a compliance reporting requirement is in GDPR Article 30 which requires companies to create a "record of processing activities(ROPAs),which will allow regulators to validate how an organization is adhering to GDPR requirements. With this goal in mind, the records should show "why" (the processing purpose) and "how" the data is being processed within systems, vendors and organizations. Solely focusing on the "wha,t" namely data elements (e.g. email address, identification number) may cause an organization to overlook important information required to properly assess and manage risk.

An example of managing individual rights requests is in CCPA Section 1798.130, which requires companies to disclose information requested and "the disclosure shall cover the 12-month period preceding the business's receipt of the verifiable request." Responding to such a request would require locating the process or activity that touches that data, which would be facilitated by having a comprehensive and up-to-date data inventory.

Once the business process flows have been recorded and assessed for risk, the organization can make decisions about where to invest remediation resources based upon where the highest risk lies. While the word "inventory" may imply a static list at a point in time, a data inventory for privacy compliance management should reflect how data moves through the organization's business processes.

Stakeholders across the organization will need to participate in building and recording business process flows because the processes often involve multiple departments (e.g. Marketing, HR, Procurement, Info Sec).

To gain stakeholder support towards this effort, the following benefits can be highlighted:

Business Unit	Process Focus	Benefits to Business Unit & Business
Information Technology	Identifying storage redundancies	• Reduce infrastructure complexity • Identify cost savings
Information Security	Understanding what data resides in which systems	• Prioritize protection efforts – focus on high risk, high value • Establish appropriate access controls • Identify cost savings
Operations	Visualizing flows and uses of data throughout the organization	• Reduce redundancies • Improve efficiencies • Identify cost savings
Procurement	Identifying points at which the organization shares information with third party vendors and understanding the sensitivity of the data being processed (including shared)	• Support risk-based vendor • management • Greater efficiency in contract • management • Identify cost savings

Building a Data Inventory and Data Flow Map to Help Manage Privacy Compliance

Multiple Approaches

There are multiple approaches to building and maintaining a data inventory. The two most common approaches that companies use are a "systems" based approach and a "data processing activity" based approach.

The "systems" based approach looks at the systems and end points of a business process flow (focused on the infrastructure and security of the personal data). The "data processing activity" approach, looks at the type of personal data processed, and whether these data can be used based on purpose and intent.

The following example highlights how the two approaches might work for an online retailer.

An online retailer selling clothing provides an online shopping cart for customers to place an order and have the merchandise shipped to them. In addition to collecting the data elements necessary for fulfilling an online order (e.g., name, address, payment info), the retailer also collects a customer's national identification number, but no one is sure why.

Using the systems-based approach, the organization would identify which systems and vendors were used (e.g., shopping cart, credit card processing vendor), but may not identify all of the data types collected (e.g., national identification number).

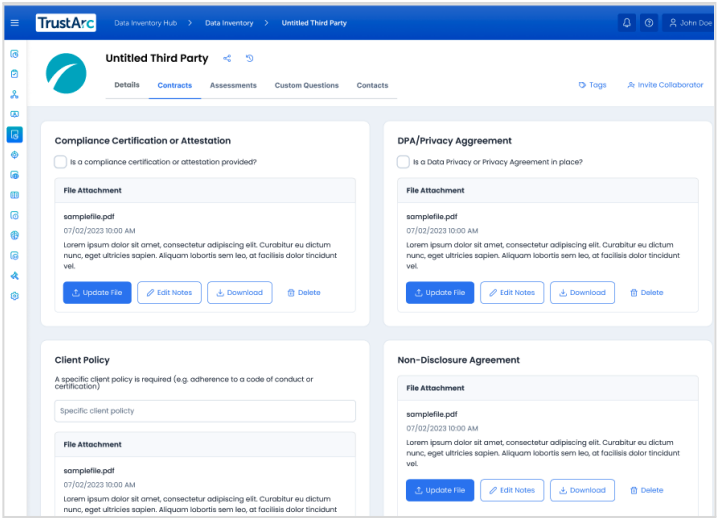
Using the "data processing activity" approach, which follows the data collected through the purchase process, would likely force the question about why the organization was collecting national identification numbers. With this approach, it is more likely that the organization would discover that sensitive personal data was being collected which was not needed and thus creating unnecessary risk for the organization.

Data Inventory Tools

After selecting an approach, you need to select the tool you will use to record and manage these processing activities. A common tool today is a spreadsheet (mainly due to availability), but a growing number of organizations are electing to implement a dedicated data privacy inventory management software from providers like TrustArc for efficiency, automation, and long-term cost savings.

Each of these tools has benefits and drawbacks. Using spreadsheets is less expensive and requires less training, but can also become complicated to manage and update once you have hundreds of business activities recorded. Spreadsheets also don't provide an audit trail of changes and don't easily support having multiple contributors across an organization. Aside from maintaining accuracy through automation, spreadsheets also do provide an Article 30 report or similar summary reports often requested by the authorities.

Using a dedicated data privacy inventory management software like TrustArc's will have higher upfront cost and training requirements, but will also offer a lot of benefits, including: tailored workflows guiding users through the process; pre-configured lists of data elements to select from, increasing the accuracy of the information; built-in collaboration and audit trail recording; visual data flow mapping tools; compliance reporting templates; and much more.



Getting Started

Before mapping all your personal data processes, start with a pilot project using one business unit to test and validate the methodology used to gather the information needed. Then use early deliverables from the pilot to secure better engagement for the broader project.

Asset inventories and vendor lists can be leveraged to help get an idea of the size and scope of the inventorying personal data processing and mapping project.

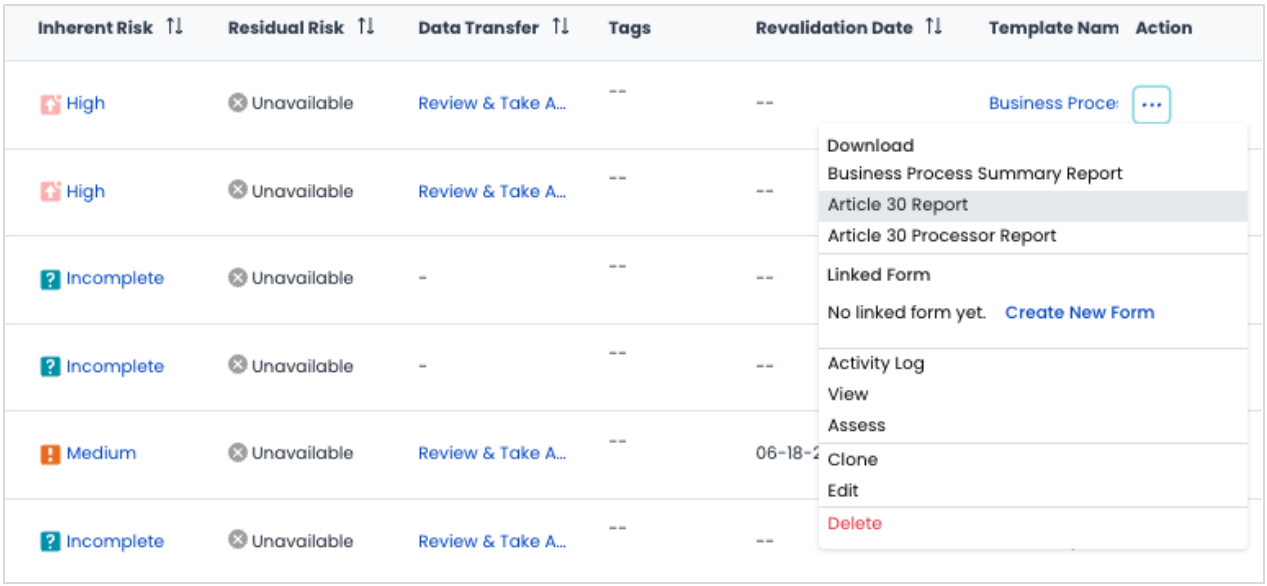
While the number of personal data processes you need to map will depend on the size and complexity of your organization, most have dozens to hundreds of data processing activities. Some examples of common business processes are provided in the table below:

Account Management	Finance	Legal
• Client Onboarding and Support • Online Order Tracking	• Customer Invoice and Billing • Employee Payroll	• Information Security Risk Assessments • Partner Contracts
Business Operations	**HR**	**Marketing**
• Customer Data Import • CRM Data Management	• HR Benefits • Talent Management Program	• Website Contact Forms • Emails Sent to Customers
Engineering	**IT**	**Sales**
• Backlog Management • Software Development Life Cycle	• Data Storage • Employee Laptop Replacement	• Lead Management – Events, Trade Shows • Updating Client Account Records

Producing a GDPR Article 30 Report

GDPR Article 30 is one of the most common types of compliance reports a data inventory can help address. Having up-to-date business process information will be key to meeting GDPR Article 30 compliance reporting requirements because the organization must produce the reports upon request from a data supervisory authority. Maintaining up to date and accurate information on your organization's processing will also help to demonstrate accountability that the processing activities are compliant with GDPR. Using an automated solution that can help keep records of these business processes up to date and produce on demand reporting.

Example of TrustArc's on demand Article 30 report generation



To comply with Article 30 you will need to demonstrate all details of personal information collection, where it's stored, shared, and used, and who is responsible for those data records. The record of processing activities must be in writing, including electronic form.

Controllers are required to record the following activities:

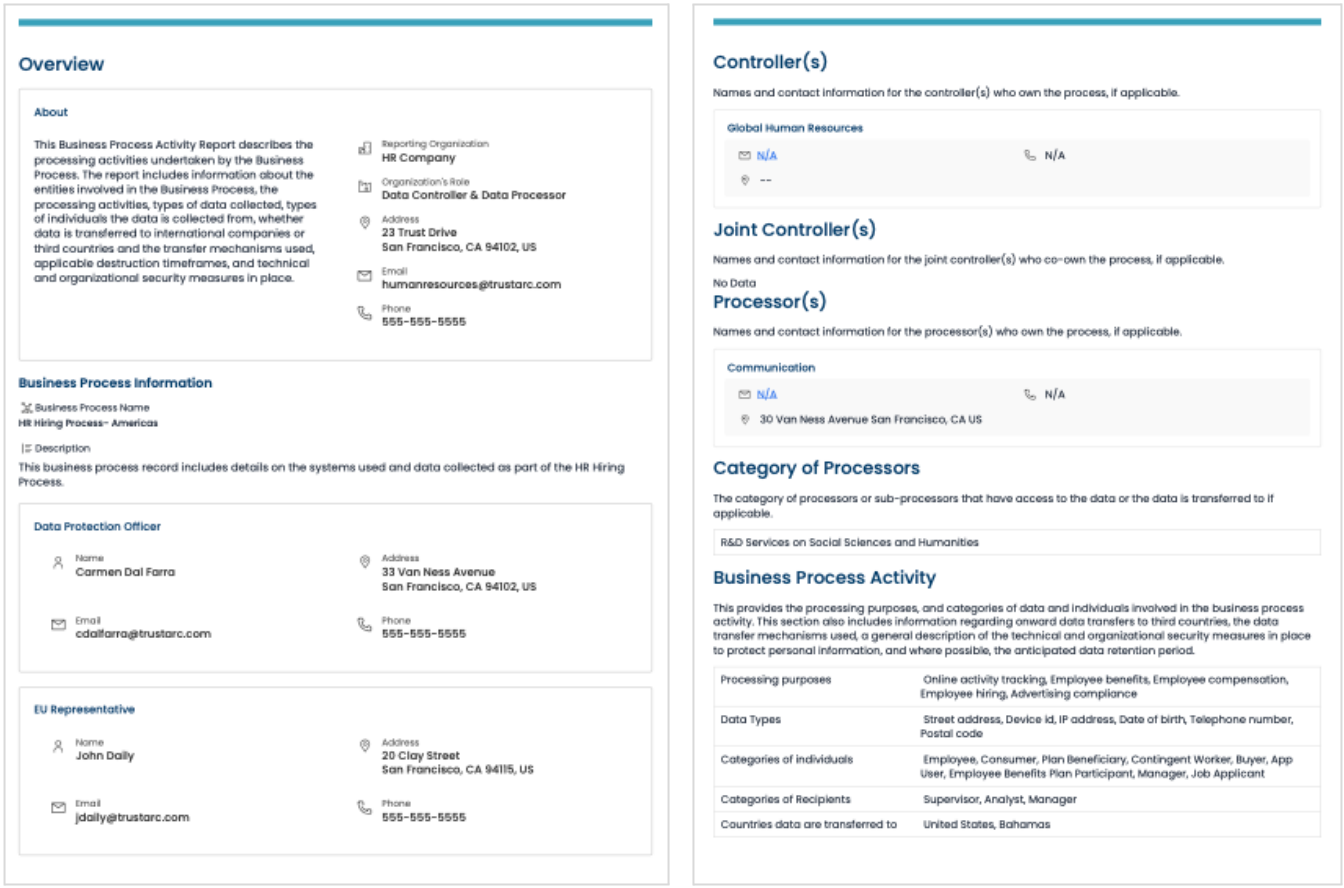
- The name and contact details of the controller (and if applicable) the joint controller, the controller's representative, and the data protection officer
- The purposes of the processing
- A description of the categories of data subjects AND the categories of personal data
- The categories of recipients to whom the personal data have been or will be disclosed
- The legal basis for the specific processing activities (e.g., consent, contract, legal obligations, etc.)
- Where applicable, transfers of personal data to a third country including the identification of that third country

and in the case of transfers the documentation of suitable safeguards (adequacy)
- Where possible, the time limits for deleting the different categories of data
- Where possible, a general description of the technical and organizational security measures

Processors are required to record the following activities:

- The processing purposes on behalf of controllers
- The technical measures
- Data Transfers
- Controllers of who the data is processed for

Example of a TrustArc Article 30 Report (PDF)



Overview

About

This Business Process Activity Report describes the processing activities undertaken by the Business Process. The report includes information about the entities involved in the Business Process, the processing activities, types of data collected, types of individuals the data is collected from, whether data is transferred to international companies or third countries and the transfer mechanisms used, applicable destruction timeframes, and technical and organizational security measures in place.

Reporting Organization: HR Company
Organization's Role: Data Controller & Data Processor
Address: 23 Trust Drive, San Francisco, CA 94102, US
Email: humanresources@trustarc.com
Phone: 555-555-5555

Business Process Information

Business Process Name: HR Hiring Process- Americas

Description: This business process record includes details on the systems used and data collected as part of the HR Hiring Process.

Data Protection Officer

Name: Carmen Dal Farra
Address: 33 Van Ness Avenue, San Francisco, CA 94102, US
Email: cdalfarra@trustarc.com
Phone: 555-555-5555

EU Representative

Name: John Daily
Address: 20 Clay Street, San Francisco, CA 94115, US
Email: jdaily@trustarc.com
Phone: 555-555-5555

Controller(s)

Names and contact information for the controller(s) who own the process, if applicable.

Global Human Resources
N/A
N/A
--

Joint Controller(s)

Names and contact information for the joint controller(s) who co-own the process, if applicable.

No Data

Processor(s)

Names and contact information for the processor(s) who own the process, if applicable.

Communication
N/A
N/A
30 Van Ness Avenue San Francisco, CA US

Category of Processors

The category of processors or sub-processors that have access to the data or the data is transferred to if applicable.

R&D Services on Social Sciences and Humanities

Business Process Activity

This provides the processing purposes, and categories of data and individuals involved in the business process activity. This section also includes information regarding onward data transfers to third countries, the data transfer mechanisms used, a general description of the technical and organizational security measures in place to protect personal information, and where possible, the anticipated data retention period.

Processing purposes	Online activity tracking, Employee benefits, Employee compensation, Employee hiring, Advertising compliance
Data Types	Street address, Device id, IP address, Date of birth, Telephone number, Postal code
Categories of individuals	Employee, Consumer, Plan Beneficiary, Contingent Worker, Buyer, App User, Employee Benefits Plan Participant, Manager, Job Applicant
Categories of Recipients	Supervisor, Analyst, Manager
Countries data are transferred to	United States, Bahamas

Producing a Third Party Vendor Risk Assessment Report

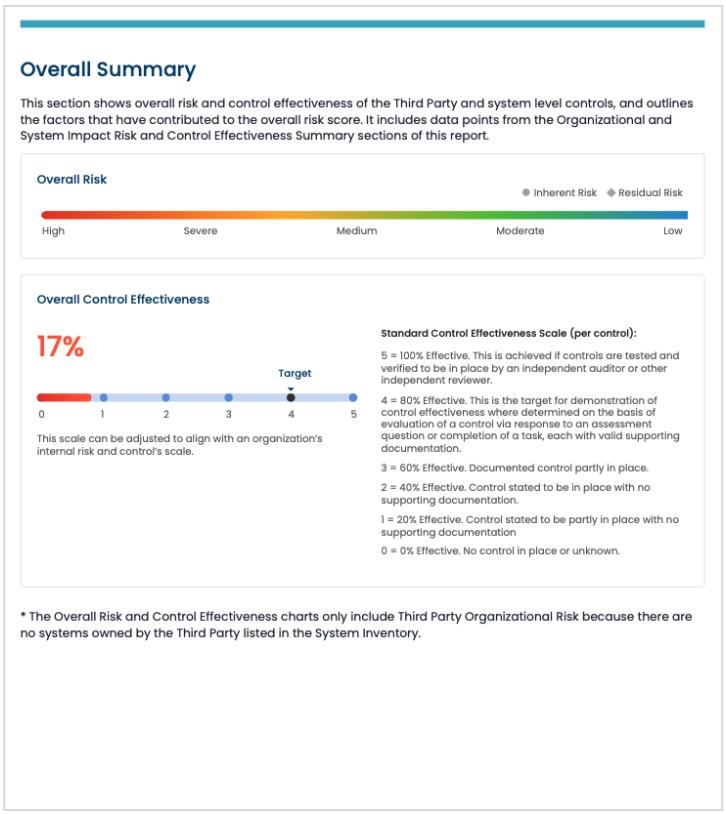
For compliance with the California Consumer Privacy Act (CCPA), companies are not required to maintain a data inventory. Practically speaking, however, complying with the CCPA for vendor management is nearly impossible without a data inventory. Companies that need to be compliant with CCPA, for example, must identify and ensure their business partners (Service Providers, Contractors, and Third Parties) are compliant with CCPA and should perform regular scans of online 3rd party tracking technologies (e.g., trackers shared by ad tech vendors) and annual vendor assessments of

service providers and contractors for CCPA Compliance.

Here are some of the records to track for inventory of all vendors, systems, business processes, and organization units with the following activities:

- The categories of personal information it has collected about the consumer, customer and/or employee
- The categories of sources from which the personal information is collected.
- The business or commercial purpose for collecting, selling, or sharing personal information.
- The categories of third parties to whom the business discloses personal information.
- The specific pieces of personal information it has collected about that consumer.

Example of a TrustArc Third Party Vendor Report (PDF)



Overall Summary

This section shows overall risk and control effectiveness of the Third Party and system level controls, and outlines the factors that have contributed to the overall risk score. It includes data points from the Organizational and System Impact Risk and Control Effectiveness Summary sections of this report.

Overall Risk

Inherent Risk ◆ Residual Risk

High | Severe | Medium | Moderate | Low

Overall Control Effectiveness

17%

Target

0 1 2 3 4 5

This scale can be adjusted to align with an organization's internal risk and control's scale.

Standard Control Effectiveness Scale (per control):

5 = 100% Effective. This is achieved if controls are tested and verified to be in place by an independent auditor or other independent reviewer.

4 = 80% Effective. This is the target for demonstration of control effectiveness where determined on the basis of evaluation of a control via response to an assessment question or completion of a task, each with valid supporting documentation.

3 = 60% Effective. Documented control partly in place.

2 = 40% Effective. Control stated to be in place with no supporting documentation.

1 = 20% Effective. Control stated to be partly in place with no supporting documentation

0 = 0% Effective. No control in place or unknown.

* The Overall Risk and Control Effectiveness charts only include Third Party Organizational Risk because there are no systems owned by the Third Party listed in the System Inventory.

Third Party Control Effectiveness Summary

The Third Party Control Effectiveness Summary Table below outlines the Control Categories and References the third party organization was assessed against. The table includes information about the status of outstanding actions, number of pending actions, and the control effectiveness score for that Control Category.

Third Party Risk Assessment Type:
Standard Third Party Vendor Risk Assessment

Control Category	Status	Actions Pending	Control References	Control Effectiveness
Monitoring and Assurance	Action Required	3 of 3	• Continually monitor and periodically evaluate program maturity. • Periodically assess and audit the effectiveness of program controls and risk-mitigation.	20% (Below target)
Policies and Standards	Action Required	6 of 6	• Develop policies, procedures, and guidelines to define and deploy effective and sustainable governance and controls for managing data-related risks.	13% (Below target)
Processes	Action Required	8 of 8	• Establish, manage, measure, and continually improve processes for implementing all necessary controls to mitigate risks to appropriate levels.	10% (Below target)
Awareness and Training	Action Required	6 of 6	• Communicate about the value and risks associated with data as well as program and process expectations. Provide both general and contextual training, including professional certification training. Reinforce messages periodically.	13% (Below target)

TrustArc's Data Inventory, Mapping, & Vendor Risk Management Solution

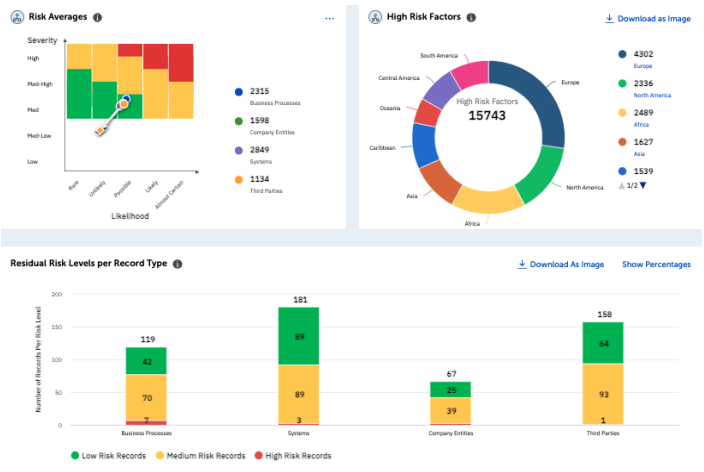
Data Inventory Hub

TrustArc's Data Inventory Hub helps organizations build and manage a data inventory, automatically generate visual data flow maps throughout the data lifecycle, and can automatically generate on-demand compliance reporting such as GDPR's Article 30, and automatically detect if any data element is at risk of non-compliance with CCPA.

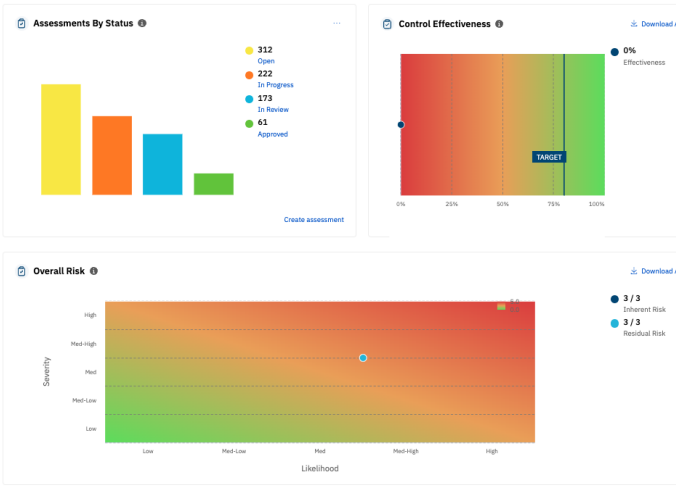
The "intelligence risk engine" within the product automatically analyzes a company's privacy risk based on GDPR high-risk principles and 650+ controls based on global standards, laws, and regulations.

The risk engine can automatically save up to 75% of the time it would take to analyze the risk manually and can seamlessly kickoff DPIAs PIAs, TIAs, and more using TrustArc's Assessment Manager for risk remediation and privacy risk assessments. Within the Risk Profile capability, jurisdictional analysis is available including country level legal framework analysis to streamline their data transfer risk analysis. This way all you need to do is focus on ensuring the appropriate safeguards are in place based on the data transfer risk.

Automatically score and evaluate privacy risk metrics within Data Inventory Hub, including Systems, Vendors, Company Affiliates, and Internal Processes.



Download and export automated company and vendor risk reports.



Generate automated follow up actions for each record and know when you need to conduct a PIA or Vendor Assessment.

Search here | Filters | Edit Columns

Record...	Record Type	Inherent...	Risk...	Risk...	Residual Risk	Data...	Data...	Action
NV BP Test4	Business Process	High	Start Assessment	None	Unavailable	Low	Start Assessment	...
NV Test3	Business Process	High	Start Assessment	None	Unavailable	Unavailable	Start Assessment	...
00--Test3.9	Company Entity	High	None	Incomplete	Low	High	None	...
NV BP Test2	Business Process	High	Start Assessment	None	Unavailable	Unavailable	Start Assessment	...
NV BP Test1	Business Process	High	Start Assessment	None	Unavailable	Unavailable	Start Assessment	...
Clone - Record...	Business Process	Incomplete	Start Assessment	None	Unavailable	Unavailable	Start Assessment	...
descriptionTest...	Business Process	Incomplete	Start Assessment	None	Unavailable	Unavailable	Start Assessment	...

Automate your data inventory, mapping and reporting, risk scoring, and risk remediation today!

Book a Demo

About TrustArc

As the leader in data privacy, TrustArc automates and simplifies the creation of end-to-end privacy management programs for global organizations. TrustArc is the only company to deliver the depth of privacy intelligence, coupled with the complete platform automation, that is essential for the growing number of privacy regulations in an ever-changing digital world. Headquartered in San Francisco, and backed by a global team across the Americas, Europe, and Asia, TrustArc helps customers worldwide demonstrate compliance, minimize risk, and build trust. For additional information visit www.trustarc.com.