



From Risk to Reason: Impact Assessments Explained

Protect rights. Reduce risk. Power up your privacy program.



Managing personal data in today's digital landscape means staying alert to privacy risks, especially when launching new systems, deploying AI, or updating technology.

Privacy assessments are your first line of defense: a proactive way to identify, evaluate, and manage privacy risks at every stage of development.



Your risk radar for data decisions

What are privacy assessments? Privacy assessments help you spot vulnerabilities before they become costly problems. Think of them as essential risk mitigation tools for any project involving personal data.



"Privacy assessments help you identify and mitigate risks before they escalate."

— Joanne Furtsch, VP, Privacy Knowledge, TrustArc

One size doesn't fit all. Choose smart.

Different risks require different tools. Here are the key types of assessments — and when to use them:

Type	Use It To	Applies When	Look For	Region/Notes
Privacy Impact Assessment (PIA)	Evaluate how a program or service may affect individuals' privacy	Launching new initiatives or systems with potential data impact	Known risks or potential harms to individuals' rights	U.S. and global programs
Data Protection Impact Assessment (DPIA)	Meet GDPR requirements for high-risk processing	Profiling, surveillance, AI, or large-scale data use	Legal obligations; EU blacklists / whitelists	Required under GDPR (Europe)
Legitimate Interest Assessment (LIA)	Determine if "legitimate interest" is a lawful basis for processing	Relying on Legitimate Interest as legal basis for processing	Purpose, Necessity, Balancing test (UK ICO guidance)	Recommended in UK/EU
Privacy Threshold Assessment	Decide if a deeper assessment (PIA/DPIA) is needed	Uncertain risk level of a data activity	Type of data, purpose, affected individuals, volume	Use ROPA to simplify
Transfer Impact Assessment (TIA)	Ensure lawful international data transfers	Sending personal data across borders	Safeguards in destination country; risk of access; protection equivalency	Essential for cross-border compliance

The benefits of being proactive

Assessments are strategic privacy tools that protect your business and your customers.



Regulatory Compliance

Stay on the right side of the law.



Early Remediation

Resolve issues before rollout.



Privacy by Design

Build privacy in from day one.



Transparency

Understand your systems and vendors.



Risk Identification

Spot risks before they become problems.



Cost Savings

Avoid expensive mistakes and rework.

Make your assessments count

- ☐ **Start early** — before data processing begins.
- ☐ **Revisit regularly** — especially if risks change.
- ☐ **Align** with regulations and internal risk tolerances.
- ☐ Use your **ROPA as a foundation** for threshold assessments.
- ☐ **Document everything** — your assessment is your evidence.
- ☐ **Revalidate** high-risk activities over time.

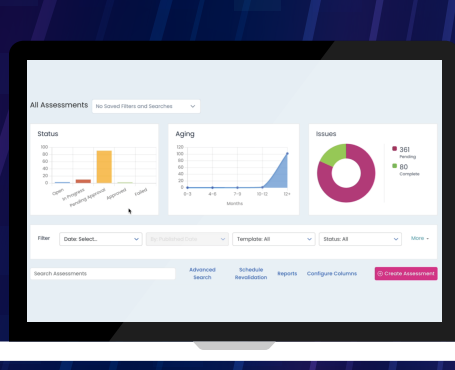
Each assessment is a snapshot in time. Make sure your safeguards evolve with your data.

Automate Risk Detection. Accelerate Compliance.

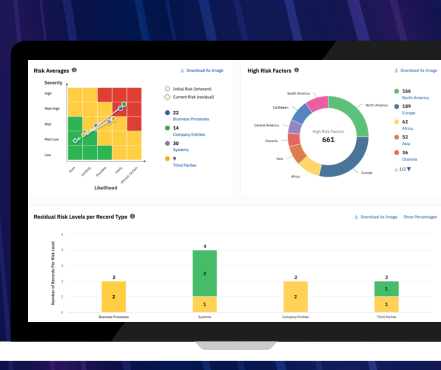
Manual assessments won't scale. TrustArc can.



Assessment Manager



Data Mapping & Risk Manager



Simplify and accelerate privacy and vendor assessments.

- Configurable workflows
- Automated remediation
- Built for your business processes

Map personal data and manage risk across your ecosystem.

- Intelligent data flow mapping
- Auto-risk scoring and TIA alerts
- Assessment recommendations at your fingertips

Quickly identify high-risk records, get instant assessment recommendations, and take action with TrustArc.

REQUEST A DEMO

Want more privacy power moves? [Explore the full Privacy PowerUp Series](#) for infographics, articles, and videos that put you in control.