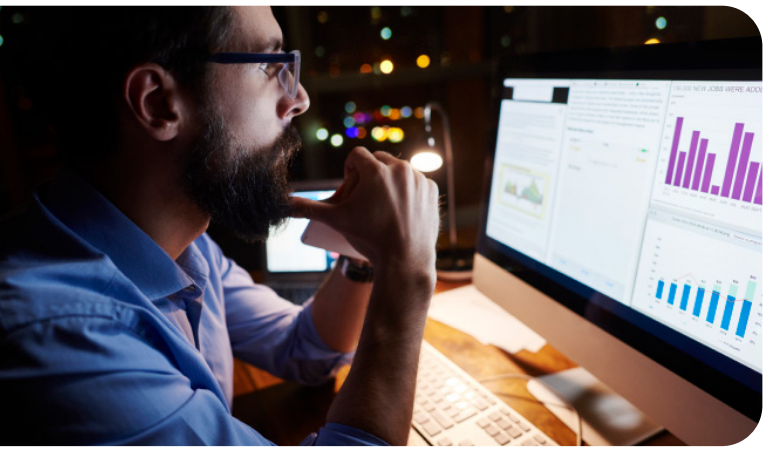
syrenis

GUIDE



Data Privacy Metrics: How to Measure the ROI of Privacy Programs

syrenis.com

Introduction

As privacy emerges as a hugely important business function, privacy programs rarely need to justify their existence in strict return-on-investment (ROI) terms.

That is, privacy is becoming a “table-stakes” function and programs typically do not have to prove that they cost less than they add in revenue or avoid in costs, like regulatory and legal costs.

However, organizations want to understand the value they receive and how the privacy program is succeeding. Also, any privacy program needs to track its own projects and trends.

In other words, while strict ROI measurements can be useful, strong metrics gathering is a must-have for any privacy program.

What Data Privacy Metrics Can You Track?

A strong set of metrics that creates a clear picture of program efficiency and effectiveness, identifies positive or negative trends, and tracks progress on goals is arguably the most important component of a mature program.

10 privacy metrics that organizations can use to measure the effectiveness of their privacy programs:

1. Data Breach Incidents:

- Number of data breaches experienced over a specific period.
- Severity and impact of each data breach, measured by the volume and sensitivity of data compromised.

2. Compliance Audit Results:

- Percentage of compliance audit findings related to privacy regulations (e.g., GDPR, CCPA) resolved within a defined timeframe.
- Number of compliance violations identified during audits and remediated appropriately.

3. Data Subject Requests:

- Volume and type of data subject requests received (e.g., access requests, deletion requests).
- Timeliness and accuracy of responses to data subject requests, measured by response times and completion rates.

4. Privacy Training and Awareness:

- Participation rates in privacy training programs and workshops across different departments.
- Results of privacy knowledge assessments or quizzes administered to employees.

5. Privacy Impact Assessments (PIAs):

- Number of PIAs conducted for new projects, systems, or processes involving personal data.
- Identification and mitigation of privacy risks and vulnerabilities through PIAs.

6. Privacy Policy Updates:

- Frequency of updates to the organization's privacy policy in response to regulatory changes or internal privacy program enhancements.
- Clarity and transparency of privacy policy language, measured by readability scores or user feedback.

7. Incident Response Time:

- Average time taken to detect and respond to privacy incidents or breaches, from initial detection to resolution.
- Effectiveness of incident response procedures in containing and mitigating the impact of privacy incidents.

8. Vendor Compliance:

- Percentage of vendors and third-party service providers compliant with the organization's privacy requirements.
- Results of vendor privacy assessments and audits conducted to evaluate compliance with contractual obligations.

9. Customer Trust and Satisfaction:

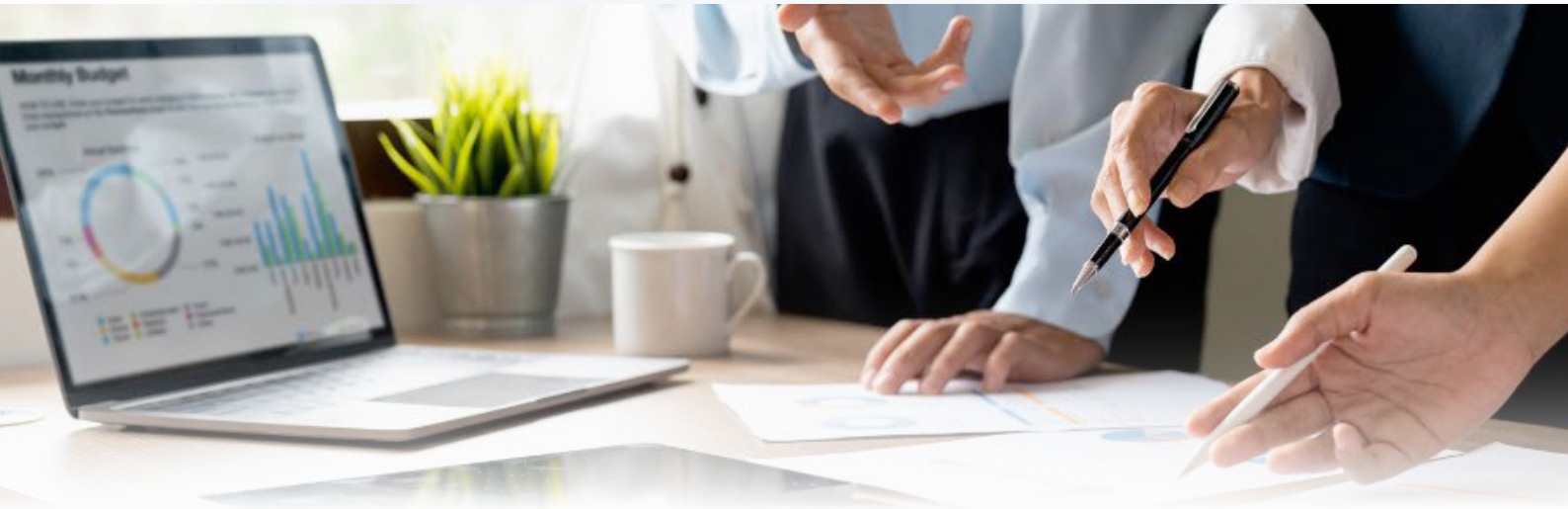
- Customer satisfaction and transparency scores.
- Net Promoter Score (NPS) or similar metrics measuring customer loyalty and advocacy based on perceived privacy protection.

10. Data Protection Investments:

- Total budget allocated to privacy and data protection initiatives, including technology investments, staff training, and compliance efforts.
- Return on investment (ROI) of privacy-related expenditures, calculated based on cost savings from avoided breaches or regulatory fines.

Metrics allow for targeted problem-solving, create strong business cases to back up budget requests, motivate workers towards a common goal, and demonstrate compliance with applicable laws and internal policies. Cost-benefit analyses, like time-to-market, revenue, receivables turnover, and profit are straightforward numbers to collect.

However, metrics related to functions that are typically considered cost centers are more challenging. How do you measure cost avoidance success? How do you measure consumer trust?



Common Metrics Chart

Organizations track a range of activities and trends, yet there is a fundamental set of privacy metrics that many organizations analyze to prove ROI. Typically, these metrics encompass daily activities within privacy programs, such as tallying individual complaints and requests, managing incidents or breaches, providing privacy compliance training to staff, conducting data mapping exercises, performing privacy impact assessments, negotiating data processing agreements, and more.

Naturally, the foundation of robust metrics lies in the acquisition of accurate and thorough data. Organizations differ in the categories and specific metrics they prioritize and report. The following chart, though not exhaustive, offers insight into some prevalent metrics.

Category	Item	Metrics
Individual Rights	Data Subject Requests (DSRs) Deletion Requests and Processing Objections	• Received • Closed • In progress • Duration • % satisfied and % satisfied within required time • Requests by type, region, SLA times
	Privacy Incidents/ Breaches	• # of incidents by type/severity/business unit/entity/region • # of impacted customers • % of incidents by type, closed with SLA commitments • % of incidents where root cause has been identified and corrective action taken • # and % of incidents notified to regulators and data subjects • # and % of incidents reported within X hours/days of determination • Mean time to discovery (measure of detective capability) • Mean time to resolve (measure of efficiency of processes)
	Privacy Complaints	Same metrics as Privacy Incidents/Breaches
	Privacy General Queries	Same metrics as Privacy Incidents/Breaches
		• Data sale and cookie opt-outs • Consent for processing activity • Consent for data sharing • Opt-in consent for email marketing

Category	Item	Metrics
Training and Awareness	Privacy Trainings Privacy Awareness and Education	• Offered • Employee training • % of targeted employee base who completed training on time • Attendees (in person) • % of employees passing privacy challenge • # of privacy certifications obtained • # of additional enablement materials created and viewed (e.g. awareness emails, news clippings, white papers, web pages, website visitors, internal playbooks, privacy champion Business Units (BUs), privacy champions)
	Privacy FAQs Processes and Guidelines Established	• Employee engagement • Functions in the organization that privacy engages with and who are the most frequent customers
Commercial	Data Processing Agreements (DPAs) Security/Data Protection Addenda	• Negotiated customer • Closed customer • Negotiated vendor • Tracking materially altered terms from standardized language • Timeframes to closure
	Vendor Reviews	• Vendor privacy reviews/risk assessments (# completed, # in process, # planned, # scores) • Vendor control assessments (# completed, # in process, # planned, findings) • PCI/DSS assessments and status for each vendor • Vendor privacy compliance issues (#, severity, status against target closure date, etc)
	RFI/RFP	• Privacy compliance attestation requests completed • Timeframes to completion • # of standardized privacy RFI/RFP Q&A available
	M&As/Divestitures/TSA/ Joint Ventures	• Negotiated/closed • Time to complete privacy due diligence • Number of remediation actions identified
	Supply Chain	• # Agreements for data sharing • % Agreements with privacy contractual language

Category	Item	Metrics
Accountability	Policy and procedures Notices (consumers, employees)	• # inventory • Whether current • Date last updated/reviewed
	Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs)	• # of identified high-risk data processing activities requiring a DPIA (as a % of total processing activities recorded/as a % of initial screening/gating assessments) • # of PIAs / DPIAs completed • Time vs SLA
	Transfer Impact Assessments (TIAs)	• # of transfer impact assessments (post Schrems II) • # of vendor questionnaires
	Data Mapping/Records of Processing Activities (RoPAs)	• # of applications data mapped • # of applications that require data mapping • % of required applications mapped/not mapped • # of completed RoPAs
	Regulatory	• # of regulator inquiries (type, opened, closed)
	Business Unit/Function	**Per Business Unit:** • Is a privacy steward or accountable person appointed? (Y/N) • Business unit privacy operating model in place and documented? (Y/N) • # and % privacy compliant apps processing PI • Progress status (R/Y/G or % complete) for outstanding BAU or regulatory change implementation actions • # and status (on track, overdue) of compliance monitoring/audit actions
Privacy Stewards (hub & spoke)	Privacy projects in product teams	• # of Personal Information Management Systems (PIMS) remediated • # of DPIAs supported • # of Rules of Procedure (ROPs) supported • # of department personal data use reviews for data extraction • # of cross-functional privacy projects • # of DSRs supported • # of department specific data privacy trainings offered • # of data privacy FAQs and awareness communications created (department/role-specific)
Policy	Legislative work Investor Ratings and Environmental Social Governance (ESG)	• Bills monitored • New laws • Review status • Rating agency scores

How Do You Develop a Set of Privacy Metrics?

An effective, right-sized, and targeted metrics program in the privacy space is hard to create. However, a simple step-by-step process to develop an approach to metrics can help ease the journey and result in a better outcome.

Following are high-level steps to develop a strong set of privacy metrics:

1. Determine Privacy Priorities
2. Consider the Type of Metric
3. Articulate Use
4. Define Stakeholders
5. Develop
6. Document a Process
7. Implement & Refine

1. Determine Privacy Priorities:
A “rule of thumb” for metrics is: we measure what is important and what we measure becomes important. This means that selecting the right, most important things is critical to a successful metrics program. The topics that are important will also change as the privacy program matures, and as the external and internal environments change, so it is important to re-evaluate how metrics align with priorities on a regular basis (see step 7).

For example, a young privacy program may have goals related to employee awareness and training, completing projects related to closing compliance gaps, and getting a handle on an effective individual rights process. On the other hand, a more mature privacy program might prioritize enhancing consumer data collection processes to increase trust, making individual rights management more efficient, and establishing a stronger third-party management program. Regardless of the program’s maturity or the organization’s specific privacy pressures, metrics should align with priorities.

2. Consider The Type of Metric:
For each priority, next an organization can consider whether the critical component is completion, quality, cost, or outcome and define metrics accordingly. In our previous example, the young privacy program has a goal of raising employee awareness and training.

In this second step, the organization will want to determine whether the critical component is completion of training development and implementation, quality of the training or understanding, cost to develop or implement relative to a budget and/or benchmark number, or training outcome/result.

3. Articulate Use:
Metrics for metrics’ sake are just numbers. Metrics that drive understanding and, finally, either confidence in current decisions or adjustments in practices, are power. Metrics take time and resources to collect, so unless the organization takes action using the knowledge that metrics provide, there is cost for no organizational benefit. A critical part of a metrics program is to understand – and document – how the organization will use the metrics.

In the young privacy program example, the organization may determine that it will use completion metrics to adjust developmental project plan steps to remove roadblocks. It may also use quality metrics to improve future training materials.

4. Define Stakeholders:
Metrics should be understandable and accessible by all relevant stakeholders. Carefully defining the stakeholders for each metric will help ensure that the people who can take action and make decisions have access to the data. Similarly, it will help the team display metrics in an understandable way and/or provide training for stakeholders so that they all understand deeply enough to make smart decisions based on data.

In our example above, the organization may determine that the privacy team overseeing the training development project should receive milestone/deadline information, are empowered to act if they see a concerning trend, and have the ability to understand the data as it is presented. The training development team may need to have access to quality metrics so that they can adjust future training or provide supplemental training.

5. Develop:
Once an organization understands the goals to measure, the type of metrics that are appropriate for each goal, how the organization will use the data, and who will use the data — defining the actual metrics becomes easy.

In our example young privacy program, which has a goal of raising employee awareness and training and wants to measure completion and quality, defining the metrics becomes straightforward. If the critical component is completion, the organization would measure project milestones against defined deadlines, or percentage of employees who have completed training. If quality measures are critical, the organization might measure employee satisfaction rates regarding the training or test scores on privacy concepts after training. A priority on cost could result in metrics related to dollars spent relative to a budget and/or benchmark number. Similarly, a priority on outcome could mean the organization would establish metrics relevant to post-training behavior improvement, such as tracking the number of customer complaints related to privacy issues.

Note that some metrics should have clear measurements for success. For example, if an organization establishes metrics related to training completion rates, it may be useful to set a definition of success – aiming at, say, 95%. Other metrics may be aimed more at tracking trends rather than defining success. These metrics may not have a success measure. For example, tracking numbers of individual rights requests might be aimed at the goal of having enough resources to fulfill the requests in the allotted time. Rather than including a success measure in the metric, it may be more appropriate to establish a decision trigger, such as 'when we reach more than 5 opt-out requests a day, we will meet to determine resourcing needs.'

6. Document a Process:
A documented process does not have to be elaborate or complicated, but even a one-page process flow map will help an organization be clear and rigorous about the when, who, how often, and expected outcomes of metrics collection and review. The process documentation might include background information that links goals, stakeholders, metrics, and any success measures and decision triggers. It may also detail data collection techniques and assumptions, plus a cadence and feedback loop and revision cycle description.

7. Implement & Refine:
Successful privacy programs mature, and certainly external and internal environments change over time. Metrics should evolve accordingly. A regular, perhaps annual, review and refinement of privacy metrics will help a privacy program continue to measure the right things and act appropriately.

Though, every organization's privacy program is different and so may benefit from different metrics, there is useful benchmarking research into privacy metrics. Specifically, the International Association of Privacy Professionals (IAPP) sponsors regular privacy governance research. Though the full report is only available to IAPP members, anyone can view the executive summary of the 2023 Annual Privacy Governance Report. In the full report, the IAPP describes the most common privacy topics about which organizations gather metrics. Top topics include PIA/PbD, privacy program, third-party management, privacy risk and controls management, and privacy policy management (updates and revisions).

syrenis

Contact Us
hello@syrenis.com

US Office
Suite 700, 3379 Peachtree Road NE
Atlanta, Georgia 30326, United States
+1 844 585 6264

UK Office
V2, Sci-Tech Daresbury, Warrington,
WA4 4AB, United Kingdom
+44 (0) 20 4551 9501