ISACA

GLOBAL EDITION

The State of Data Privacy IN 2024

Privacy continues to play an essential role in upholding and increasing digital trust, maintaining and growing positive reputations, and even preventing some cybersecurity incidents for organizations that prioritize it. As the data privacy landscape remains ever-changing and volatile, professionals who can fill in skills gaps have many opportunities for career growth ahead of them.

ISACA surveyed more than 1,300 professionals who work in data privacy roles to gather feedback on staffing, organization structure, policies, budgets, training and more. See key insights below and access the full global research report at www.isaca.org/privacy-in-practice-2024.

Data Privacy Skills in Demand

Privacy roles are in high demand in 2024,
but technical privacy roles are most needed.

TECHNICAL PRIVACY ROLES:
62% say there is increased demand

LEGAL/COMPLIANCE ROLES:
55% say there is increased demand

Previous Compliance/Legal experience
61% report previous compliance/legal experience as very important in determining if a privacy candidate is qualified, followed by **prior hands-on experience in a privacy role at 56%**.

BIGGEST SKILLS GAP AMONG PRIVACY PROFESSIONALS:
Experience with different types of technologies and/or applications **(63%)**

TO FILL PRIVACY SKILLS GAPS, ORGANIZATIONS ARE:
Training to allow non-privacy staff who are interested to move into privacy roles **(50%)**

Increasing usage of contract employees or outside consultants **(39%)**

Clarity and Confidence Remain Elusive

34%
Only one-third of organizations find it easy to understand their privacy obligations

43%
Less than half say they are *very or completely confident in their organization's privacy* team's ability to ensure data privacy and achieve compliance with new privacy laws and regulations

MOST COMMON OBSTACLES ORGANIZATIONS FACE WHEN FORMING A PRIVACY PROGRAM:

- **41%** Lack of competent resources
- **39%** Lack of clarity on the mandate, roles, and responsibilities
- **37%** Lack of executive or business support
- **37%** Lack of visibility and influence within the organization

Most Common Privacy Program Failures

PRIVACY BUDGETS

43% say their privacy budget is underfunded

ONLY **36%** say their budget is appropriately funded

TRAINING MUST BE A PRIORITY
Respondents cite the most common privacy failures as:

- **49%** Lack of or poor training
- **44%** Not practicing privacy by design
- **42%** Data breaches

86% indicate their organization provides privacy awareness training for employees

52% of organizations provide privacy awareness training to new hires

66% of organizations provide training to all employees annually

60% of organizations review and revise privacy awareness training at least annually

71% believe that privacy training has had a strong or some positive impact privacy awareness in the organization

The metric most used to track the effectiveness of privacy training is surprisingly not a **decrease in privacy incidents (56%)**, but the number of **employees completing training (65%)**.

MONITORING EFFECTIVENESS OF PRIVACY PROGRAMS IS MOST OFTEN DONE BY:

- **49%** Performing a privacy risk assessment
- **44%** Performing a privacy impact assessment (PIA)
- **38%** Performing a privacy self-assessment
- **34%** undergoing a privacy audit/ assessment

The Business Value of Privacy by Design

Organizations who practice Privacy by Design are more likely to:

Have more employees in privacy roles within their organization (15 vs. 9 among all respondents)

Say their technical privacy department is **appropriately staffed** (42% vs. 34% among all respondents)

Those who practice Privacy by Design place higher importance on the following qualifications:

Decrease privacy skill gaps by:

- Training to allow non-privacy staff who are interested to move into privacy roles
- Increased use of performance-based training to attest to actual skill mastery
- Increased reliance on Artificial Intelligence or automation

Use many more privacy controls in total, overall, than are legally required:

54%	50%	59%
Data minimization and retention controls	Data quality and integrity	Cryptographic protection

- **71%** Are much more likely to be very or completely confident in their organization's privacy team's ability to ensure data privacy and achieve compliance with new privacy laws and regulations
- **50%** Feel their privacy budget is appropriately funded
- **66%** More likely to look at the number of privacy incidents as a metric to assess effectiveness of privacy training

Overcoming skills gaps, utilizing privacy by design to facilitate trust, and allocating appropriate budgets and training will be essential for success in 2024 and beyond.

SOURCE: ISACA's Privacy in Practice 2024, www.isaca.org/privacy-in-practice-2024