iapp KPMG

# PR!VACY R!SK STUDY 2023

## EXECUTIVE SUMMARY

# Foreword

**This year's Privacy Risk Study represents the most comprehensive study of privacy risk undertaken by the IAPP in collaboration with KPMG.**

Since 2015, the IAPP has published an annual Privacy Risk Study to help determine trends in privacy risk management across demographics.

Beginning in 2017, analysis from Form 10-K submissions — annual public disclosures required by the U.S. Securities and Exchange Commission — was added to highlight the impact of privacy risk disclosures and the extent organizations publicly detail their personal data processing and privacy regulation methods.

This year, instead of just relying on public disclosures, we asked senior privacy leaders to explain their risk management practices. We also highlighted the results of interviews held with senior privacy leaders through workshops and interviews.

Ongoing regulatory change around the globe, new technologies (including artificial intelligence), and uncertainty from an inability to predict the future amplify privacy risks for organizations.

This study explores some of the most significant privacy challenges faced by organizations and what those organizations do to manage enterprise privacy risks. We believe this study can aid in developing a roadmap for managing and mitigating many of the privacy risks identified.

**Saz Kanthasamy**
Principal Researcher, Privacy Management, IAPP

**Sylvia Klasovec Kingsmill**
Global Cyber Privacy Leader, KPMG International
Partner, KPMG Canada

# Scope

## Our analysis uses three discrete data sets:

1. Workshops held with senior privacy leaders in 2022. We asked participants to enumerate, rank, categorize and plot their privacy risks for the year. This information was then collected and analyzed to determine what kind of risks are top of mind for senior privacy professionals.

2. Interviews with privacy leadership from 14 variously sized organizations in 2022 and 2023. Participants, representing six different industry sectors and three continents, were asked a series of questions regarding four different domains of privacy risk. These answers were then entered into a standardized matrix to help us understand trends across participating organizations.

3. Annual reports, 10-K forms and other publicly available external disclosures from organizations from 2022 and 2023.

# Executive Summary

## While the complexity, variety and scale may vary from organization to organization, all organizations that process personal data contend with privacy risk.

Whether it's uncertainty in the ability to deliver on a privacy compliance program for the next year due to ongoing regulatory change, the challenge of obtaining and subsequently maintaining full compliance with proliferating, and even conflicting, privacy laws around the world, or uncertainty from inability to predict the future — organizations need to find ways to identify, assess, evaluate and treat privacy risk.

In this climate, organizations increasingly have to grapple with a complex privacy risk environment fraught with regulatory and economic uncertainties. It is an environment replete with new and evolving harms through the proliferation of emerging technologies, changing consumer expectations on privacy, and increasing scrutiny on business initiatives and market trends.

In this year's report, privacy leaders identified geopolitical instability, rapidly maturing and emerging technologies, lack of available talent, and increasing shareholder and regulatory expectations as some of the most significant challenges, revealing concerns about an increasingly fragmented and unpredictable world.

Against this backdrop, we found organizations taking steps to manage enterprise privacy risks considered the following to support the identification, assessment, evaluation and treatment of privacy risk: Roles and responsibilities, methodology, technology, communications and continuous improvement.

# Key takeaways

→ The five highest priority privacy risk domains identified by participants were data breaches, noncompliant third-party data processing, ineffective privacy by design implementation, inappropriate personal data management and insufficient privacy training for employees.

→ The most common and most emerging privacy risk identified by participants was difficulty maintaining compliance across various regulatory regimes with differing and/or evolving requirements.

→ Additional top-ranked emerging risks included balancing data localization requirements with EU business needs, unintended consequences due to immaturity in managing the privacy risks that occur through the use of AI and privacy risks resulting from efforts to monetize data.

→ Regulation/compliance, data management and governance were the top three most common risk domains identified by participants.

**21%**

Only about 21% of organizations empowered the third line of defense to undertake privacy audits.

**30%**

Almost 30% of organizations use spreadsheet technology to help manage their privacy risk efforts.

**50%**

Only 50% of organizations have an established privacy risk appetite.

**64%**

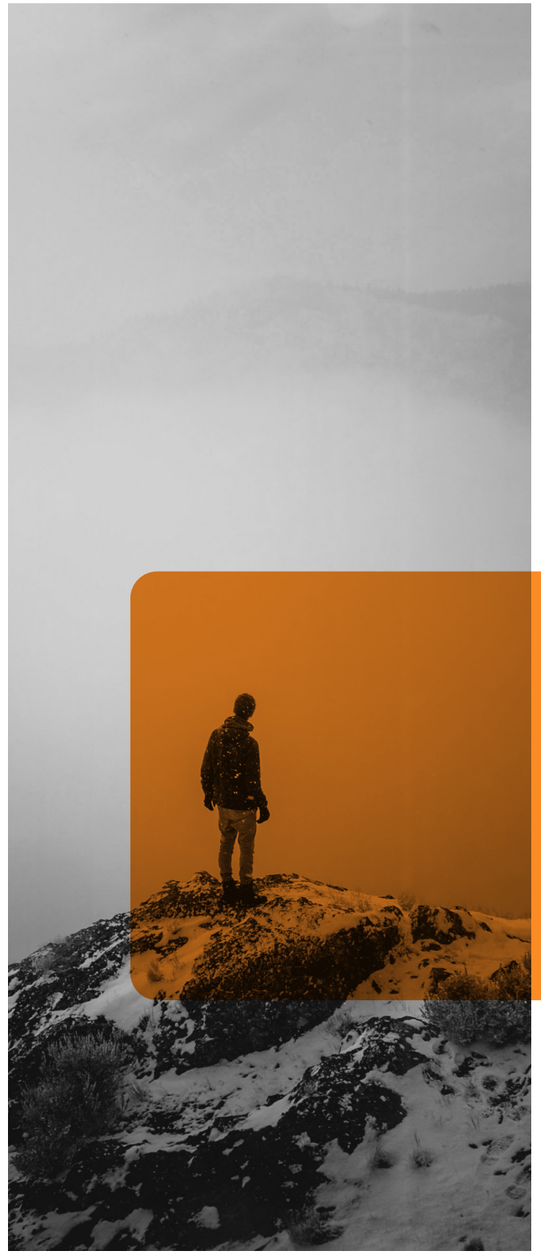
64% of organizations have a privacy risk management program that is fully integrated into their overall enterprise risk management program.

**83%**

83% of organizations place some kind of privacy risk information in their annual report.

**93%**

Almost 93% of organizations indicated privacy is a top-10 organizational risk, and 36% ranked it within the top five.



# Contacts

**Saz Kanthasamy**
Principal Researcher, Privacy Management, IAPP
skanthasamy@iapp.org

**Brandon Lalonde**
Research and Insights Analyst, IAPP
blalonde@iapp.org

**Joe Jones**
Director of Research & Insights, IAPP
jjones@iapp.org

**Sylvia Klasovec Kingsmill**
Global Cyber Privacy Leader, KPMG International
Partner, KPMG Canada
skingsmill@kpmg.ca

## Follow the IAPP on social media

Published June 2023.