accenture

# PRIVACY - STATURE AND SUSTAINABILITY IN THE INFORMATION AGES

# Accenture's 2019 Privacy Study

Based on a survey of 100 privacy executives across North America and Europe—highlights that financial institutions continue to face significant residual privacy risk following recent changes in regulatory focus and lack a plan to deliver a sustainable operating model. Furthermore, while the onset of consumer rights regulation presents a rare opportunity to elevate a regulatory response to a platform for competitive differentiation, fragmented responsibilities among study respondents are preventing financial institutions from realizing broader business objectives.

# Executive Summary

## Gaining stature, not just visibility

Evolution of privacy regulation to encompass consumer rights, first precipitated by Europe's General Data Protection Regulations (GDPR) and subsequently the California Consumer Protection Act (CCPA) in the United States, has elevated the visibility of privacy with 70% of 2019 Privacy Study respondents considering it a key material risk. With over half of respondents identifying privacy risk monitoring as the level of risk remaining after controls have been developed and applied, focus now turns toward establishing a Privacy function with the capabilities commensurate to this new status.

## Joining the dots with security and data

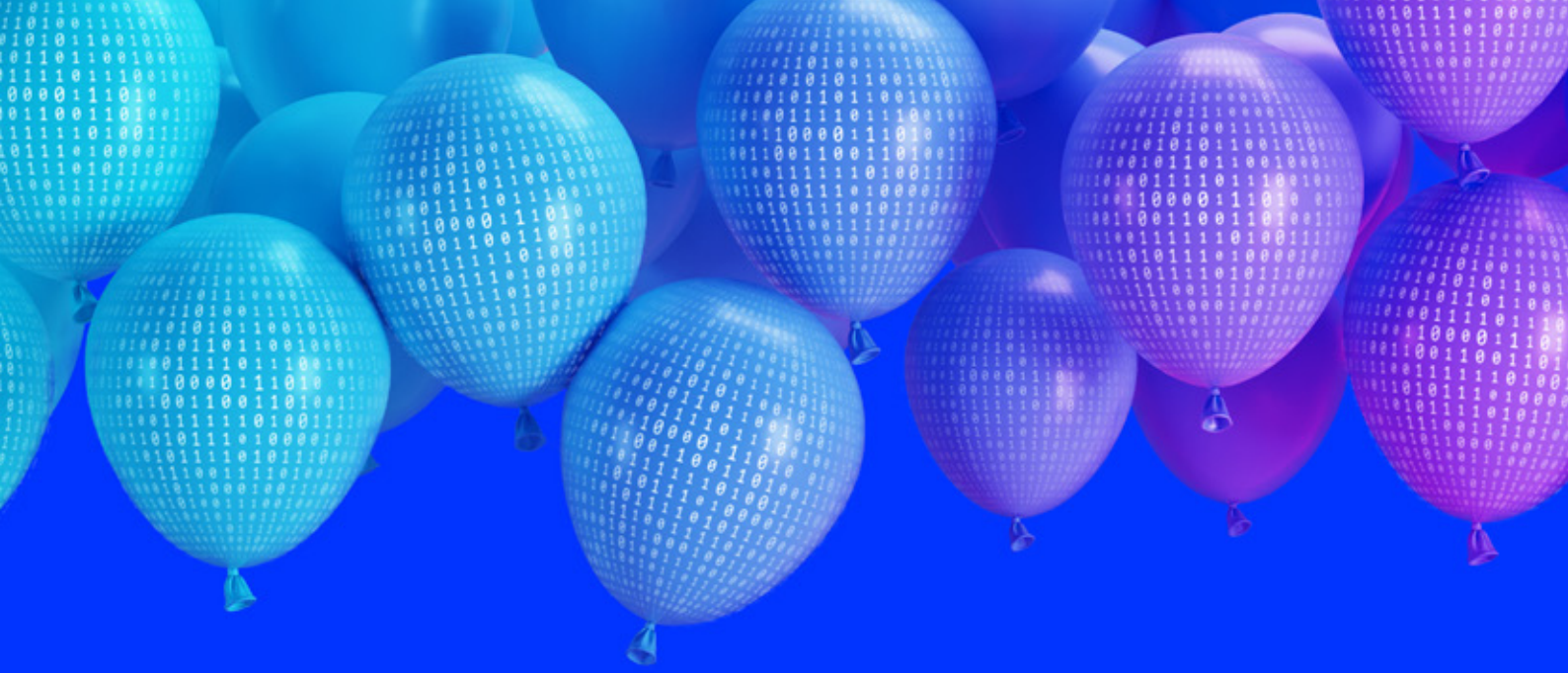
The importance of establishing the stature of Privacy is underscored by the interconnected nature of privacy, security and data risks. Such dependencies necessitate an effective engagement model with Information Security and Data Management for Privacy and yet over 70% of financial institutions surveyed as part of Privacy Study organize these domains separately. Symptoms of this separation can be seen by concerns with the effectiveness of adjacent controls, with 41% of respondents seeing records and information management as a major residual risk, and the severity of these challenges can only deepen as additional regulations threaten to shine a light through organizational cracks.

## Capturing a broader value proposition

The speed of business in the information age heightens privacy, security and data risks though also presents opportunity to elevate customer experience through hyper-personalization of services. Our Global Financial Services Consumer Study indicates consumers are willing to share information when there is perceived value exchange. Over-indexing responses so they become solely a compliance activity may therefore impede broader value propositions for the business. While 72% of Privacy Study respondents indicate their organizations use consent, this is the start of a journey for financial institutions to leverage compliance as a platform for differentiated customer experience and a competitive advantage, as evidenced by 87% of firms experiencing sales delays due to privacy concerns from customers according to an industry study.

## Charting a bold, sustainable path forward

Establishing the stature of the Privacy function, communicating expectations of other stakeholders, and capturing broader business opportunity requires clarity of strategy and yet 1 in 3 financial institutions surveyed as part of the Privacy Study lack a clear roadmap and the resources to address their residual privacy risks. Pressure on privacy executives to communicate a clear plan is increased by the 55% rise in the perceived impact of data breaches over the last two years, and the increased resources to be made available over the next 12 months among three-quarters of respondents. Bold moves are required to accelerate the journey for Privacy, built on the fundamentals of a control framework reflective of the new reality of risk in the information age and focused on delivering sustainable value to the business.



# GAINING STATURE, NOT JUST VISIBILITY

Privacy risk is not new for financial organizations though it has evolved into a holistic view encompassing consumer rights, precipitated by Europe's General Data Protection Regulations (GDPR) and subsequently in the United States by the California Consumer Protection Act (CCPA).

Furthermore, the proliferation and impact of data breaches, the recognition of the value of data, and renewed regulatory focus—including significant fines in Europe amounting to approximately $126 million to-date—has elevated the visibility of privacy, with 70% of Accenture's 2019 Privacy Study respondents considering it a key material risk.

The consumer centricity of regulations underlines privacy's emergence as a risk that every individual at virtually any financial institution can impact. As such, privacy provides a further use case for the shift in accountability for compliance towards the first line of defence outlined in our Compliance Risk Study last year. This is also indicated by the increasing focus of appointing accountable leaders for privacy programs in the first line of defence, to own the new business process and workflows required by regulation.

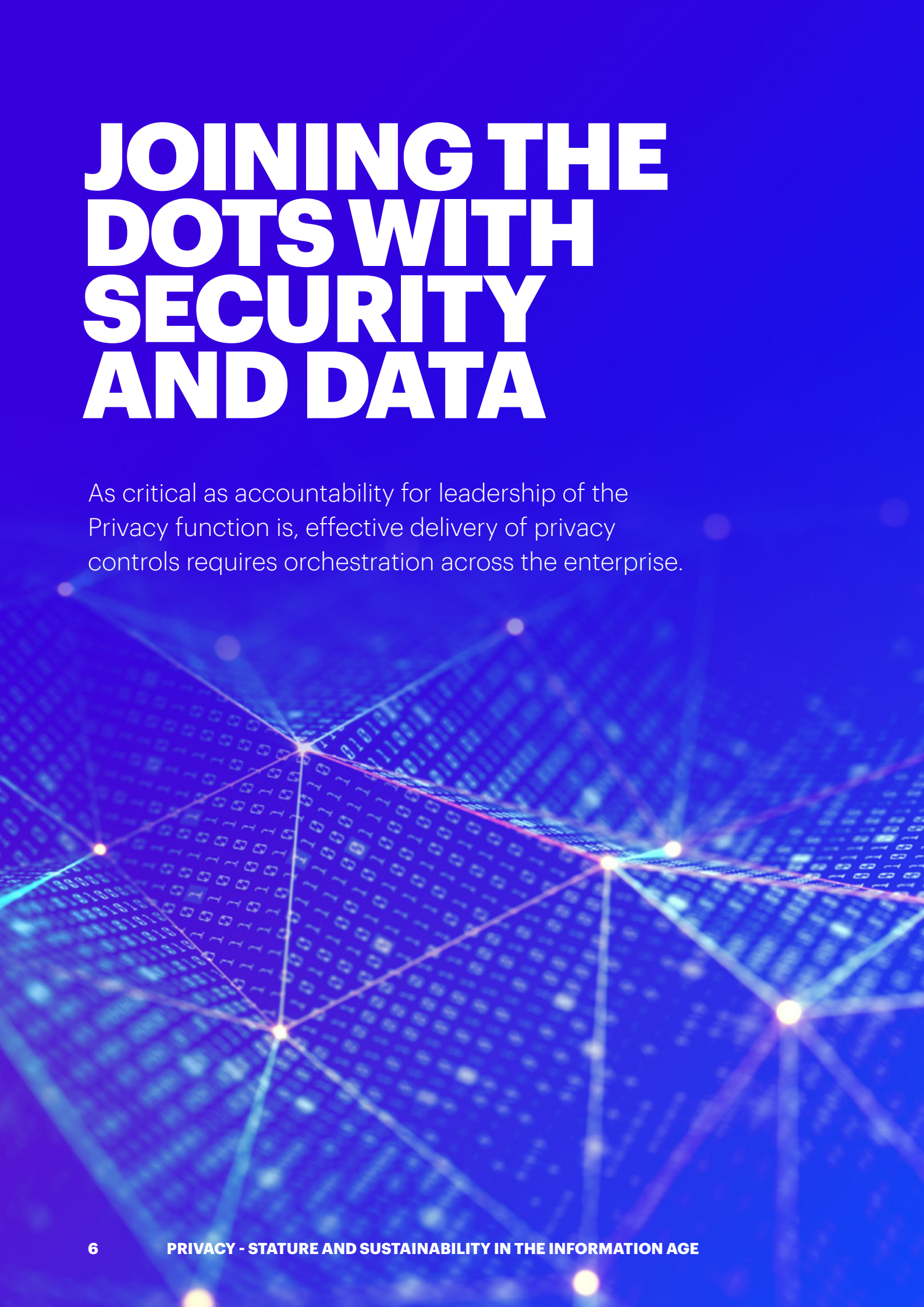
However, beneath the regulatory headlines and increased first line engagement, concerns regarding stature and sustainability remain. Over half of 2019 Privacy Study respondents identify privacy risk monitoring as a key residual risk, highlighting the need for capabilities commensurate with privacy's status as a material risk. Automated tooling to drive data discovery and subsequent detective controls, in conjunction with dedicated workflows with clear accountability to drive consistent and efficient servicing of consumer requests are examples of the fundamentals that should be in place.

Privacy executives might look at the evolution of compliance following the financial crisis or the comparatively recent—and quicker—rise to prominence of information security. Both functions have had to establish stature at pace following regulatory impetus, balancing the focus on core control frameworks with effective technology planning. Much as these precedents are available, and the regulatory case for change evident, the challenge remains for Privacy to establish its stature and deliver a sustainable operating model across the first and second lines of defence.

Over half of 2019 Privacy Study respondents identify privacy risk monitoring as a key residual risk, highlighting the need for capabilities commensurate with privacy's status as a material risk.

# JOINING THE DOTS WITH SECURITY AND DATA

As critical as accountability for leadership of the Privacy function is, effective delivery of privacy controls requires orchestration across the enterprise.



Information Security and Data Management have been partners in the first line of defence for several years though the onset of consumer rights and its dependencies for effective third-party management places further premium on closely managing these inter-dependencies. In several financial institutions, double-hatting the role of the Chief Information Security Officer to be the Chief Privacy Officer has been an organizational response, yet over 70% of financial institutions surveyed as part on the Privacy Study organize the domains of privacy, information security and data management separately.

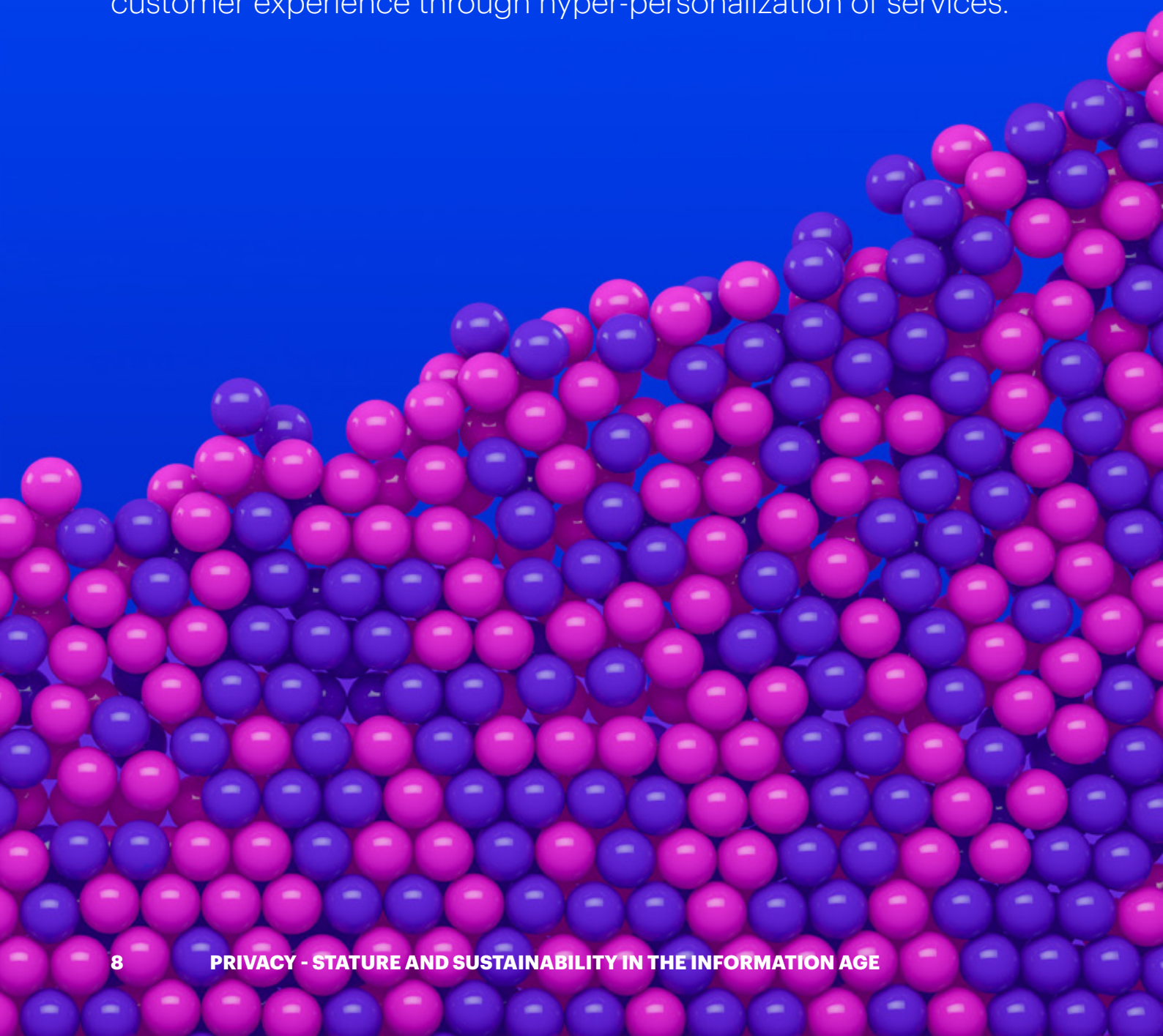
Establishing an engagement model across multiple parties can be challenging, and further complexity for financial institutions is expected as Operations, Marketing and Procurement all become part of the day-to-day network of functions that require the effective orchestration for privacy. Symptoms of the challenges to-date can be seen by concerns with the effectiveness of controls whose delivery rely on multiple teams. For example, 41% of Privacy Study respondents see records and information management, itself a major dependency for effective decisioning of "right to erasure" requests under GDPA and CCPA, as a major residual risk. However, without concerted action the risks impacting the business should continue to compound, a trend somewhat reinforced by our 2019 Global Risk Management Study which reported that 89% of risk managers are not fully capable of assessing risks associated with adoption of new technologies such as artificial intelligence (AI).

Financial institutions able to incorporate "privacy by design" as a key consideration of customer journeys are well positioned to embed privacy beyond the perimeters of the function. Providing privacy by design principles for new technology deployment, such as abilities to activate depersonalization of data or to dispose of information on request, has been a key focus for financial institutions in recent months. Incorporating these disciplines in day-to-day decisions are critical complements to more traditional forms of collaboration, for example in responses to cybersecurity events such as malicious data loss and associated regulatory engagement.

The challenge presented to the first line of defence to strengthen their engagement model can be a mirror to that presented to the second line of defence. Consumer-centric privacy regulations have in many cases driven revisions to governance structures, new business processes and the introduction of new technologies. Each of these components introduce elements of operational and compliance risks that require comparable revision to control frameworks and resources for their effective execution. All this at a time, especially in the United States, of ongoing flux in the regulatory environment that is expected to continue to expose financial institutions slow to identify and manage changes in their risk profile.

# CAPTURING A BROADER VALUE PROPOSITION

The speed of business in the information age compounds privacy, security and data risks though also presents opportunity to elevate customer experience through hyper-personalization of services.



The speed of business in the information age compounds privacy, security and data risks though also presents opportunity to elevate customer experience through hyper-personalization of services. Our consumer research previously indicated that 70% won't do business with a company they can not trust to keep personally identifiable information (PII) safe. Though on the flip side of this equation, more than three-quarters of consumers surveyed by Accenture are willing to share the data required for benefits such as personalized offers, more efficient and intuitive services, and more competitive pricing. And an almost equal number (73%) are willing to share more personal information if companies are transparent on its use.

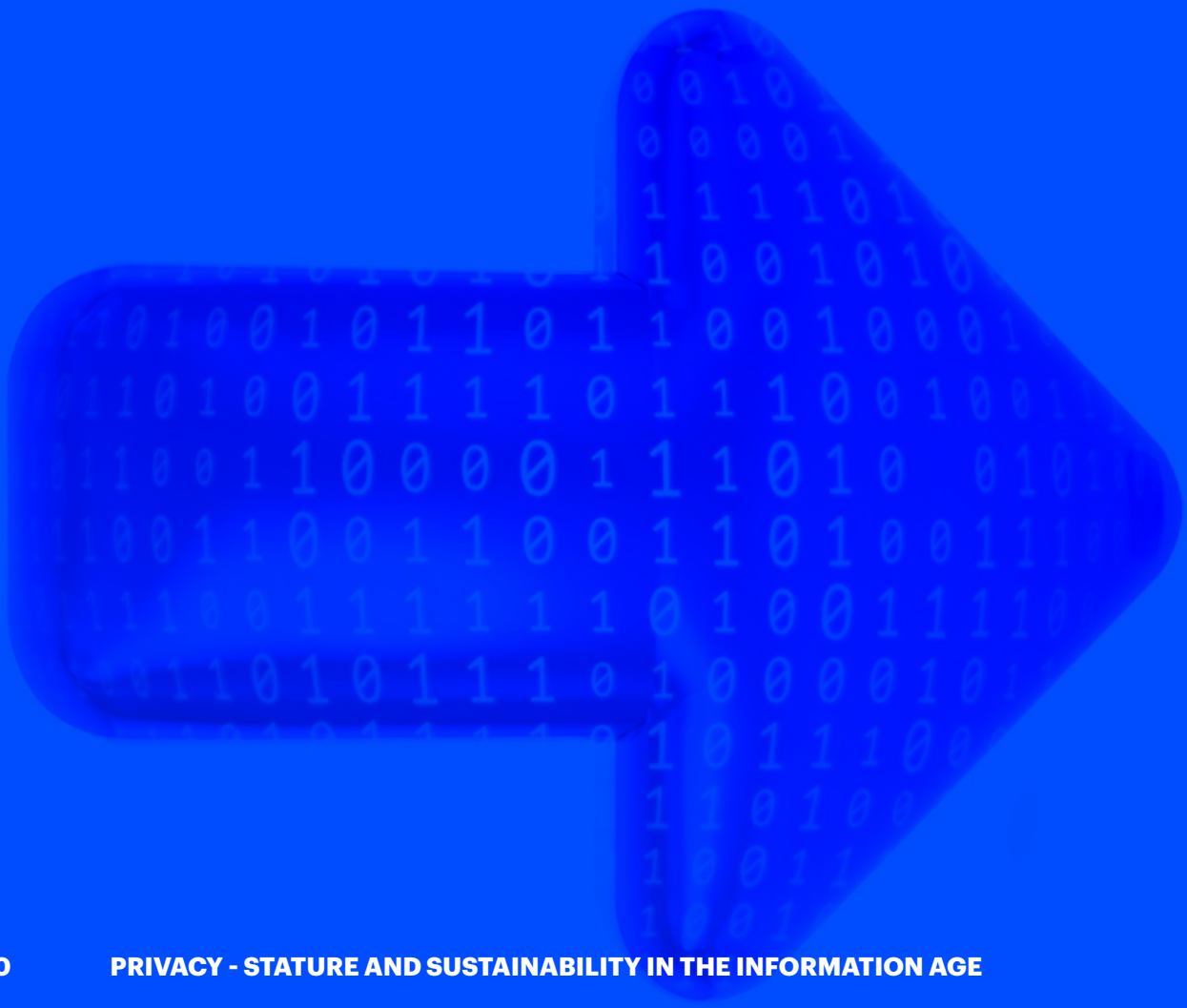
Financial institutions that are able to understand how people perceive and value data privacy, and the behavioral triggers that impact how they manage it, have an opportunity for differentiation. In taking inspiration from other industries, financial institutions might consider how organizations are differentiating themselves with consumer journeys that are as innovative as a wearable technology that allow for users to augment their experience. In this instance, consumers have been willing to share their information because they are benefiting from it. At the same time, managing consumer experience is important by avoiding practices that make a consumer uncomfortable, such as showing the same ad across devices or ads on a social media site based on shopping history on another site. In practice this should inform development of the privacy framework to be more than a practice focused solely on compliance to one that partners with the business to offer differentiated customer journeys and experience.

Seven in ten (72%) Privacy Study respondents indicate their organizations use consent to tailor customer-facing products and services, though leading financial institutions are making further strides to integrate their privacy programs into their broader value proposition. Examples include combining data design preferred practices with qualitative insights to better communicate how data is stored and used, or positioning consumers with decisions which are most relevant to them such as noteworthy changes in spending behaviours. Replicating and scaling these examples feels like a natural part of the journey for financial institutions to leverage Privacy as a platform for differentiated customer experience and a competitive advantage.

The speed of business in the information age compounds privacy, security and data risks though also presents opportunity to elevate customer experience through hyper-personalization of services.

# CHARTING A BOLD, SUSTAINABLE PATH FORWARD

Capturing broader business opportunity, in parallel to establishing the stature of the Privacy function, and communicating expectations of other stakeholders requires clarity of strategy, yet 1 in 3 Privacy Study respondents lack a roadmap to address their residual privacy risks.



As previously mentioned, with data breaches having risen in their perceived impact by over half during the past two years the pressure on privacy leaders to communicate a clear strategy has further increased. Additional expectations come from the increased resources being made available for the function as 76% of respondents expect to receive additional funding for the Privacy function over the next 12 months.

Bold moves are required to accelerate the journey for Privacy, built on the fundamentals of a control framework reflective of the new reality of risk in the information age and focused on delivering value to the business. Leaders are likely to be those that can distil lessons learned from prior maturity journeys in areas such as compliance and information security, as well as those that can evidence the leadership required to drive concerted action across multiple stakeholders, infusing a culture of privacy awareness throughout the organization.

Such moves are critical amidst a regulatory and industry landscape that continues to evolve. Engaging beyond the four walls of organizations to connect with peer leaders and industry forums such as the Business Roundtable in the United States can add a further dimension to planning for the Privacy function of the future. The emphasis on the privacy leaders of today to clarify their strategy and elevate their functions is a precursor to organizations positioning themselves to take advantage of a window of opportunity to create market differentiation by reducing barriers to furthering customer trust.

Bold moves are required to accelerate the journey for Privacy, built on the fundamentals of a control framework reflective of the new reality of risk in the information age and focused on delivering value to the business.

# About the Authors


## Ben Shorten

Ben is a Managing Director – Accenture Financial Services, Finance & Risk and leads the Compliance & Privacy offerings group for Financial Services in North America. He has extensive experience across corporate, investment and retail banking, as well as insurance, delivering regulatory responses to privacy regulation globally and in parallel establishing the capabilities to provide and sustain privacy operating models of the future.

Ben can be reached at:
**benjamin.j.shorten@accenture.com**

## Iain Duke-Richardet

Iain is a Director – Accenture Financial Services, Finance & Risk. Iain has broad Financial Services and management experience, and is a thought leader on risk and compliance guidance topics including compliance function structure and management, global technology-related legal and regulatory issues, books and records, cybersecurity, and privacy.

Iain can be reached at:
**iain.duke-richardet@accenture.com**

## Umer Hamid

Umer is a Senior Manager – Accenture Financial Services, Finance & Risk and is the General Data Protection Regulation (GDPR) Lead for Financial Services across Europe, Asia and Latin America. He is an experienced GDPR practitioner who brings deep industry insights and practical implementation experience across all GDPR capabilities.

Umer can be reached at:
**umer.hamid@accenture.com**



## Acknowledgments

The authors would like to thank the following Accenture employees for their contribution to this document: Anwar Ali and Dino Landingin.

## About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 505,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is **www.accenture.com**



200185

## References


1 "2019 Accenture Global Financial Services Consumer Study." Access at: https://www.accenture.com/us-en/insights/financial-services/financial-services-consumer-study-2019.

2 "Consumer Privacy Survey – The growing imperative of getting data privacy right," Cisco Cybersecurity Series 2019. Access at: https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf.

3 Risks associated with data and privacy breaches have seen the second-biggest increase in perceived impact: 55 percent of financial services firms say they have a greater impact today than they did two years ago. "Accenture 2019 Global Risk Management Study – Financial Services Report." Access at: https://www.accenture.com/us-en/insights/financial-services/global-risk-study.

4 "DLA Piper GDPR Data Breach Survey 2020," DLA Piper, January 20, 2020. Access at: https://www.dlapiper.com/en/us/insights/publications/2020/01/gdpr-data-breach-survey-2020/.

5 "Accenture 2019 Global Risk Management Study - Financial Services Report." Access at: https://www.accenture.com/us-en/insights/financial-services/global-risk-study.

6 "2018 Global Consumer Pulse Research," Accenture.

7 "2019 Accenture Global Financial Services Consumer Study." Access at: https://www.accenture.com/us-en/insights/financial-services/financial-services-consumer-study-2019.

8 "Accenture Interactive's 2019 Consumer Pulse Survey." Access at: https://www.accenture.com/us-en/insights/digital/see-people-not-patterns

9 "Your Personal Avatar Can Now Board a Cruise Ship With You," Wired, January 3, 2019. Access at: https://www.wired.com/story/carnival-medallion-cruise-tagalong-avatar/.

10 "Accenture Interactive's 2019 Consumer Pulse Survey." Access at: https://www.accenture.com/us-en/insights/digital/see-people-not-patterns

11 "Accenture 2019 Global Risk Management Study – Financial Services Report." Access at: https://www.accenture.com/us-en/insights/financial-services/global-risk-study.