Predicts 2020: Embrace Privacy and Overcome Ambiguity to Drive Digital Transformation

Published: 14 November 2019 **ID:** G00463442

Analyst(s): Bart Willemsen, Nader Henein, Bernard Woo

Privacy and data protection are enforced by a growing number of regulations around the world. These predictions highlight for security and risk management leaders the correlation between new technology and regulatory impact, customer dependency, and commercial opportunity.

Key Findings

- People are actively demanding privacy protection — and legislators are reacting. More than 60 countries have introduced privacy laws in response to citizens' cry for transparency and control.
- Myriad requirements protect privacy value and demand control over personal data throughout the data life cycle, forcing organizations to meet customer demand, demonstrate transparency and notice, use personal data purposefully, and exercise control over that data in every aspect of the life cycle.
- Regulations drive organizations to position a capable, empowered senior-level privacy officer to enable, monitor and enhance both compliance maturity and customer satisfaction.
- Subject rights request (SRR) and universal consent and preference management (UCPM) are among the tools purchased by organizations to establish and maintain their privacy programs. As the program evolves, additional technologies like pseudonymization, anonymization, masking and privacy preservation in analytics and business intelligence (ABI) are parts of the program's evaluation.

Recommendations

Security and risk management (SRM) leaders who focus on technology, information and resilience risk should:

- Drive the privacy program at scale by automating repetitive and high-traffic use cases. Two areas that represent opportunities for automation are SRRs and UCPM.

- Be proactive by adopting governance agility instead of responding to each jurisdictional challenge. To get ahead of the curve; build a holistic and adaptive privacy program that scales across the organization.
- Ensure privacy risk is observed and managed across the organization by appointing a privacy or data protection officer (DPO); or, if the span of control needed is too large for one person to oversee, establish a central privacy office.
- Pursue enhanced privacy management, compliance insight and privacy control over personal data by first using existing capabilities from bordering disciplines. Plan to spend additional budget on new capabilities.

Strategic Planning Assumptions

Before year-end 2023, more than 80% of companies worldwide will be facing at least one privacy-focused data protection regulation.

By 2023, 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% today.

By year-end 2022, more than 1 million organizations will have appointed a privacy officer (or data protection officer).

Through 2022, privacy-driven spending on compliance tooling will break through to over $8 billion worldwide.

Analysis

Last year, Gartner observed that general customer dissatisfaction, erosion of trust and privacy invasion are increasing. Today, we find that these sentiments extend into all interactions between customers, organizations and devices. Lawmakers continue to respond by creating new privacy and data protection laws. Industries respond to these laws for reasons of compliance. Yet, a proactive approach to privacy and data protection helps organizations increase success, improve image and raise customer trust levels by enhancing customer engagement and establishing a companywide, proactive and competitive privacy program (see "IT Score for Privacy").

What You Need to Know

Gartner observes a global movement of modern privacy and data protection laws in the making that are in line with many of the principles encountered in the EU's General Data Protection Regulation (GDPR). The resulting granular control over personal data will drive organizations to acknowledge the business-enabling characteristics of customer trust and satisfaction.

Privacy requirements have an impact on staffing and the implementation of new technology. Various technology developments will fail over time as they insufficiently address privacy-by-design and protection-by-default principles. Meanwhile, evolving regulatory challenges require adoption of

modern technologies to adequately manage risk of noncompliance, to control personal data from ingestion or creation during its life cycle and including end of life, and to improve the privacy UX (see “Practical Privacy — A Definitive Guide to Privacy UX”).

Strategic Planning Assumptions

Strategic Planning Assumption: Before year-end 2023, more than 80% of companies worldwide will be facing at least one privacy-focused data protection regulation**.**

Analysis by: Bart Willemsen

Key Findings:

- Organizations can be confronted with data protection requirements in a variety of ways. This can include where a customer (citizen, employee, consumer, patient etc.) is protected, where the organization is established, and as part of the supply chain (including acting as someone’s data processor or subprocessor).
- After implementation of the EU’s GDPR, Gartner observed more than 60 jurisdictions that have enacted postmodern privacy and data protection laws, or that are writing and proposing bills to that end. These include jurisdictions around the world, such as Argentina, Australia, Brazil, Egypt, India, Indonesia, Japan, Kenya, Mexico, Nigeria, Panama, the U.S., Singapore and Thailand (see Note 1).
- Failure to comply increasingly bears a heavy cost. We are seeing considerably raised stakes regarding financial sanction options (e.g., $7,500 *per impacted individual* in case of a deliberate transgression; for GDPR it’s a maximum of 4% of annual revenue); but there are also personal jail sentences possible and civil codes (e.g., Mexico[1]).

Market Implications:

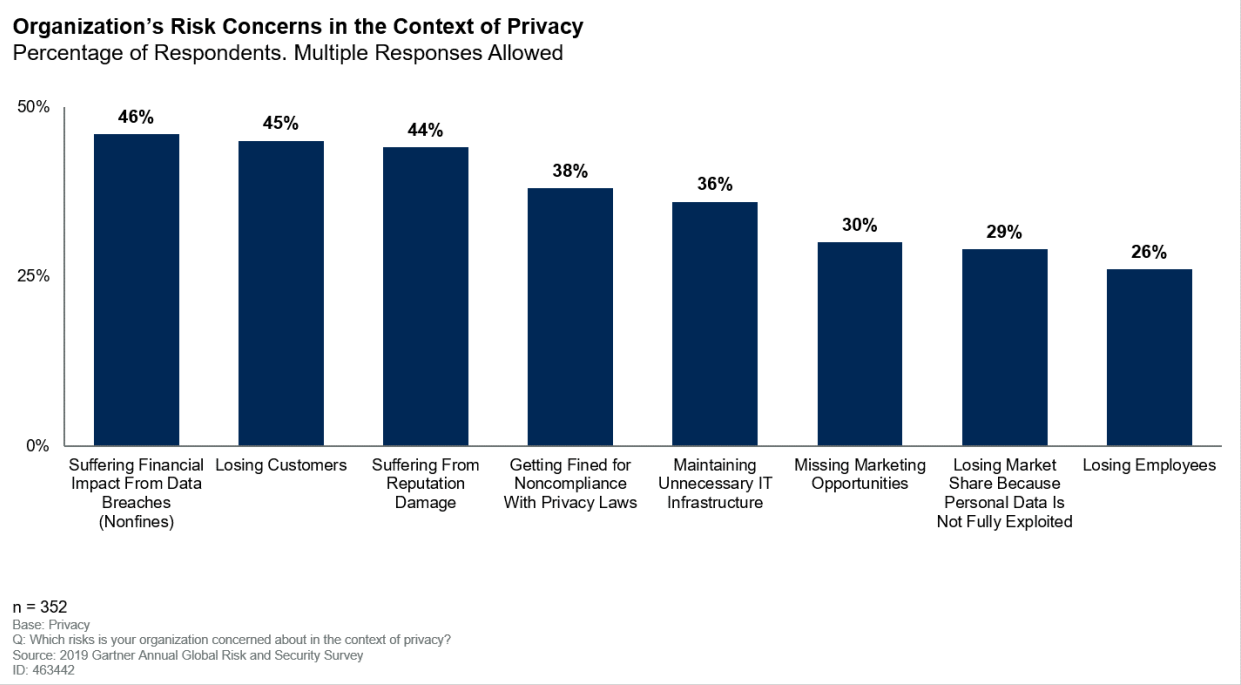
Organizations that operate internationally are facing a new operating environment where they need to comply with many if not all of these new laws. Hence they have a choice to make: They can complete a readiness project for each law as it comes into effect or they can build a foundational privacy program based on principles or common elements shared by the majority of data protection laws. Thus, adjustment would be needed only as necessary to specific requirements found in each jurisdiction’s laws. Obviously, the latter is preferred.

Organizations must stay up to date through professional legal and privacy feeds and establish consistent norms in handling personal data through a (global) privacy management program. Organizations can be confronted with both domestic privacy laws or those abroad, with laws protecting a customer or an employee; and through collaborative partnerships as part of a supply chain. In all cases, encountering requirements that protect the privacy value and demand control over personal data from the onset to the end of the data life cycle will be unavoidable. These requirements force organizations to meet customer demand, demonstrate transparency and notice, use personal data purposefully, and exercise control over that data in every aspect. There will be a

need for privacy-enhancing technologies, privacy management and compliance documentation, and operational data-centric controls. The postmodern privacy era of today triggers multiple jurisdictions to establish new privacy laws, impacting how organizations treat personal data. Customers demand the ability to exercise their privacy rights and will move to the competition if they feel they're ill-served in that respect. To maintain a competitive advantage, and to continue successful international digital business, every organization needs to proactively address shortcomings in the privacy discipline.

Organizations that choose to ignore the requirements found in data protection laws ignore them at their own peril, as they all include some form of financial penalty that can be administered by regulators for noncompliance. In some cases, there's even a risk of considerable jail sentences. Recent scandals have left consumers much more alert to the privacy practices of the organizations that they interact with. Where they do not trust that their privacy rights will be respected, there is an increasing move to competitors. This is not lost on privacy leaders in organizations, who indicated in the 2019 Gartner Annual Security and Risk Survey that loss of customers is their second highest concern from a privacy perspective[2] (see Figure 1).

Figure 1. Organization's Risk Concerns in the Context of Privacy



Recommendations:

- Abandon the thought of approaching privacy from a pure compliance perspective. Such a mindset will result in one readiness project after another as additional jurisdictions enact data protection legislation. Instead, take a strategic approach and focus on building a privacy program based on principles that are common across multiple privacy laws.

- Scale existing solutions where possible to create a solid and consistent approach to (personal) data processing by using capabilities from cloud access security brokers (CASBs), data loss prevention (DLP), file analysis (FA) and data-centric audit and protection (DCAP) (see “Beyond GDPR: Five Technologies to Borrow From Security to Operationalize Privacy”).
- Focus on establishing an information governance framework to accompany technology controls that will drive processing of personal data in accordance with privacy requirements across the enterprise.

Related Research:

“Cool Vendors in Privacy Management”

“Use These Frequently Asked Questions When Starting a Privacy Program”

“Use These Privacy Deliverables in Every IT Development Project”

“Toolkit: Assess Your Personal Data Processing Activities”

“Toolkit: Setting Up a Privacy Program”

Strategic Planning Assumption: By 2023, 65% of the world’s population will have its personal information covered under modern privacy regulations, up from 10% today.

Analysis by: Bart Willemsen, Nader Henein, Bernard Woo

Key Findings:

- Since the GDPR became enforceable in May 2018, jurisdictions that have proposed or even passed modern data protection legislation include Brazil, China, Egypt, Japan, Nigeria, Panama, Thailand and the U.S.
- In the U.S., states such as Maryland, Massachusetts, New York and Texas are contemplating state-level data protection similar to that enacted in California. In addition, there are at least six bills under debate for a federal data protection law.

As countries introduce privacy laws to work toward parity with the GDPR, they move one step closer to achieving mutual adequacy. Japan did this by creating a virtual zone in which data can travel unhindered. Data globalization and joining this new economic zone have presented regulators in many countries with a great opportunity to differentiate their local providers in a very competitive global market.

Market Implications:

In 2019, Gartner analysts continue to receive a significant volume of privacy-related inquiries. However now the scope of questions has broadened to include matters like the California Consumer Protection Act (CCPA), India’s proposed Personal Data Protection Bill (DPB) and Brazil’s Lei Geral de Proteção de Dados Pessoais (LGDP).

Privacy is becoming a conviction-based motivator and privacy-first products are likely to follow that trend. A similar trend was observed for other conviction-based motivators like “fair trade” (e.g., coffee), “organic” (e.g., food) and “cruelty-free” (e.g., cosmetics). A decade ago, products in these categories demanded a premium and were only on offer by specialty outlets. Today, large multinationals have adopted these conviction-based motivators across their core products as well as their supply chains. The 2019 Organic Market Report reveals that the U.K. organic market is now into its eighth year of steady growth, on target to reach £2.5 billion by 2020.[3]

Organizations are also looking to technology to assist with not only the readiness efforts, but also to automate portions of the privacy management program once it is established. Technology relevance spans compliance assessment and documentation, to capabilities that govern and control the personal data life cycle. Two areas that have direct impact on the customer and represent opportunities for automation are the handling of subject rights requests and the processes for consent and preference management (CPM) (see “Practical Privacy — Executing Subject Rights Requests” and “Market Guide for Consent and Preference Management”).

Recommendations:

- For organizations that operate globally, standardize operations in accordance with the GDPR, then adjust as required for local requirements.
- Focus on enhancing privacy capabilities in your organization (see “The State of Privacy and Personal Data Protection, 2019-2020”).
- Use technology solutions to automate portions of your privacy management program. Two areas that represent opportunities for automation are SRRs and CPM.

Related Research:

“Hype Cycle for Privacy, 2019”

“Move to Contextual Privacy in Digital Society”

“IT Score for Privacy”

“Use These Frequently Asked Questions When Starting a Privacy Program”

Strategic Planning Assumption: By year-end 2022, more than 1 million organizations will have appointed a privacy officer (or data protection officer).

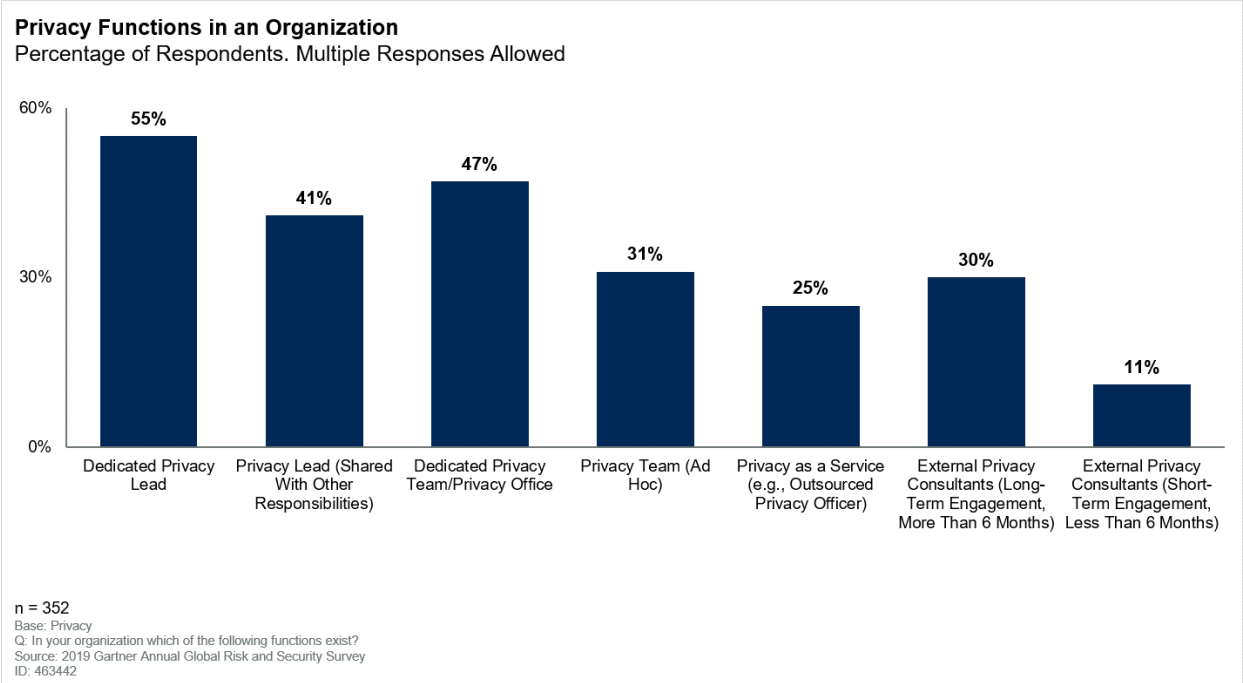
Analysis by: Bart Willemsen

Key Findings:

Before the GDPR took effect in 2018 there were a few thousand official privacy officers worldwide. Now it is estimated that already half a million organizations rely on the expertise of a privacy officer in 2019.[4] According to the 2019 Gartner Global Annual Risk and Security Survey, about 25% of

organizations also make use of outsourced privacy officers; and 30% have external, long-standing engagements (longer than 6 months) with privacy consultants (see Figure 2).

Figure 2. Privacy Functions in an Organization



The partial reliance on external aid shows that hired privacy leaders may serve multiple organizations. Most of this has been driven by the GDPR. However, many of the upcoming privacy laws contain similar requirements for dedicated workforce professionals.

Market Implications:

Organizations that have avoided hiring a privacy officer because they were not subject to the GDPR, now have to catch up nonetheless. Recruiting a privacy officer who successfully drafts and executes an organization's privacy management program requires a well-defined set of responsibilities, tailored to the specific organization, and hiring someone with a broad skill set.

The privacy officer conducts privacy risk assessments focused on specific business processes or applications. This role also identifies and suggests priorities for the organization and determines how to maintain and improve adherence to regulatory requirements and corporate policies. The privacy officer will craft privacy training and awareness programs and set up a privacy incident response plan.

A shortage of privacy leaders in the professional market creates pressure to hire the appropriate experts in a timely manner. The salaries of both chief privacy officers (CPOs) and DPOs are

expected to continue to rise. It will be important to continue to observe correct placement and specialties/capabilities of such professionals.

Finally, current developments show that drafting, implementing, operationalizing and enforcing a privacy program across the organization is more often than not a matter of multiple people working together. There is a strong relationship between the privacy professional(s) and the security lead, the HR department, procurement, legal, and audit and compliance. As such, the span of control in larger organizations is often too much for one professional. Though one million organizations may have appointed a privacy officer, this does not mean there are one million privacy professionals. On the one hand we see parts of the function being outsourced, and such service providers may serve multiple organizations at once. On the other hand, many organizations rely on a privacy office, rather than one officer, and hence require more than one professional.

Recommendations:

- This one we like to keep simple: Appoint a privacy officer, ideally one who reports directly to the board. Whether the current regulatory landscape demands it or not, having a dedicated lead for the privacy discipline is necessary to help co-steer the corporate strategy and affect the organization on strategic, tactical and operational levels.

Related Research:

“Toolkit: Privacy Policy”

“IT Score for Privacy”

“5 Areas Where AI Will Turbocharge Privacy Readiness”

Strategic Planning Assumption: Through 2022, privacy-driven spending on compliance tooling will rise to more $8 billion worldwide.

Analysis by: Bart Willemsen

Key Findings:

- The privacy-driven technology market is still emerging. Today’s post-GDPR era demands a wide array of technological capabilities, well beyond the standard Excel sheets of the past.
- Among the many tools purchased by organizations to establish and maintain their privacy programs are:
  - Governance, risk and compliance (GRC) or integrated risk management (IRM)
  - Dedicated pure-play privacy tooling for compliance documentation and remediation workflows
  - SRR management
  - UCPM

- In the evolution stage, after establishing and maintaining a privacy program, additional technologies like pseudonymization, anonymization, masking, and privacy preservation in analytics and business intelligence (ABI) come into play.
- There is a strong overlap with, and privacy-driven spend in, the security realm, including consultancy and services, data-centric audit and protection tools, data loss prevention and data breach management services.

Market Implications:

With requirements in all referenced technologies and in tech markets that are driven in part by privacy requirements, the cumulative $8 billion spend could be considered a conservative estimate (see “Beyond GDPR: Five Technologies to Borrow From Security to Operationalize Privacy”). What is certain is that privacy, as a conscious and deliberate discipline, will continue to grow and play a considerable role how and why service providers and vendors develop their products. Privacy-driven spend will thus increase in at least two ways:

1. It will influence the spend of connected stakeholders, including marketing leaders, CIOs, chief information security officers (CISOs) and chief data officers (CDOs) as part of their overall purchasing strategies.
2. There will also be an increase in dedicated privacy budgets for the evolving discipline itself.

On the one hand, organizations require more detailed control over personal data. Necessary capabilities include discovery, mapping and classification or a connection to purposeful processing (see “Use These Privacy Deliverables in Every IT Development Project”). This in turn dictates how access management is architected, data processors are instructed, and privacy notices are formed, for example. It also brings clarity to how to respond to SRRs and how to determine whether or not something (such as a request for deletion) must be honored. The data-centric protection storyline includes lineage and usage logging, secure storage and transmission, as well as logical or even physical deletion of personal data. Consumer identity and access management (CIAM) and identity as a service (IDaaS) providers can offer a way to track a customer’s personal data and control it on an attribute level.

On the other hand, organizations are encouraged to automate privacy management. This includes tooling for compliance demonstration, gap analyses and remediation workflows, automating records of processing activities (ROPAs) and data protection impact assessments (DPIAs), as well as consent, preference and privacy rights management. A manual approach is unsustainable, and organizations must budget their privacy expenses across the operation. In return, a mature privacy posture helps reduce storage costs, obtain valuable business insights and a compliant data monetization architecture, enhance customer trust and retention, and avoiding hefty sanctions for possible noncompliance.

Recommendations:

- Achieve the desirable level of control over personal data throughout the data life cycle by consolidating and integrating data-centric security tools, and prefer those solutions that are effective specifically on personal data distinction in postmodern privacy.
- Demonstrate compliance — or the roadmap toward it — by adopting privacy management tooling that delivers the necessary insight and documentation befitting the regulatory privacy requirements your organization is confronting.
- Take a risk-based approach to privacy-driven spend by determining which capabilities require automation, and design augmentation of frequently repeating activities to reduce compliance cost and manual labor burdens.

Related Research:

"5 Areas Where AI Will Turbocharge Privacy Readiness"

"Beyond GDPR: Select and Control Your Service Providers to Ensure Privacy Protection"

"Beyond GDPR: Five Technologies to Borrow From Security to Operationalize Privacy"

"Cool Vendors in Privacy Management"

"Cool Vendors in Privacy Preservation in Analytics"

A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

On Target: 2019 Prediction — By 2020, 30% of all data protection officers will be hired "as a service."

It may be a year early, but we highlight this prediction, on the one hand, in support of the prediction about privacy officers, and on the other hand to establish that it was at least in part on target. More than three years have passed since this prediction was published, and Gartner client inquiries and the annual 2019 Gartner Global Risk and Security Survey have shown that, on average, organizations deploy more than one privacy professional. The survey referenced indicates that 25% of respondents signal that they deployed a privacy officer as a service in 2019. Forty-one percent of respondents admit they also make use of outsourced help, both in the short term (less than six months) and in the midterm (more than six months). This leads us to believe that a large portion of DPOs are indeed outsourced; and in 2020 this is expected to grow further due to a shortage of available qualified professionals.

Missed: 2016 Prediction — By 2019, half of the world's larger companies processing personal data will perform privacy impact assessments; only 10% will have a defined automated PIA process.

Privacy and data protection impact assessments are among the key methods to implement a risk-based privacy program (see "Toolkit: Assess Your Personal Data Processing Activities"). Unfortunately there is only circumstantial evidence available to see how many organizations are and are not executing DPIAs. The number of organizations estimating themselves in compliance with GDPR more than a year after it took effect is dramatically low.[5] In itself, this not only pertains to conducting DPIAs, but also to the notion that a successful DPIA is a repeated activity. The nature of the considerable number of questions Gartner fields relating to such assessments implies with reasonable certainty that the prediction of 50% of large organizations conducting these assessments frequently is amiss. Though mandated in many postmodern privacy regulations, the majority of such regulations still have to take effect. The push on frequently conducting these assessments will grow internationally, but the prediction was obviously set too soon to achieve the expected coverage.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Move to Contextual Privacy in Digital Society"

"Market Guide for Consent and Preference Management"

"Toolkit: Privacy Policy"

"Hype Cycle for Privacy, 2019"

"Improve Privacy Culture by Categorizing Security Incidents"

Evidence

[1] "Penalties vary from a warning notice to fines ranging from 100 to 320,000 days of the minimum daily wage in Mexico City to imprisonment. These penalties may double in the case of sensitive personal data. Prison sentences are formally in the range of three months to five years, and double when it pertains to sensitive data (so up to *ten years* in prison)." "Law and Practice," Chambers and Partners.

[2] The 2019 Gartner Annual Security and Risk Survey was conducted from March 2019 through April 2019. The focus was to better understand how risk management planning, operations, budgeting and buying are performed, especially in the following areas: SRM, business continuity management, security compliance and audit management, and privacy.

The research was conducted online among 698 respondents in the following countries: Brazil (n = 138), Germany (n = 135), India (n = 140), the U.S. (n = 142) and the U.K. (n = 143).

Qualifying organizations have at least 100 employees and $50 million (USD equivalent) in total annual revenue for fiscal year 2018. All industry segments qualified, with the exception of agriculture, construction, IT services and software, and IT hardware manufacturing.

Furthermore, each of the four technology-focused sections of the questionnaire required the respondents to have certain job roles/categories and have at least some involvement or responsibility with at least one of the technology domains we explored. The findings in this research refer to the privacy-specific domain (n = 352).

Interviews were conducted online and in a native language. The sample universe was drawn from external panels of IT and business professionals. The survey was developed collaboratively by a team of Gartner analysts who follow these IT markets and was reviewed, tested and administered by Gartner's Research Data and Analytics team.

Disclaimer: Results of this study do not represent "global" findings, or the market as a whole, but are a simple average of results for the targeted countries, industries and company-size segments covered in this survey.

[3] "Organic Market 2019," Soil Association.

[4] "Approaching One Year GDPR Anniversary, IAPP Reports Estimated 500,000 Organizations Registered DPOs in Europe," International Association of Privacy Professionals (IAPP).

[5] "Championing Data Protection and Privacy, a Source of Competitive Advantage in the Digital Century," Capgemini Research Institute.

Note 1 Postmodern Privacy and Data Protection Laws

Jurisdictions around the world that have postmodern privacy and data protection laws include:

- Argentina ("República Argentina — Poder Ejecutivo Nacional 2018 — Año del Centenario de la Reforma Universitaria")
- Australia ("Australia: Privacy Act Amendments to Pack a Punch," Mondaq [Free, registration required.])
- Brazil ("Brazil's New Data Protection Law: The LGPD," Cooley's cyber/data/privacy practice.)
- Egypt ("Egypt Passes First Data Protection Law," PrivSec.Report.)
- India ("Data Protection Bill to Be in Place by December: Law Minister Ravi Shankar Prasad," The Economic Times.)
- Indonesia ("Draft Personal Data Protection Act," Indonesia Ministry of Communication and Information [Depkominfo].)
- Japan ("The Framework for Mutual and Smooth Transfer of Personal Data Between Japan and the European Union Has Come Into Force," Personal Information Protection Commission Japan.)
- Kenya ("An Update on the Data Protection Bill 2019: A Step Forward for Kenya," Bowmans.)
- Mexico ("Mexico: New Law for the Protection of Personal Data," Mondaq. [Free, registration required.])

- Nigeria ("Nigeria: Nigeria's 2019 Data Protection Regulation: A Fair Scale for Privacy and Commercial Rights?" Mondaq. [Free, registration required.])
- Panama ("Panama: Panama Approves Law on Protection of Personal Data," Mondaq. [Free, registration required.])
- The U.S. (see "Hype Cycle for Privacy, 2019")
- Singapore ("Legislation and Guidelines," Personal Data Protection Commission Singapore.)
- Thailand

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp