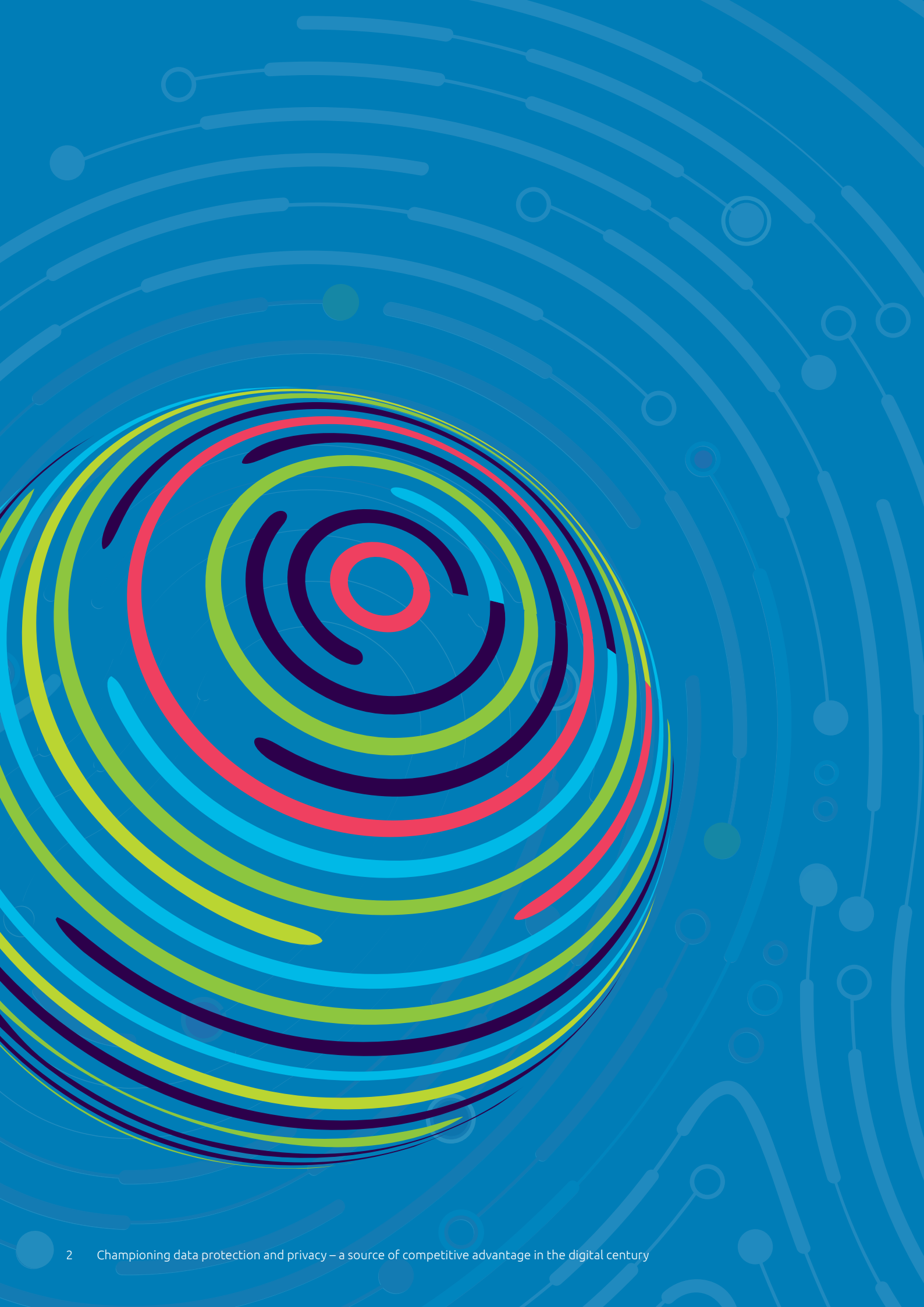


Championing Data Protection and Privacy

*a source of competitive advantage
in the digital century*



Executive Summary – key takeaways

Compliance levels do not meet expectations

- Only 28% of firms say they are compliant with the GDPR today, with 30% “close to compliant.”
- Looking forward, just over two-thirds of organizations expect to be compliant with the upcoming CCPA (California Consumer Privacy Act).

Achieving and maintaining compliance poses significant challenges

- Two-thirds of organizations have hired full-time employees to support GDPR compliance efforts.
- Over a third point to legacy IT systems as a major challenge to both GDPR and CCPA compliance.
- Almost all organizations (90%) have received from data subjects queries related to the GDPR and 13% received more than 5,000 queries in the past year.

Being proactive brings big benefits and competitive advantage

- Organizations that are fully compliant with the GDPR outpace partially compliant organizations across a range of areas, including first-order priorities (revenue performance) and secondary benefits (such as consumer satisfaction and employee morale).
- Firms realized higher-than-expected secondary benefits – 79% of compliant organizations reported an improvement in employee morale and 91% of compliant organizations reported an improvement in cybersecurity practices.

There are a number of priorities for increasing data protection and privacy compliance

- Embed data protection and privacy principles in the organizational culture
 - make employees aware of the importance of the issue and educate them the legal requirements and practices for data protection and privacy.
 - Enhance accountability
 - define and implement data protection policies and guidelines and create mechanisms to ensure effective monitoring of implementation privacy principles in the definition phase of the projects.
 - Use AI for data discovery and to improve data management
 - Leverage advanced technologies to automate data management and compliance-related activities for improved performance.
 - Assess how new data anonymization techniques and technologies can expand your data-sharing opportunities.
 - Industrialize risk assessment and breach mitigation
 - Use security operations centers (SOC) and leverage platform and cloud to enhance your operation.
 - Establish and integrate governance, risk, and compliance (IGRC) to build robust protection and privacy capability
 - Organizations must manage data protection and privacy end-to-end, from budgets to audit of external vendors.
- Capitalize on the ethical use of technology and strengthen stakeholder trust

Introduction

Last year, our comprehensive study – *Seizing the GDPR Advantage: From mandate to high-value opportunity* – established that compliance with data protection and privacy regulations can be a source of competitive advantage for organizations.

It has now been over a year since Europe's General Data Privacy Regulation (GDPR) came into effect and we wanted to understand how companies are coming to terms with the regulation and its implications. For this latest study, we conducted a follow-up survey to assess the current state of play and to compare and contrast the characteristics of firms that are compliant with the regulation against those that are not. To achieve these goals, we:

- Surveyed 1,100 compliance, privacy, data protection, and IT executives across ten countries and eight sectors
- Conducted in-depth interviews with executives who are experts on data protection and privacy regulations and practices
- Analyzed existing and proposed data protection and privacy regulations worldwide to explore not only how organizations are dealing with regulations that already

exist, but also how they are preparing for those that are pending.

In this report, we examine:

- **The current state of compliance with existing regulations and the level of preparedness for upcoming regulations**
- **The challenges to achieving and maintaining compliance**
- **The higher-than-expected benefits of embracing data protection and privacy regulations as an opportunity rather than merely a compliance exercise**
- **What organizations can do to flourish in the face of increasing regulation, regardless of compliance maturity**



State of play with current regulations and preparations for the next wave

Although a year has passed since the GDPR went live, the position of many organizations remains uncertain. Ahead of the launch date, they were investing to achieve compliance and were optimistic they would succeed. But 12 months on, many are not only struggling to comply with existing regulations, but also straining to prepare for *upcoming* regulations. For some, especially those that are lagging behind in compliance, the consequences have been severe.

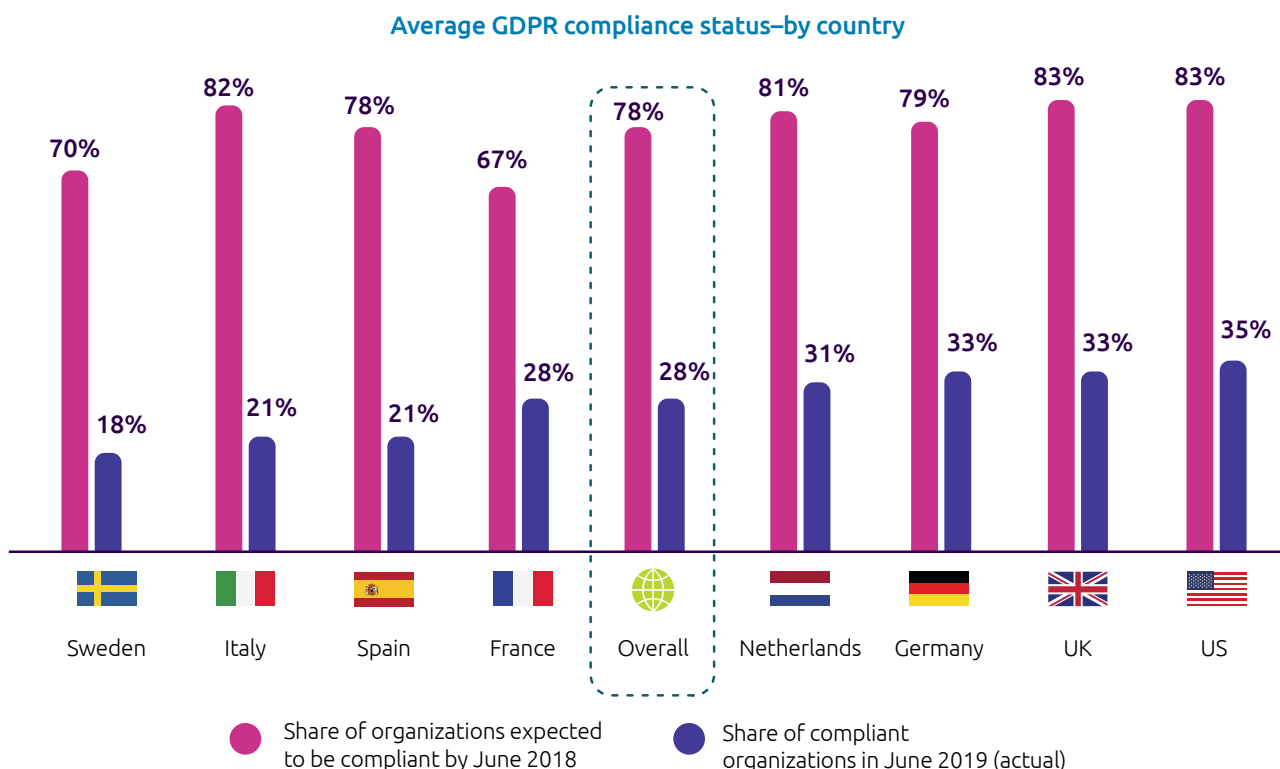
If organizations had any doubt about the repercussions of not complying with the GDPR, the history of fines over the first year of its enforcement indicates that it is not to be taken lightly. As a result, budgets for investment in data protection and privacy compliance remain high for the foreseeable future.

GDPR compliance does not meet expectations

Last year, when we surveyed executives about the GDPR, we found that over three-quarters of them (78%) expected to be compliant by the time it came into effect in May 2018. But one year on, only 28% of them make the same claim. Another 30% report that they are “close to” complete compliance,¹ but still actively resolving remaining issues. One executive told us they were getting close, saying, *“We still need a few steps to mature on the necessary documentation, so I would say we are maybe 75% to 80% compliant on the average.”*

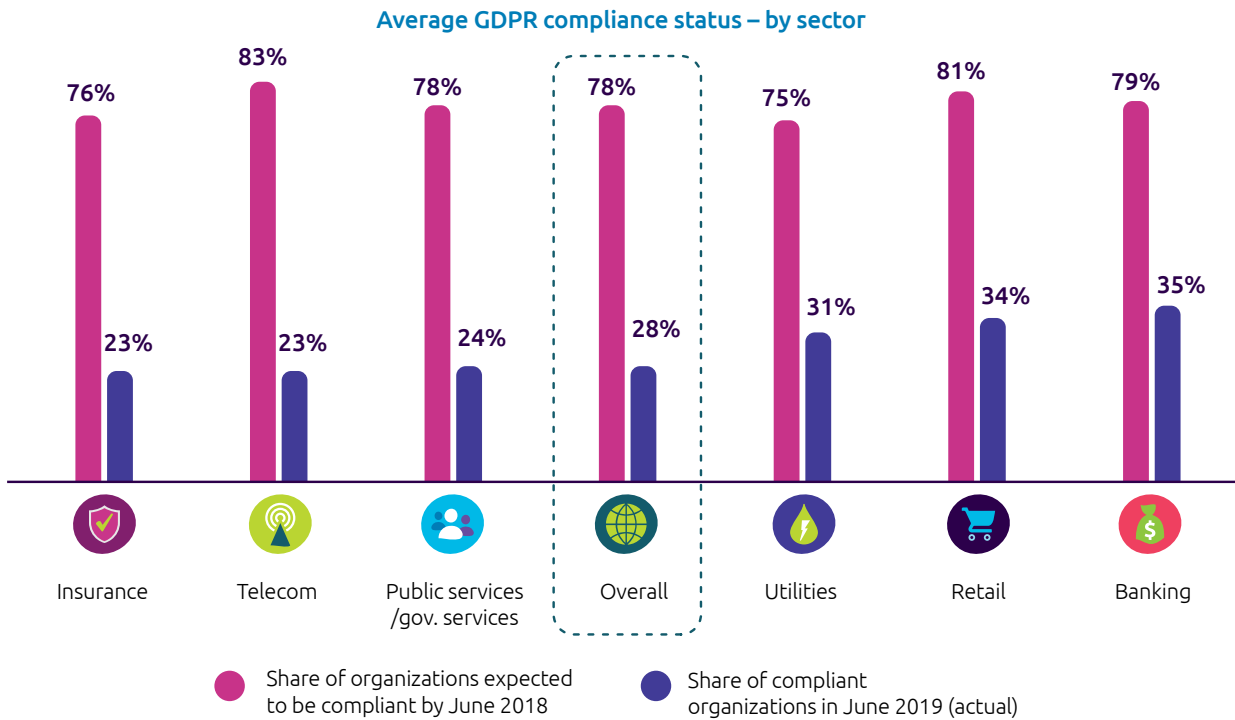
Our research shows that that non-compliance is a worldwide, cross-sector issue. None of the countries or sectors we surveyed have even come close to matching the aspirations they had in 2018.

Figure 1. More than seven in ten firms lag in GDPR compliance



Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n=1,039. GDPR Executive Survey, March–April 2018, n=1,000.

Figure 2. Banking and retail sector lead in GDPR compliance



Source: Capgemini Research Institute, Data Privacy Executive Survey, June 2019, n=1,039. GDPR Executive Survey, March–April 2018, n=1,000.

Data protection and privacy regulations are emerging globally

Although the GDPR is only intended to protect data subjects within the territorial scope of the regulation – mainly the European Union (EU) member states and the European Economic Area (EEA) countries – the effects of the regulation ripple globally. The GDPR applies to any organization anywhere in the world that controls or processes the data of EU/EEA data subjects (i.e., any data subjects within European Union member states or European Economic Area countries).

The GDPR, as well as being one of the highest-profile regulations to be enforced, is one of the first major frameworks to go live. However, a number of other initiatives are in the pipeline. Notable examples include the California Consumer Protection Act (CCPA) in the United States, the General Data Protection Law (LGPD) in Brazil, and the Data Protection Bill in India (see “The evolution of data protection laws around the world”).



The evolution of data protection laws around the world

Canada

28 federal, provincial and territorial privacy statutes.
 Personal Information Protection and Electronic Documents Act,
 Personal Information Protection Act

US

[California, Hawaii, Maryland, Massachusetts, Mississippi, New Mexico, New Jersey, New York, North Dakota, Rhode Island] has draft privacy legislation for consumers online rights.*

[Washington] has introduced a 'GDPR-style' proposal*

Mexico

Protection of Personal Data held by Private Parties Law

Colombia

Constitution: the right to privacy and the right to data rectification, Personal data processing, as well as databases Law, Processing of financial data, credit records and commercial information Law

Peru

Personal Data Protection Law (PDPL)

Chile

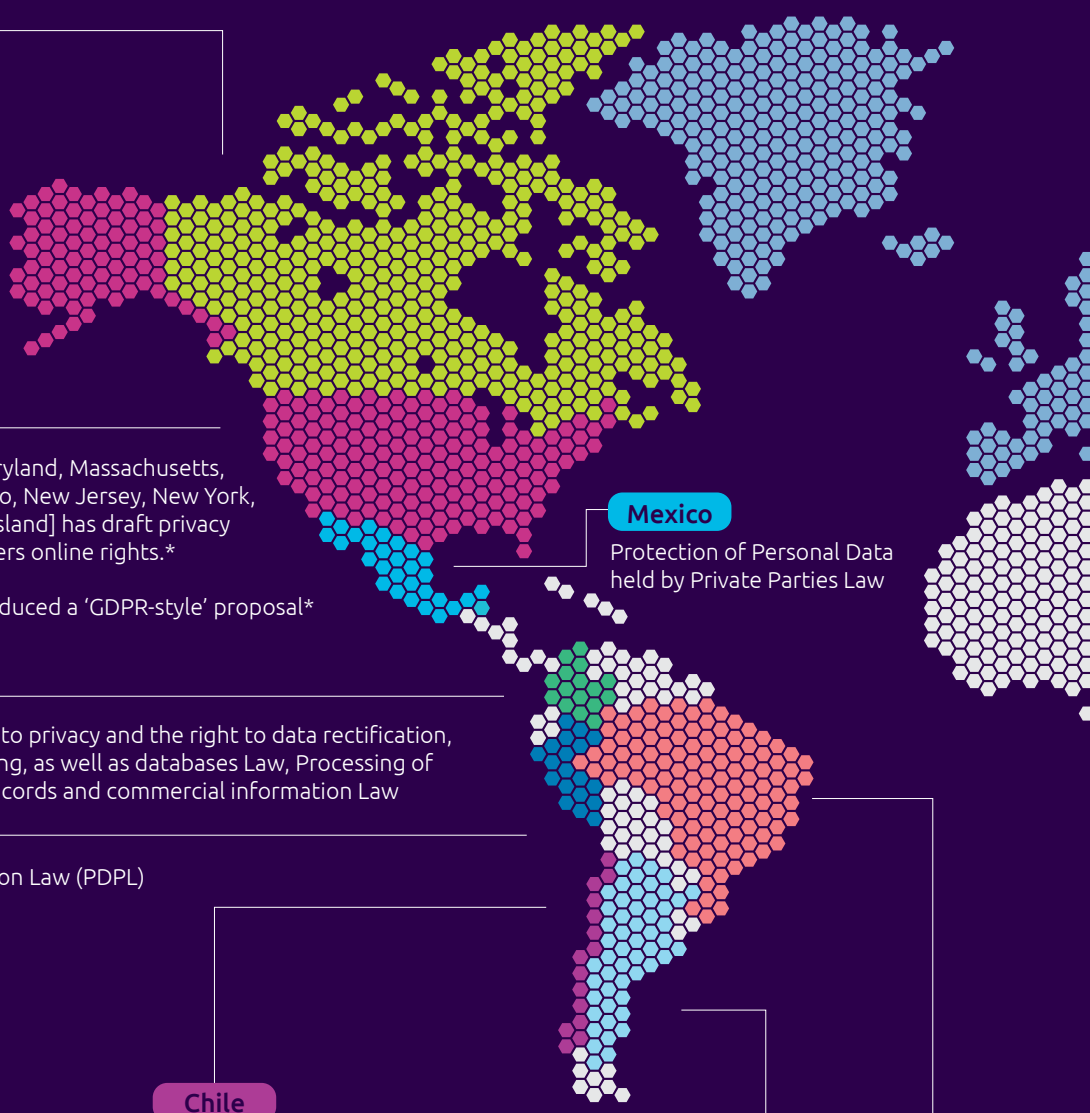
10 Laws, Personal Data Protection Law (PDPL), Banking Secrecy Law, Limitations on the handling of personal data Act, Public information access Act, Computer Crimes Act, Duties related to healthcare Act

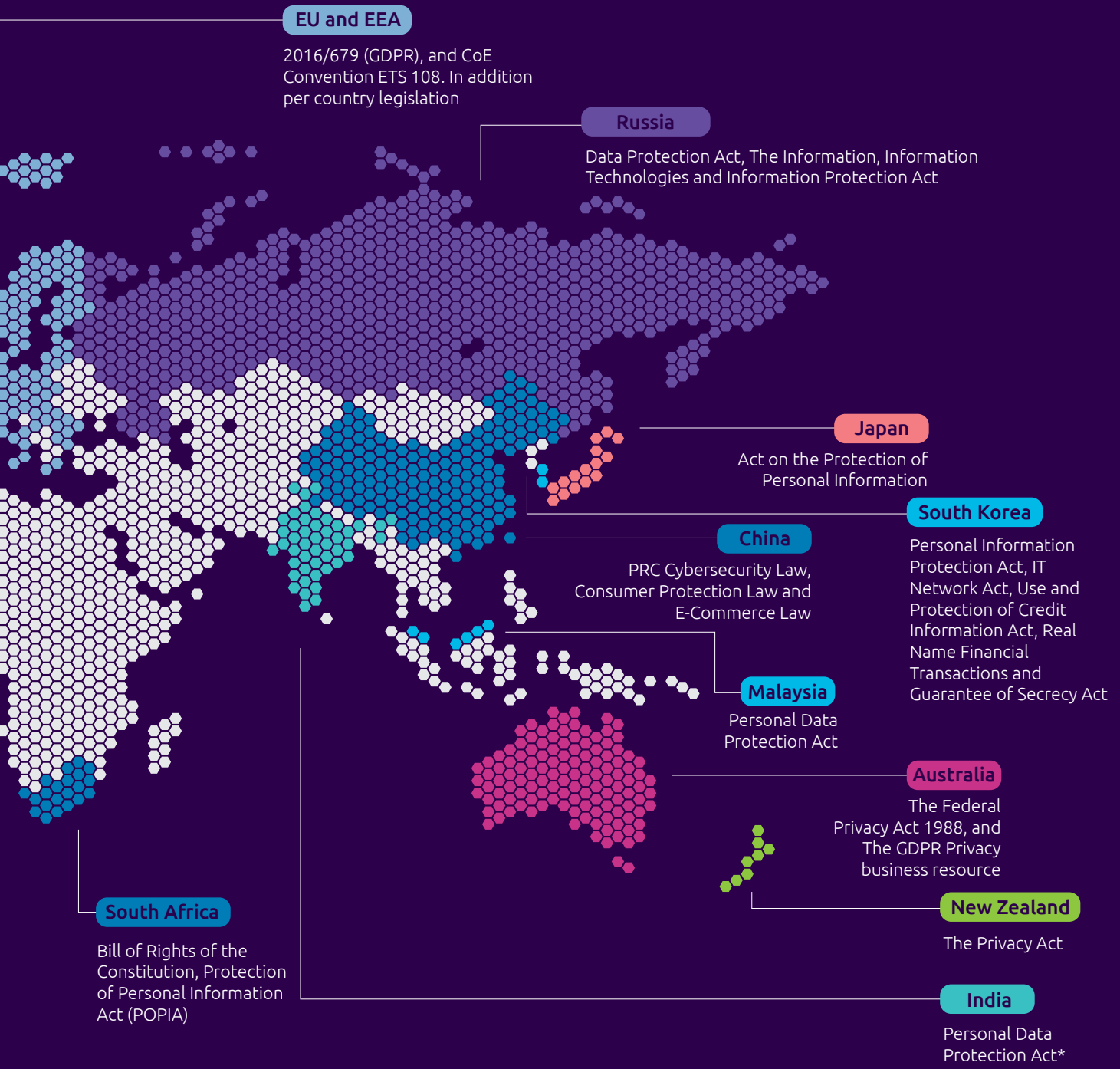
Argentina

Personal Data Protection Law (PDPL)

Brazil






Brazilian General Data Protection Law (LGPD)*





* Law/Regulation amended, but not enforced WIP

CCPA vs. GDPR, a comparison

	GDPR	CCPA
 Applicability	Applicable to private as well as public entities	Only applicable to <i>for-profit</i> entities
 Criteria for applicability	Applicable to all organizations irrespective of size	Applicable if one or more of the following criteria is met: <ul style="list-style-type: none"> – Revenue of more than \$25 million per annum – Dealing in personal data of 50,000 Californian consumers, households or devices – Deriving 50% or more of annual revenue from selling consumers’ personal data
 Territorial scope	Entities established in the EU/EEA and entities not established in the EU/EEA but offering goods and services in the EU/EEA and/or monitoring behavior of individuals located in the EU/EEA	Entities doing business in the state of California
 Penalties and fines	Penalties of 2–4% of annual revenue or €10–20 million (whichever is higher) for non-compliance	Penalties of \$2,500 per violation and \$7,500 per intentional violation. In addition, California provides for a private right of action and consumers can sue for greater of actual damages or up to \$750 per incident
 Time window to serve data subjects requests	Without undue delay and in any event within 30 days, extendable to 60 more days based on complexity of request	45 days, extendable to 90 days based on complexity and number of request

Sources: GDPR, Territorial Scope
 GDPR, What are the GDPR fines”
 GDPR, Article 12
 CCPA Senate bill 1121, Chapter 35
 California Consumer Privacy Act of 2018



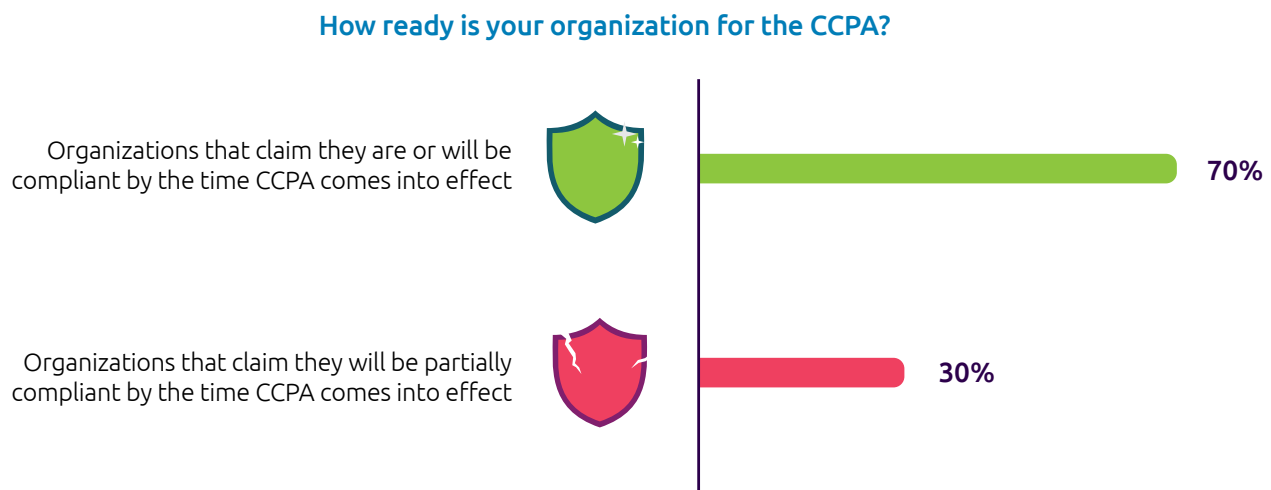
Significant cohort will not be ready for CCPA

The next major data privacy regulation will emerge in the US, with the California Consumer Protection Act (CCPA) going live on January 1, 2020. Our research shows that 30% of organizations that fall into the CCPA's remit say they will only be partially compliant by go-live. This raises two points:

- Given the size of the California economy, and the number of companies affected, this in itself is a sizeable number of firms.

- A similar situation existed with GDPR compliance in 2018, when 78% said they would be compliant by GDPR go-live. However, as we have seen from our latest 2019 data, the reality is that many missed out on compliance by go-live (when reality hit, only 28% reached compliance). This raises the possibility that many organizations are over-optimistic about being CCPA compliant.

Figure 3. A significant majority of organizations expect to be compliant with the CCPA by the time it comes into effect



Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n = 1,038.



30%

share of organizations that claim they will be partially compliant by the time CCPA comes into effect

Non-compliant organizations are already feeling pressure in the form of fines

The organizations that will not be ready – or that are over-optimistic in their assessment – could find themselves paying a high price. Failure to comply with data protection and privacy regulations can be expensive. Data Protection Authorities have now started to enforce the GDPR by imposing fines which can be up to millions. CNIL, the French data protection authority, has already doled out fines of more than €50 million a year since the GDPR came into effect. The Information Commissioner’s Office in the UK has also levied fines of more than €100 million for non-compliance with GDPR. Firms that are lagging behind in compliance (67%) or do not plan to achieve compliance (4%) face an increasing risk to enterprise value, in terms of both direct fine costs and reputational damage.

Depending on the circumstances of the violation, the fines can be punishing. For the GDPR, fines can reach as high as 4%² of worldwide annual revenue (for example, an organization with €5 billion annual revenue, could potentially be fined up to €200 million). According to the executives we surveyed, Germany and the UK top the list of countries that have pursued the most cases, with more than 20% of firms saying they have been fined by these countries.

The CCPA calculates fines differently and generally does not seek to emulate the severity of the GDPR’s most prohibitive fines. Offending firms may be liable for \$2,500 per violation per consumer affected (or \$7,500 per violation per customer

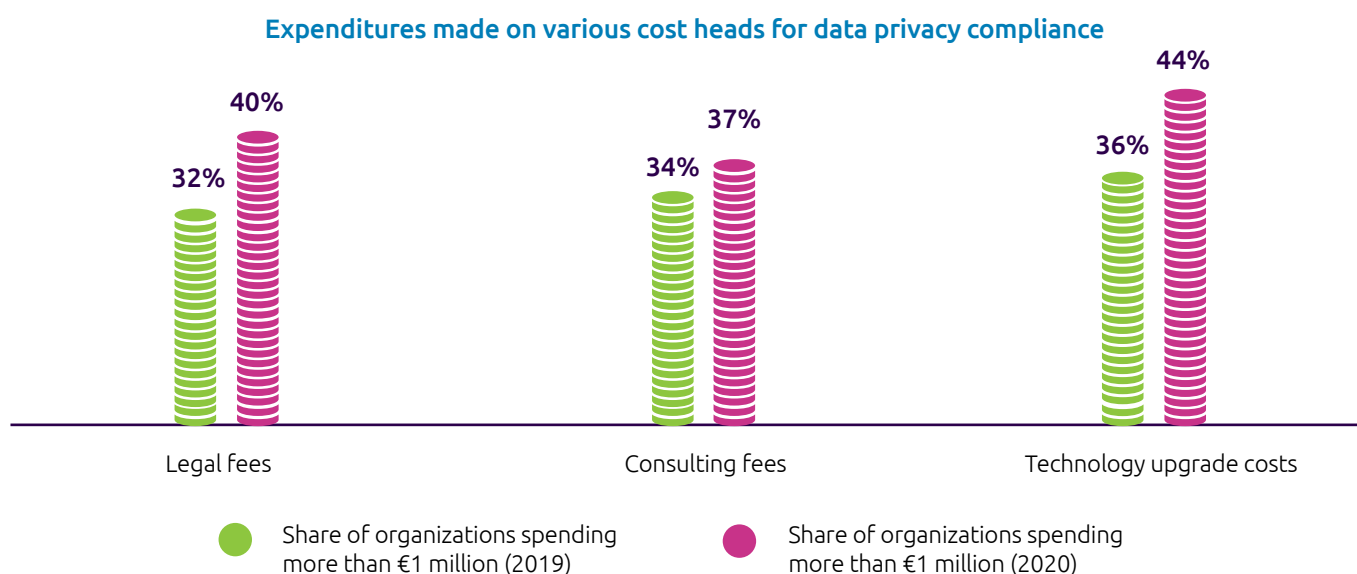
affected if the violation is determined to be intentional).³ For instance, if an organization providing services to 100,000 Californian consumers is deemed to be in breach of CCPA, it can be liable for up to \$250 million if the breach is unintentional. However, the penalty can reach \$750 million if the breach is considered intentional. The CCPA also allows consumers a private right of action to sue directly for a breach.

A significant number of organizations are investing heavily in data protection and privacy and more will join their ranks next year

To ensure compliance with existing data protection regulations – and lay the foundation for those to come – organizations are making significant investments in advice and technology upgrades. As well as adding to headcount, we find that:

- Over a third (34%) of organizations are spending more than €1 million on consulting fees in 2019 and even more (37%) expect to do so in 2020 (see Figure 4)
- Around a third (32%) are investing more than €1 million on legal fees in 2019 and this is expected to increase to 40% in 2020.
- Over a third (36%) are investing more than €1 million in technology upgrades in 2019 and this increases to 44% in 2020.

Figure 4. Expenditure for IT and consulting is poised to increase next year



Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n=1,100.

The challenges to achieving and maintaining privacy regulation compliance

Compliance with data protection and privacy regulations is perhaps not quite as easy as some organizations anticipated. *“Regulation always comes with a number of responsibilities and obligations. And, from a practical point of view, it’s very often a challenge to operationalize new regulations like this,”* says Andreas Klug, chief privacy officer at GVC Ladbrokes Coral, a UK-based gaming industry leader.

There are myriad challenges that need to be addressed to achieve compliance. These include, but are not limited to:

- Upgrading IT systems
- Updating policies and procedures
- Acquiring and training talent.

Even for firms that faced these challenges head on, the road to compliance has not been pain-free. Another executive we spoke with told us: *“Even implementing some of the smallest of requirements under the law can require considerable investment.”*

Legacy IT systems challenges compliance

When it comes to the barriers that stand in the way of robust GDPR compliance, dealing with legacy IT systems emerges as the biggest challenge (see Figure 5). **Over one in three executives** (38%) say that aligning existing IT to the GDPR is extremely complex. *“Compliance has to be built into the tools and into the technology itself,”* says GVC Ladbrokes Coral’s Andreas Klug.

When executives were asked to rate the top challenges organizations face while preparing for the CCPA, legacy IT (42%) emerged as critical. Organizations were also concerned that they are confused by the lack of clarity from data protection authorities on how they will be assessed (also an issue for 42% of respondents). Forty percent of organizations also point to a culture challenge of convincing employees of the importance of the guidelines and bringing about a mindset change.



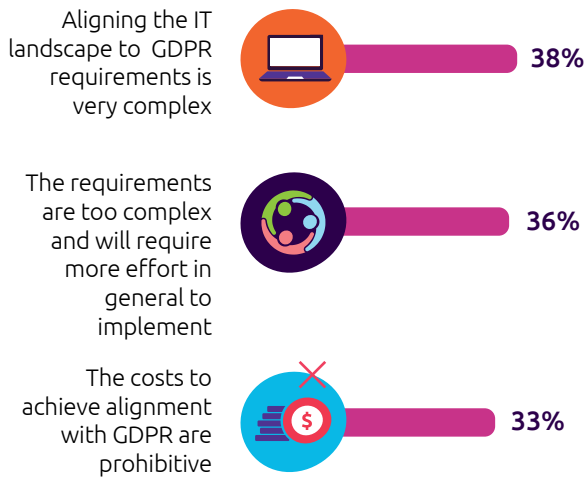
The number of queries since the GDPR went into effect are more than double what we are used to,

Paul Brocklehurst, chief information Officer of the Financial Services Compensation Scheme.

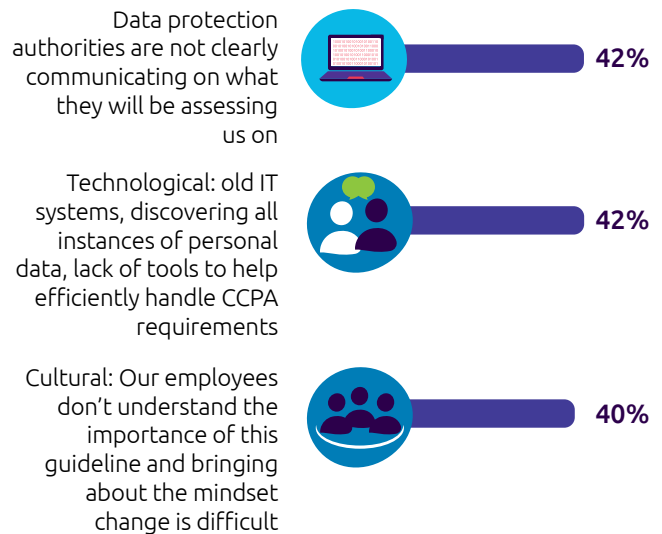


Figure 5. Legacy IT a major headache for the GDPR and CCPA

Please indicate which barriers your organization is facing in seeking closer alignment to GDPR (Top 3)



What are your biggest challenges with preparing for CCPA in your organization? (Top 3)



Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n=744.
 Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n=1,038.
 Data represents share of executives that have placed the given challenges in top three rank.

The effort to maintain compliance is ongoing and spans the globe

Despite what some executives may have anticipated (or hoped), the passing of the GDPR-effective date did not mark the end of organizations' GDPR compliance efforts. Nor will January 1, 2020 signify the end of work on CCPA compliance. The effort to maintain data protection and privacy compliance is a continuing one, confirms Michaela Angonius, VP head of Group Regulatory and Privacy, Telia Company, *"The GDPR is not something you will ever be done with. It is something that you need to work on continuously,"* she says.

For firms that are covered by the GDPR, queries from data subjects make up a significant amount of the work that goes into maintaining compliance. Almost all of the executives we surveyed (90%) have received queries, with over one in ten (13%) receiving more than 5,000 in the first year of the GDPR. *"The number of queries since the GDPR went into effect are more than double what we are used to,"* says Paul Brocklehurst, chief information Officer of the Financial Services Compensation Scheme.

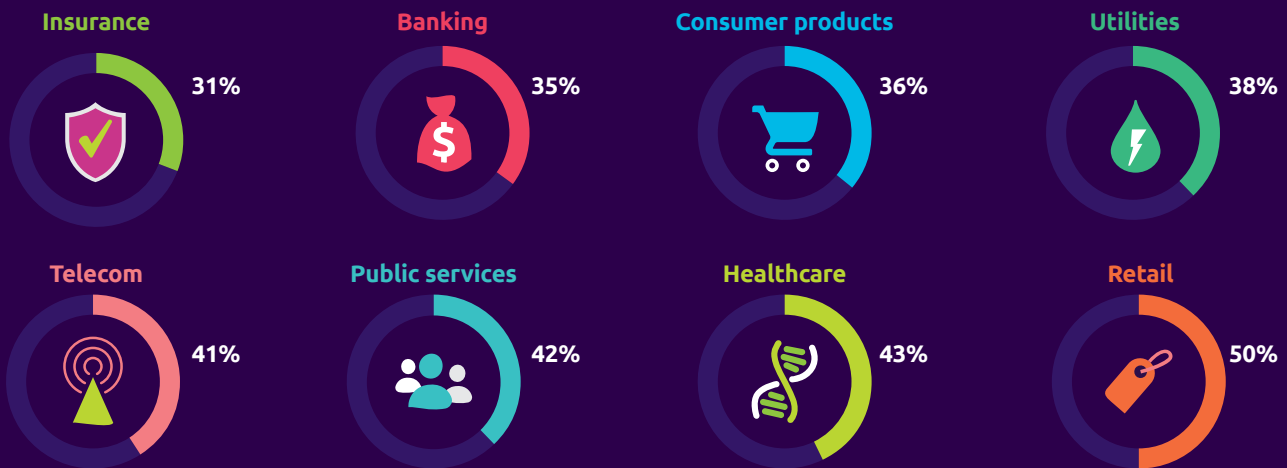
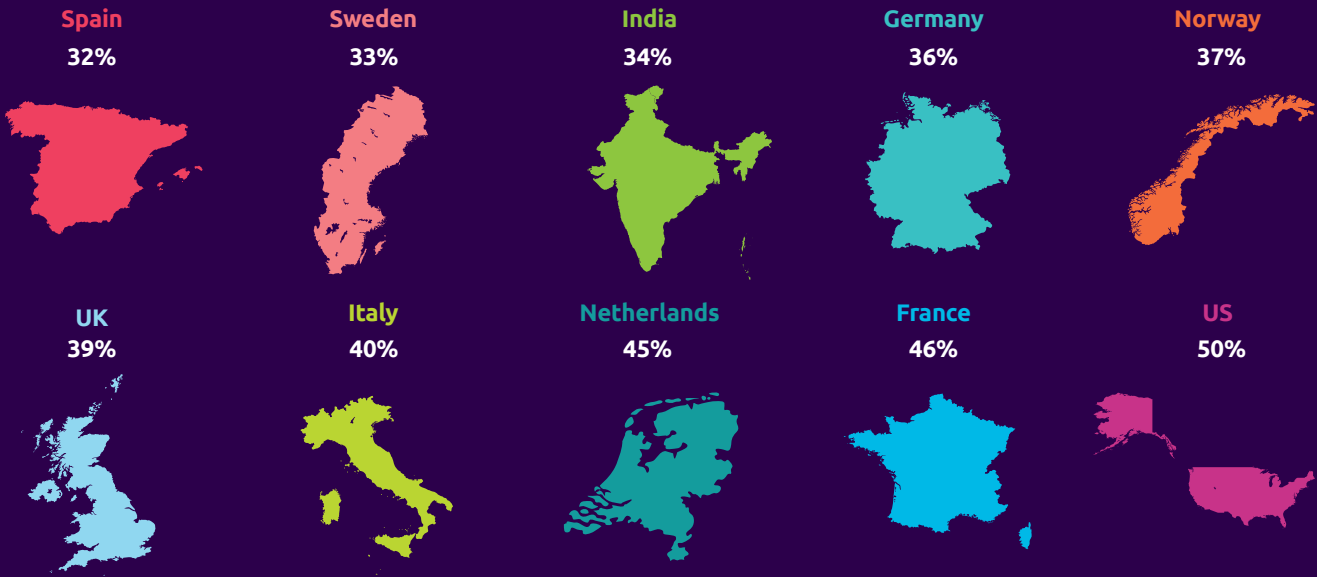
These findings are in sync with our previous survey. Last year, over half of data subjects (57%) said they would take action if

they discovered that organizations were not doing enough to protect their personal data. Of these, 72% said they would ask organizations to provide more details on the data they hold on them. Three-quarters intended to go so far as to request that their personal data be deleted (75%) and revoke consent for data processing (73%).

The global reach of the GDPR is demonstrated by the experience of US companies. Last year, executives from US-based organizations expected as many as half of their consumers to exercise their rights and initiate queries regarding their personal data. As Figure 6 shows, half of organizations covered by the GDPR in the United States have received more than 1,000 queries since May 2018. And, on a sector basis, half the firms in the retail sector reported the same thing. In terms of what customers were raising queries about, the number-one topic according to our research was data protection and the organization's ability to keep customer data safe.

Figure 6. Half of US-based firms have received more than 1,000 queries as a result of the GDPR

Share of organizations that have received more than 1,000 queries since May 25, 2018 (by country)



Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n=1,039.

In addition to data subjects raising queries with companies themselves, those who are covered by the GDPR and its protections are also approaching organizations as well as respective supervisory authorities with their complaints. According to a recent report from the BBC, “Across all the EU countries which have implemented GDPR, there has been a total of 89,271 notifications of data breaches, and 144,376 complaints from the public.”⁴ Also, the majority of the organizations we surveyed (70%) said that they have received complaints and more than half (53%) responded by modifying processes/procedures to address the issues identified. The

number-one complaint was on the data subjects’ right to be informed about the collection and use of their personal data. Organizations covered by the CCPA will undoubtedly face similar challenges, as consumers can sue companies for violating privacy guidelines.⁵

In response to this increased work, firms have hired additional full-time and part-time staff. Almost two-thirds (62%) said that they hired full-time employees to support data protection and privacy compliance while more than one-third (38%) hired part-time workers. In addition, 39% of firms outsourced data protection and privacy support.

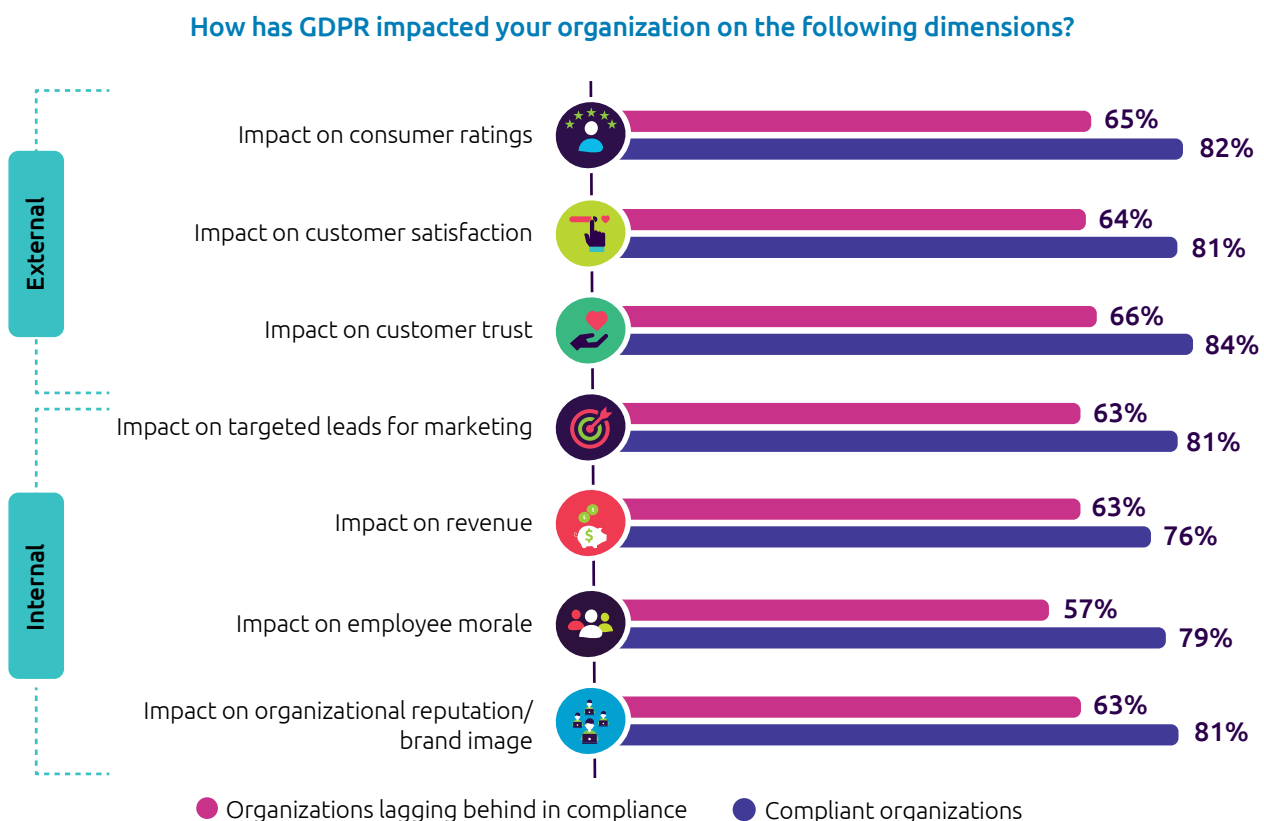
Embracing data protection and privacy as an opportunity rather than a burdensome compliance exercise brings greater benefits

Complying with the GDPR has resulted in significant benefits for organizations. **92% of executives from compliant firms say their organization has gained a competitive advantage thanks to the GDPR.** Sentiment has shifted significantly since last year's report, where only 28% of executives believed this to be the case.

To understand how benefits are falling out, we analyzed the GDPR-compliant organizations in our sample (who made up 28% of the companies) against the organizations that were lagging behind in compliance. Overall, the compliant

organizations have gained the lion's share of benefits (direct benefits as well as second-order benefits) compared to the others. For every measure – from consumer perceptions to revenue impact – **compliant organizations have outperformed non-compliant by an average of 20%** (see Figure 7).

Figure 7. Compliant organizations see higher positive impact



Executives were asked to rate these dimensions on a scale of 1–7, where 1=decreased significantly and 7=increased significantly
 Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n=1,039.

Organizations that are proactive are realizing the most benefits

Looking at the organizations that identified as compliant with the GDPR:

- **81% said that the GDPR has had a positive impact on the organization's reputation/brand image**
- **84% said trust had increased**
- **76% had seen a revenue increase**, with strong performance driving benefits such as greater customer loyalty and increases in online purchasing.

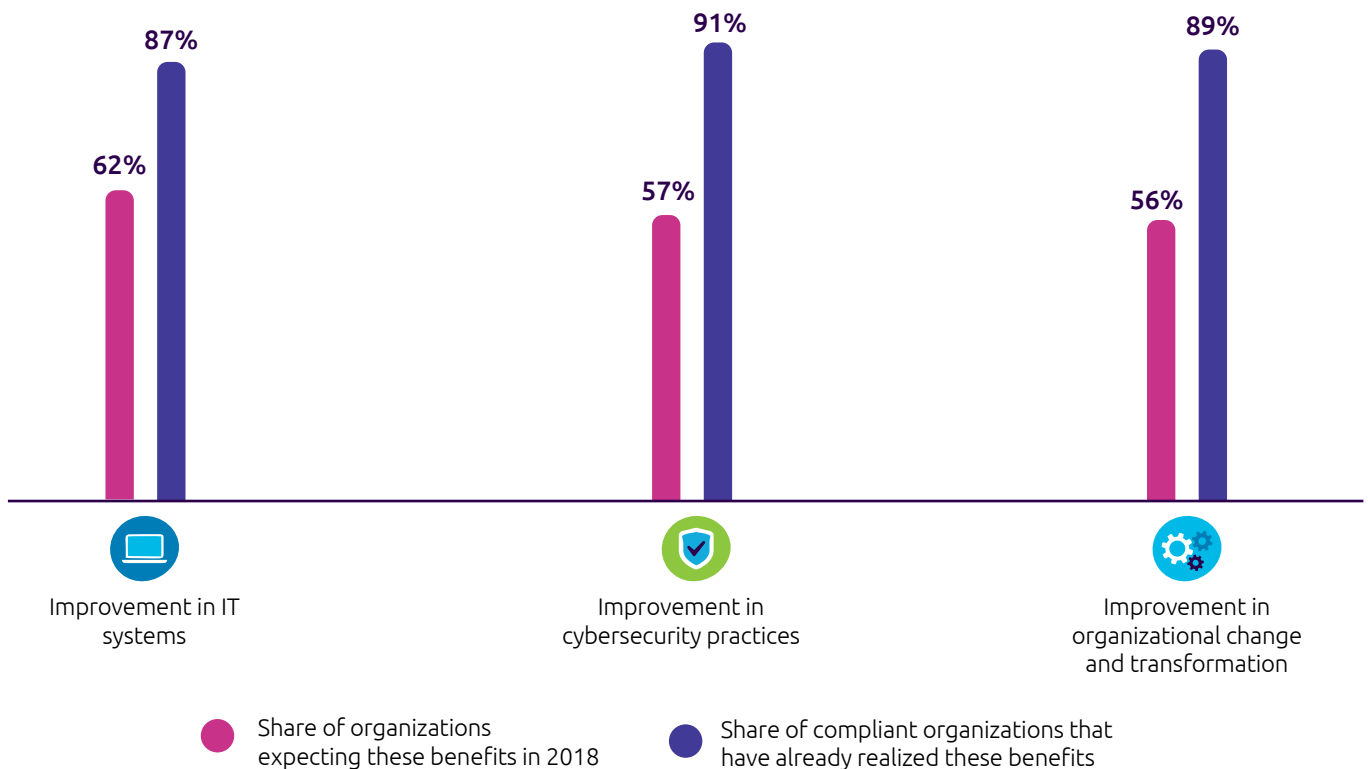
According to 81% of compliant organizations, the improved consumer trust and satisfaction had a positive impact on targeted leads for marketing. *"Customers do recognize and appreciate the level of effort and impact the GDPR compliance brings with it,"* says Henri Kujala, data protection officer for Netherlands-based HERE Technologies. *"Compliance has brought increased levels of trust."*

The hidden benefits of GDPR compliance are higher than expected

Beyond the direct benefits of increased revenue and enhanced reputation, the GDPR has also led to greater-than-expected improvement in internal processes. *"The GDPR has increased cybersecurity. It has improved awareness about data and how we use it, and what data we are using,"* says Rachel Glasser, chief privacy officer at the global digital agency, Wunderman Thompson. This is confirmed by our research, where 91% of executives from compliant organizations reported improvements in the processes for handling and managing personal data. Furthermore, these second-order benefits (such as improvements in cybersecurity practices) exceeded 2018 expectations. As Figure 8 shows, a range of areas benefited, including IT transformation, cybersecurity practices, and organizational change. In fact, second-order benefits extended as far as increasing employee satisfaction, with 79% of compliant organizations reporting an uptick in employee morale.

Figure 8. More than three-quarters of the compliant cohorts achieved second-order benefits

Do you believe that implementing GDPR has resulted in any positive second-order effects for your organization?



Source: Capterra Research Institute, Data Privacy executive survey, June 2019, n=1,039,

Benefits for individuals – the real reason the GDPR exists

According to a recent survey by the European Commission, almost two-thirds of people who provide personal data online (65%) now feel that they have at least some control over this data.⁶ Our latest research echoes this sentiment, with 84% of compliant firms saying individuals' trust increased significantly (this drops to 66% of non-compliant firms). **Four out of every five compliant organizations said they had driven better organizational reputation and consumer satisfaction,**

which in turn is translating into high consumer participation in loyalty programs. In the retail sector, as Figure 9 shows, we found that:

- Consumer participation in loyalty programs is up in 74% of compliant retail firms, compared to 54% for the non-compliant firms.
- 80% of compliant firms agree that the number of data subjects targeted in campaigns has increased thanks to the GDPR, compared to 57% of non-compliant firms.
- Online purchases have increased since the GDPR went into effect for 83% of compliant firms, compared to 63% of non-compliant firms.

Figure 9. More compliant retailers drive higher performance and benefits

Impact of the GDPR on various retail metrics



Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n=259 retailers.



Compliance has brought increased levels of trust

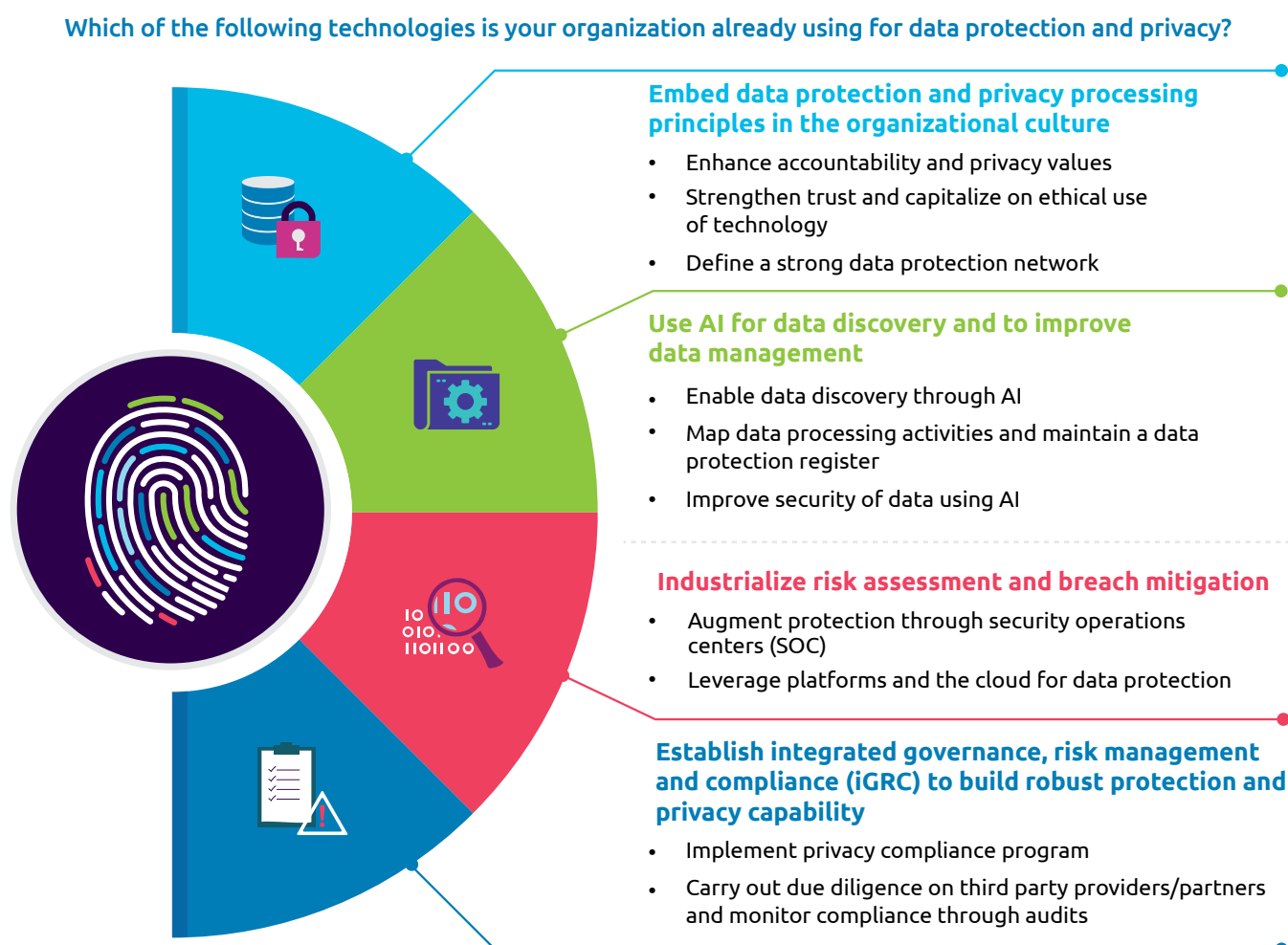
Henri Kujala, Data Protection Officer, Here technologies

What organizations should do to cope with increasing data protection and privacy regulation

Regulatory scrutiny will continue to increase and change in the years ahead. Organizations that are strategic about identifying and addressing the fundamental aspects of data protection and privacy will be best positioned for the future. To build that capability, organizations need to have the right philosophy about data protection and privacy. In other words, it is best to approach data protection and privacy proactively, rather than solely as a compliance activity. At Telia, Michaela Angonius

outlines how the company took a proactive approach. *“We started raising awareness internally, long before the law was adapted,”* she explains. *“This was because we foresaw that this would be one of the biggest compliance projects that we would undertake in the company’s history.”* Whatever an organization’s beliefs may be – or whatever its stage of compliance maturity – a number of enablers will be key not only to achieving data protection and privacy compliance, but also to maintaining and improving on it (see Figure 10).

Figure 10. Recommendations to cope with increasing data protection and privacy regulations



Source: Capgemini Research Institute analysis.

Embed data protection and privacy processing principles in the organizational culture

Enhance accountability and privacy values: As with any compliance matter, protection of personal data requires accountability. This, in turn, requires documentation that defines the principles a company uses when processing personal data. The main challenge is drafting documentation that addresses the different legal requirements while also ensuring those requirements are properly applied across the entire lifecycle of data processing. In this regard, the implementation of processes is particularly important. Taking into account business needs while drafting and implementing such policies and procedures is also key for a successful implementation of a data protection program.

However, having documented policies will achieve little if employees are not sufficiently aware of data protection and have not had the necessary training. Multiple data breach incidents occur due to sheer mishandling of data. Errors were causal events in 21% of breaches.⁷ Employees often lack context and do not understand the importance data protection and privacy regulation. Executives in our survey identified this as a top challenge, therefore a comprehensive data protection curriculum, adapted to different functions, is essential. Ensuring that data privacy is embedded in the organizational culture can build trust in the organization; 53% of compliant firms have established a public set of values that include protection of individuals' data, compared to 36% of non-compliant firms. It is therefore essential to invest on training and awareness campaign.

Strengthen trust and capitalize on ethical use of technology: How trusted an organization is by its stakeholders – from employees to customers to investors – is key to its long-term value and success. Organizations should not try to fit in the law required by principles, legal obligations, and data subjects' rights in to systems, services, and operations. Organizations that want to be trusted by stakeholders need to ensure trust by design and default in order to deliver reliability and not just by adherence to privacy laws.

With technologies such as artificial intelligence key to analyzing large amounts of data in encrypted format for privacy compliance, it is important that these technologies – and their outputs – are also trusted by stakeholders such as customers. This means addressing the ethical dimension of AI and ensuring that trust is built into smart systems. This can be done by checking for biases in the data sets that are fed into AI, putting in place the right quality controls, designing systems with human-in-the-loop review processes, and monitoring bias in development and production.

Define a strong data protection network: In order to ensure that the data protection policies and procedures are well

implemented, organizations shall appoint a strong network of data protection officers throughout the organization. This network needs to be defined in accordance with the company's structure and organization in order to ensure effective representation throughout the business units and legal entities of the company. Furthermore, it is also important to build a network of privacy relays who shall support data protection officers in their implementation program.

Use AI for data discovery and to improve data management

Enable data discovery through AI: For privacy compliance, organizations need a clear picture of all the types of personal data they process. They may, for example, possess personally identifiable data beyond name or address, including social media handles and financial transactions. A critical step is to clearly identify and map all personal data flows and where data is stored and processed within the organization. Proper data management, data profiling, analytics, data-centric architecture and Master Data Management (MDM) is essential to achieve this. MDM provides an organization the control it needs to master all of the data that it has by creating a single point of reference for consumer data and ensuring all data platforms align with this reference.

Data discovery through AI as an additional way to identify sensitive data at places and in situations where established practices may no longer be enough will be very useful, especially for large organizations operating in multiple geographies and firms undergoing mergers and acquisitions. In our research, we found that close to two-thirds of GDPR-compliant firms (65%) have AI solutions under development. AI can help organizations get clearer visibility of the consumer data that tends to sit in individual silos across the organization. It does this by improving the tracking and indexing of multiple data formats across different business units.

Map data processing activities and maintain a data protection register: The implementation of data protection constraints imposes to have a comprehensive mapping of data processing activities, including why and how personal data are processed by the company. In complex and global organizations, it is also essential to review and map key international data flows. This data mapping also enables companies to assess the level of compliance for each project and to enhance its overall level of compliance. Furthermore, the data mapping enables companies to comply with the GDPR requirement to maintain a data protection register. Such register is an inventory describing in particular the what, why and how of the personal data processing activities. Keeping such data protection register up to date enables the DPO to take local laws also into consideration to ensure compliance globally. *"We check if we have to make an amendment to our global standard to accommodate new regulations, or whether we take a hybrid approach to accommodate any local deviations,"* says Here Technologies' Henri Kujala.

Improve security of data using AI: There are a number of technical and organizational measures like identity and access management, pseudonymization, encryption and data loss prevention that can be used to ensure appropriate security levels are maintained to safeguard data. Despite the GDPR coming into effect, close to a quarter of non-compliant organizations (23%) have yet to implement approaches to safeguard personal data, such as masking, pseudonymization, etc.

Anonymization of personal data also needs to be considered while deploying new projects to enhance protection of the data processed. However, it is important to ensure that the technique implemented enable irreversible anonymization to ensure that the data ceases to be “personal data”. There are strict requirements to fall under such “anonymization qualification” – organizations therefore need to be cautious when claiming that personal data are anonymized and need to verify that they comply with the requirements defined by data protection authorities.

Organizations are increasingly turning to AI to improve the security of data. Given the risk of fines which authorities could impose and loss of consumer trust as a result of a breach, data security is becoming an important focus area for organizations. 71% of organizations use AI for data security, second only to network security at 75%. Identity and access management is also garnering organizations attention with 65% firms using AI for this area.⁸

Industrialize risk assessment and breach mitigation

Augment protection through security operations centers (SOC): Robust and operational risk assessment requires more than an ad-hoc approach. It is essential to have an

industrialized process that assesses the vulnerability of the systems that process personal data and that prioritizes issues according to the highest privacy risks. A SOC to monitor external and internal threats and vulnerabilities can improve organizational readiness to monitor and pre-empt breaches. Trained staff in SOCs also know how to escalate a security incident to the appropriate person or team in the organization, creating a more effective response to potential or on going data breaches:

- 49% of GDPR compliant firms have acted quickly and transparently when data breaches have occurred, compared to 36% of non-compliant firms.
- Over one in five non-compliant organizations (22%) have yet to document and implement procedures and processes to detect and manage data breaches in accordance with applicable laws.

Leverage platforms and the cloud for data protection: The cloud offers improved security for personal data compared to a data center. The executives we surveyed identified cloud platforms as the technology most commonly used for data protection and privacy (used by 84% of compliant firms). Stephen Schmidt, chief information security officer, AWS adds, *“Machines get racked and stacked in a data center and perhaps forgotten. People may not know what they are being used for or who put them there. You cannot hide in a cloud environment as you get visibility into exactly what you have, how it is connected and how it is configured over time. Our customers have told us repeatedly that this gives them a much, much better opportunity to secure things properly than they had before.”*

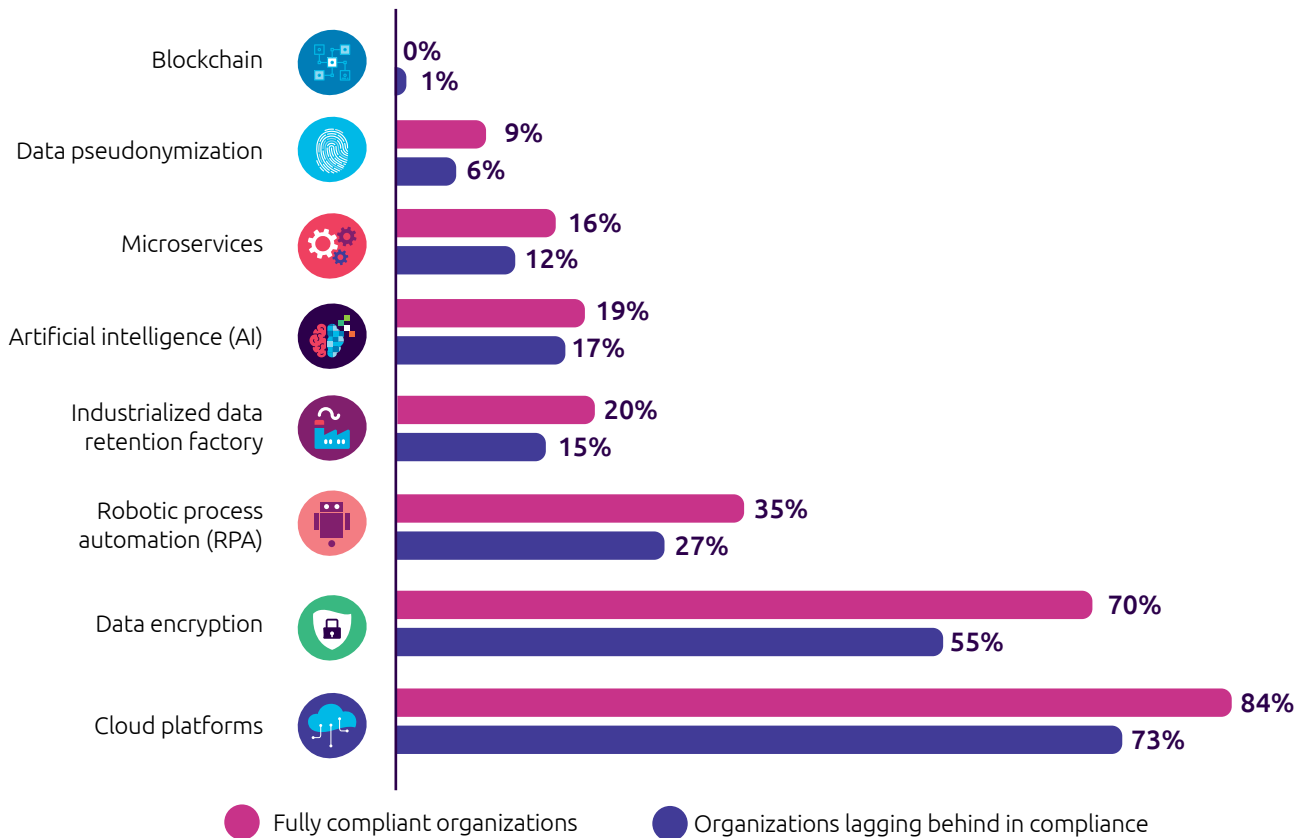


We check if we have to make an amendment to our global standard to accommodate new regulations, or whether we take a hybrid approach to accommodate any local deviations,

Henri Kujala, Here technologies

Figure 11. Cloud platforms and data encryption are organizations' choice of emerging technologies

Which of the following technologies is your organization already using for data protection and privacy?



Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n=1,100.

Establish integrated governance, risk management and compliance (iGRC) to build robust protection and privacy capability

Implement privacy compliance program: Organizations need to commit to a comprehensive privacy compliance program, addressing budget requirements, regular audits, legal policy reviews and updates, and awareness-raising programs. Critical elements are:

- **Leadership:** They need to assign a senior executive for program implementation and identify all relevant stakeholders critical for success. We found nearly one in five non-compliant organizations have still failed to appoint an executive responsible for data protection and privacy compliance.
- **Measurement:** Regular measurement of KPIs to monitor progress regarding data protection and privacy regulation compliance is critical.

One way to ensure success is by implementing iGRC for analytics and business intelligence functions in organizations by ensuring data collection, storage, and processing is always viewed from a privacy and protection perspective.

Sustained communication across the organization, coupled with a cultural shift on how employees view data privacy and protection, is essential to achieve this.

Carry out due diligence on third party providers/partners and monitor compliance through audits When relying on third party providers, organizations shall carry out thorough due diligence in particular regarding the third-party provider's or partner's the level of compliance with GDPR requirements and any other data protection legislation. Organizations must also review existing contracts with third parties/sub-contractors/cloud service providers. Privacy compliance, especially regarding access to IT systems and data subjects' personal data, is important to ensure an adequate level of personal data protection and security measures. It is also important to verify that during the entire lifecycle of

a relationship with third party providers/partners, data protection audits are scheduled. We found that:

- 82% of GDPR-compliant organizations have taken steps to ensure that technology vendors (technology product firms, cloud vendors, data centers, hardware/infrastructure, etc.) are compliant with applicable data privacy regulations, compared to 63% of non-compliant vendors.
- 61% of compliant firms also audited sub-contractors for compliance with data protection and privacy regulations, compared to 48% for non-compliant firms.



Conclusion

The increasing focus on data protection and privacy – and the introduction of more stringent regulations – is a global movement. While the GDPR is arguably the most comprehensive and far-reaching regulation so far, it is unlikely to be the last. This means that while many organizations are now grappling with the immediate need to meet compliance requirements, they must also be aware that this is not the end game. Data protection and privacy regulation is a continuous process that demands ongoing performance monitoring and improvement. Organizations need to promote a data protection and privacy mindset among employees and integrate advanced technologies to boost data discovery, data management, data quality, cybersecurity, and information security efficiencies. Firms that take these actions proactively – and view data protection and privacy regulation as an opportunity – will secure a significant competitive advantage.

GDPR readiness assessment

To see where your firm stands in terms of data privacy and protection, this maturity assessment tool is included for your convenience. Using the key immediately below, mark your organization's current level of maturity in the chart, then tally up the scores. The legend below the assessment chart indicates your firm's level of preparedness.

0-Not implemented 1-Under implementation 2-Implemented 3-Implemented, audited, and under improvement

		0	1	2	3	Score for section
Governance	A Data Protection Officer (DPO) within the organization has been appointed					
	The DPO reports to the highest management authority in the organization					
	There is a policy and methodology for privacy by design					
	A privacy notice exists that explains your organization's policy on personal data processing?					
	There a policy and methodology for privacy by default (including data minimization)					
	Agreements are in place with third-party processors of personal data					
	Training programs to raise employees' awareness on personal data issues and regulations					
Data	There is a complete overview of personal data and processing systems					
	There is a complete and up-to-date understanding of "personal data" according to the GDPR					
	There are well-defined and maintained legal grounds for processing personal data					
	There is a well-defined process for transferring data between geographies when there is a legal basis					
	The contact details of the data controller and the DPO (if applicable) are made available to the data subjects for exercising data-subject rights (i.e., the right to access, rectification, and erasure) and proper records are maintained					
	There is a policy and process for archiving/deleting data when no longer necessary					
Security	There are business processes that classify risk involving personal data as low, medium, or high to help perform data privacy impact assessments					
	There is a documented procedure and process in place to detect and manage data breaches in accordance with the GDPR (within 72 hours) and related specific laws					
	Safeguards (e.g., anonymization, masking, pseudonymization, etc.) are available to protect personal data					
Process	A business process for complaints concerning privacy and personal data processing exists					
	Regarding direct marketing activities, the consent offered by the data subjects is freely given, specific, informed, and unambiguous					
	Consent is obtained from parents in the case of processing personal data of minors					
	There is a documented procedure in place to uphold data subjects' rights (e.g., access, accuracy, erasure, etc.)					
	There is a procedure to check the correct implementation of personal data protection policies					
	There is a procedure to maintain the scope of personal data and track changes					
Total						

Overall score legend: 0–22: Low level of maturity for data privacy and protection
 23–44: Medium level of maturity for data privacy and protection
 45–66: High level of maturity for data privacy and protection

Research Methodology

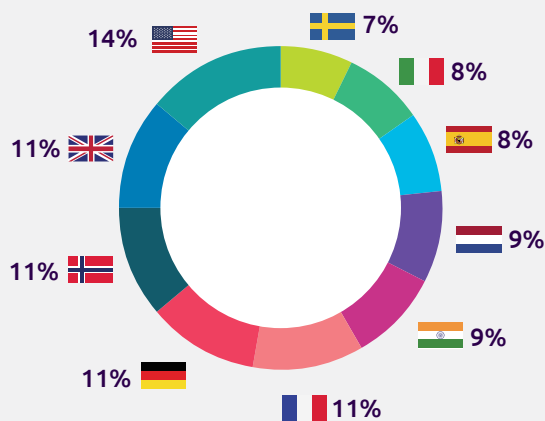
Primary surveys

Executive survey:

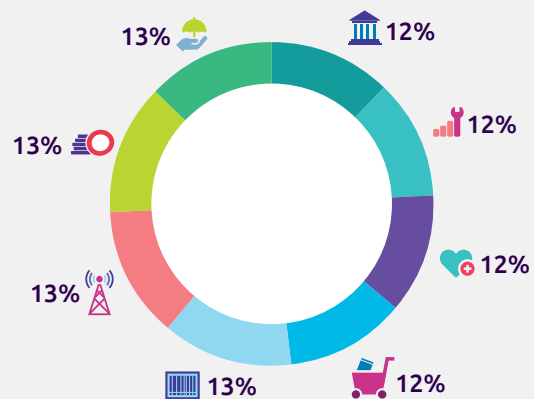
We surveyed 1,100 senior executives, director level and above, spread across eight sectors: insurance, banking, consumer products, utilities, telecom, public services, healthcare, and retail.

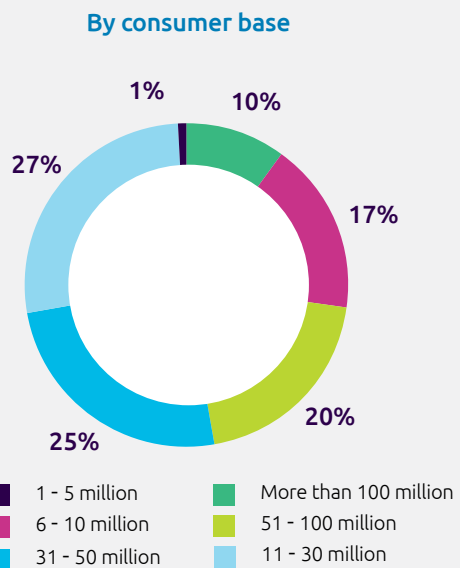
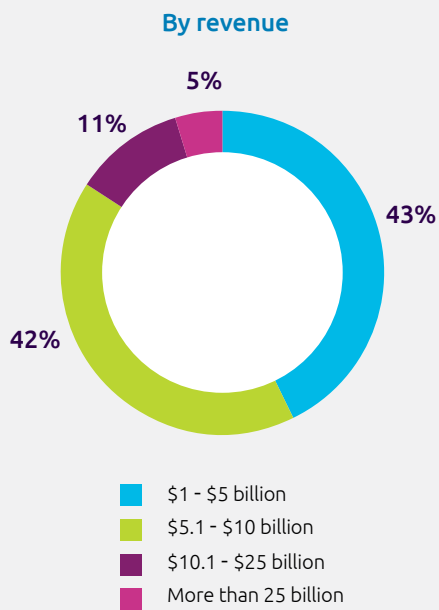
Executives belong to companies headquartered in: France, Germany, Italy, the Netherlands, Norway, Spain, Sweden, the UK, the US, and India.

By country of headquarters



By sector of operation





Focus interviews:

We also conducted interviews with industry leaders and experts, examining the current status and impact of data privacy regulations.

Achieve and maintain the unavoidable opportunity with Capgemini's GDPR and Data Privacy Services

GDPR has now been in effect for over a year, and we are starting to see similar regulations being implemented across the globe

We can implement practical solutions to help you achieve and maintain compliance and use data more strategically to benefit from the many opportunities that effective Data Privacy offers—in terms of greater trust and competitiveness. And we do so in the most cost-effective way possible. Our thousands of professionals in all regions deliver agility in both our working practices and digital capabilities, providing strategic consultancy and hands-on implementation across the GDPR and general Data Privacy lifecycle. They ensure organizations get access to deep experience in the domains that truly matter: Change Management and Digital Transformation, Governance, Risk & Compliance, Security & Protection and Data Management and Governance. We're able to design and hardwire increased trust across the entire process, safeguarding the personal data rights of individual citizens, customers and employees – and turning that into wider operational and business gains.

Our approach to achieve and sustain compliance and help you take advantage of the opportunity, is built around the comprehensive portfolio of modular and scalable services below. Let us show you how accelerating your Data Privacy journey can bring significant benefits and competitive advantage. If you wonder whether you've missed out on the advantages, the development of proof of concepts can help guide decisions. If you need to make sure you remain compliant our As-a-Service, cloud-based models allow you to start small and cost effectively.

Assessment Services: Delivers a view on your processing compliance, strategic vision, Data Privacy awareness and integrates all internal and external teams.

Program Services: Designs the program to get you moving towards Data Privacy compliance and allows you to adapt and customize regulatory principles to your specific challenges, context, processes and culture.

Data Discovery Services: Allows you to understand and document where personal data exists throughout your organization and is the starting point for many aspects of Privacy Regulation, such as responding to access requests.

Data lifecycle services: Privacy requires organizations to only use as much data as is required to successfully complete a given task. It cannot be reused for another purpose without further consent a valid legal ground (such as consent). Individuals have the right to request that their data to be erased after a specific task, and our lifecycle services ensure that care is taken during the creation, processing and disposal of data.

Consent and Individual's Rights Management Services: Analyses where consent is needed and how it can be (re)obtained. Implements processes and systems, which allow individuals to invoke their rights, such as the right to access their data and the right to be forgotten.

Pseudonymizing Services: Provides role-based access, masked and anonymized data for purposes like testing, marketing and analytics, and allows you to share data with external and internal audiences.

Data Protection Services: Defines and implements controls and solutions to ensure the proper protection of structured and unstructured data, and so reduce risk. Controls include access, encryption, key management and database access monitoring.

Breach Management and Reporting Services: Security-operations-center-as-a-Service for monitoring external threats and vulnerabilities, plus Data-leak-prevention-as-a-Service for monitoring personal data repositories and flows.

Assurance Services: Once you are compliant, our Assurance Services ensure you remain so by monitoring, maintaining and updating your systems, processes and policies.

References

1. Compliance, in this case, means the surveyed organizations' interpretation of fully meeting the requirements of the GDPR.
2. EU, "What are the GDPR Fines?," April 2018.
3. IAPP, "Top 5 Operational Impacts of CCPA: Part 5 – Penalties and enforcement mechanisms," August 2018.
4. BBC, "Four times more data breaches logged in UK," May 2019.
5. CSO, "California Consumer Privacy Act (CCPA): What you need to know to be compliant," July 2019.
6. The General Data Protection Regulation, "Special Eurobarometer 487a," June, 2019.
7. IAPP, "Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization." February 2016.
8. VentureBeat, "Intel open-sources HE-Transformer, a tool that allows AI models to operate on encrypted data," December 2018.

About the Authors



Zhiwei Jiang

Executive Vice President and CEO, Capgemini Insights & Data

zhiwei.jiang@capgemini.com

Zhiwei Jiang is the CEO of the Insights and Data (I&D) Global Business Line (GBL) at Capgemini where he leads the global team of 15,000+ staff members across North America, Europe and Asia Pacific. Capgemini I&D GBL is consistently ranked as a leader in data and analytics domain by Gartner, Forrester, Everest, Nelson Hall and other analysts. Zhiwei has deep domain expertise in data analytics, data trust, data integration, data quality, risk, and regulations; he has extensive management and execution experience spanning multiple continents, including Europe, America, and Asia. Previously, Zhiwei was a managing director at Deutsche Bank, managing finance and risk IT in application services and also led Deutsche Bank's connectivity domain globally and managed equities IT for the EMEA and APAC regions.



Ron Tolido

Executive Vice President and CTO, Capgemini Insights and Data

ron.tolido@capgemini.com

Ron is the lead-author of Capgemini's TechnoVision trend series and responsible for Artificial Intelligence within Capgemini's Chief Technology & Innovation Network. With global clients, he focuses on innovation, agile architecture, digital strategy and AI.



Steve Jones

Executive Vice President, Capgemini Insights and Data

steve.g.jones@capgemini.com

Steve Jones an EVP at Capgemini and the Head of Insights and Data North America. Steve is a published author and regular contributor to journals including the Financial Times and CIO.com, he was the creator of the industry's first unified architecture for big, fast, secure, managed data: The Business Data Lake, which is now an Open Standard via Open Group. Steve works with clients on how to evolve their information landscapes away from batch oriented BI towards insight at the point of action, where analytics embedded within operational flows becomes the norm.

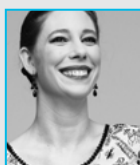


Graham Hunt

Director-UK Financial Services Insights and Data

graham.hunt@capgemini.com

Graham Hunt specialises in Data Ethics, Data Privacy and Regulatory Reporting for Financial Services Organisations. He has helped organisations set up Data Protection Office functions and has hands on experience in running DPOs and Breach Management triage, rectification and longer-term customer data remediation. He has worked in the four big banks in the UK as well as a number of other financial services organisations over the past 30 years.



Isabelle BUDOR

Vice President, Capgemini Invent, Data Privacy & Ethics Leader

isabelle.budor@capgemini.com

Isabelle leads the Data Privacy & Ethics offer for France and co-leads the Capgemini Group Data Privacy Offer. She has helped many clients with privacy, BCRs, GDPR operational transformation in various sectors such as Financial Services, Oil & Gas, Industry, Customer Product and Citizen Services. She is also now very much focused on new privacy topics such as portability or how to make AI privacy compliant and more generally how to build a trusted, ethical and sustainable AI.



Emmanuelle Bartoli

Group Data Protection Officer

emmanuelle.bartoli@capgemini.com

Emmanuelle is the Group Data Protection Officer and Legal Cybersecurity Lead. She is responsible for defining Capgemini data protection and cybersecurity compliance program from a legal standpoint. She works closely with the internal stakeholders to ensure that data protection constraints are taken into account in the entire lifecycle of our projects while remaining business oriented. Emmanuelle has developed an extensive experience and knowledge on data protection as she started her career with the French Data Protection Authority (CNIL), prior to joining another IT company as the Group DPO and being a Senior Associate at two major UK and US law firms.



Paul van der Linden
Principal Consultant, Capgemini Insights and Data
paul.vander.linden@capgemini.com

Paul is a certified GDPR practitioner (CIPM, CIPT, CIPP/E) and has been involved in GDPR implementations throughout Europe since 2016. He is a certified architect (TOGAF 9) with a background in data management, BI, analytics, data warehousing, big data, master data management and data governance. He has written various articles and co-authored books on these topics. Paul contributed to Capgemini's GDPR Building Blocks.



Jerome Buvat
Global Head of Research and Head of Capgemini Research Institute
jerome.buvat@capgemini.com

Jerome is head of the Capgemini Research Institute. He works closely with industry leaders and academics to help organizations understand the nature and impact of digital disruption.



Jeff Theisler
Managing Consultant, Capgemini Invent North America
jeffrey.theisler@capgemini.com

Jeff Theisler is a managing consultant with Capgemini Invent. He helps clients solve complex business problems, with and without the use of technology-based solutions. Recently, he has been working with the Capgemini Research Institute exploring topics of global interest.



Alex Wortmann (PhD)
Executive Vice President, Capgemini Netherlands
alex.wortmann@capgemini.com

Alex is Executive Vice President in Capgemini Insights & Data



Sumit Cherian
Manager, Capgemini Research Institute
sumit.cherian@capgemini.com

Sumit is a manager at the Capgemini Research Institute. He leads research initiatives across sectors to help clients understand how digital technologies disrupt business landscape and consumer behavior.



Yashwardhan Khemka
Manager, Capgemini Research Institute
yashwardhan.khemka@capgemini.com

Yash is a manager at the Capgemini Research Institute. He likes to follow disruption fuelled by technology across sectors.

The authors would like to especially thank Tor-Stale Hansen and Subrahmanyam KVJ from Capgemini Research Institute for their contribution to the report.

The authors would also like to thank Pengcheng Lee, Sally Li, Odile Durand, Himanshu Gupta, Srividya Manchiraju, Faisal Saudagar, Ganesh Samvaran, Vinutha Naik, Krithika Venkataraman, Ramana Bhandaru, Ivar Aune, Jose Luis Diaz-Rivera, Eva Terni, Karl Bjurstrom, Jens Middborg, Fabio Tinetti, Fredrik Gunnarsson, Scott Sweet, Drew Morefield, Ashvin Parmar, Aaron Fontenot, James Farnsworth, Ulf Larson, Kristin O'Herlihy, Bob Underwood, Chris Cooper, Carmen Dufur Mendivil, Niraj Parihar, Mark Battersby, Willem de Paepe, Pierre-Luc Refalo and Philippe Kerael for their contribution to the report.

About the Capgemini Research Institute

The Capgemini Research Institute is Capgemini's in-house think tank on all things digital. The Institute publishes research on the impact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The Institute has dedicated research centers in India, the United Kingdom, and the United States. It was recently ranked Top 1 in the world for the quality of its research by independent analysts.

Visit us at www.capgemini.com/researchinstitute/

For more information, please contact:

Global

Zhiwei Jiang

zhiwei.jiang@capgemini.com

France

Isabelle Budor

isabelle.budor@capgemini.com

Nordics

Shuja Rahman

shuja.rahman@capgemini.com

Dach

Christian Kaupa

christian.kaupa@capgemini.com

UK

Chris Cooper

chris.cooper@capgemini.com

Lee Smith

lee.c.smith@capgemini.com

Spain

Jose Luis Diaz-Rivera

jose-luis.diaz-rivera@capgemini.com

Carmen Dufur

carmen.dufur@capgemini.com

Italy

Fabio Tinetti

fabio.tinetti@capgemini.com

India

Himanshu Gupta

himanshu.gupta@capgemini.com

China

Sally Li

sally.li@capgemini.com

Netherlands

Paul Van der Linden

paul.vander.linden@capgemini.com

US

Steve Jones

steve.q.jones@capgemini.com

Sweden/Finland

Ulf Larson

ulf.larson@capgemini.com

Discover more about our recent research on digital transformation



[Why addressing ethical questions in AI will benefit organizations](#)



[Cybersecurity talent—the big gap in cyber protection](#)



[Seizing the GDPR Advantage: From mandate to high-value opportunity](#)



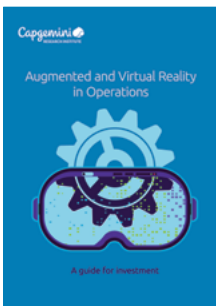
[Digital Transformation Review: 12th Edition](#)



[Cybersecurity: The New Source of Competitive Advantage for Retailers](#)



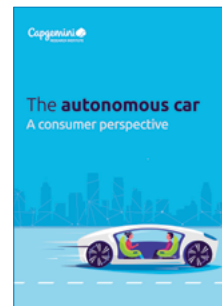
[The need for speed: Four recommendations to turbo-charge digital performance in the automotive industry](#)



[Augmented and Virtual Reality in Operations: A guide for investments](#)



[Reinventing Cybersecurity with Artificial Intelligence](#)



[The Autonomous Car: A Consumer Perspective](#)





About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Visit us at

www.capgemini.com

People matter, results count.

The information contained in this document is proprietary. ©2019 Capgemini.
All rights reserved.