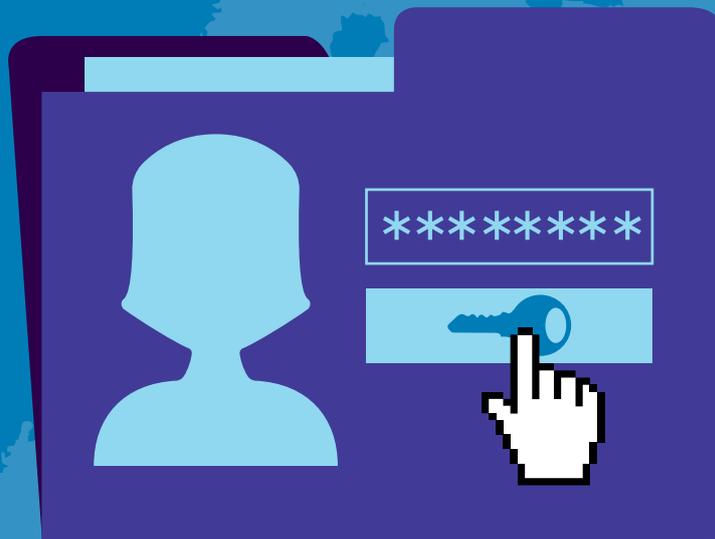




Seizing the GDPR Advantage

From mandate to high-value opportunity



By Capgemini Digital Transformation Institute

Introduction



Europe's Global Data Protection Regulation (GDPR) is a ground-breaking regulation that aims to put control over personal data back into the hands of individuals. Sighting this uphill task and fearing stricter regulatory action owing to non-compliance, many organizations are scrambling to be ready as soon as possible. In this report, we look beyond the compliance side of GDPR and uncover the latent opportunity that can help organizations gain individuals' trust and competitive advantage. We surveyed 6,000 individuals and 1,000 industry executives across eight countries to gather their views on this subject (see Research Methodology for more details). Our research affirms that:

- The GDPR is an opportunity waiting to be tapped – individuals are more willing to engage with, and be more loyal to, organizations that protect data, and going above and beyond the GDPR brings even greater reward.
- However, most organizations are not ready to seize this opportunity – significant work remains to be done to increase not only compliance levels but also compliance maturity and to bridge the gap between the preparedness of organizations and the expectation of individuals.
- An immature approach will have significant consequences because consumers are prepared to take action if they are unhappy with organizations' GDPR compliance performance.
- To convert the GDPR from mandate to opportunity, organizations must take a series of steps, ranging from educating customers and citizens and winning their trust, to building a culture of respect for personal data within the organization.

The GDPR is an opportunity waiting to be tapped



“Whatever the size of your organization, the GDPR is essentially about trust. Building trusted relationships with the public will enable you to sustainably build your use of data and gain more value.”

Steve Wood, deputy commissioner for policy at the UK’s Information Commissioner’s Office (ICO)¹

Steve Wood’s words are a rallying cry to see Europe’s General Data Protection Regulation as more than just a compliance exercise. Instead, organizations should see it as a significant opportunity to build consumer trust and turn organizational data into value in a sustainable way. However, despite this clear prize on offer, many organizations have limited ambitions and a perfunctory approach to ensuring compliance by the go-live date of May 25, 2018.

We surveyed 6,000 European consumers and 1,000 industry executives to determine and quantify the wider GDPR opportunity. Our research finds that complying with GDPR – and going above and beyond its requirements – offers significant benefits.

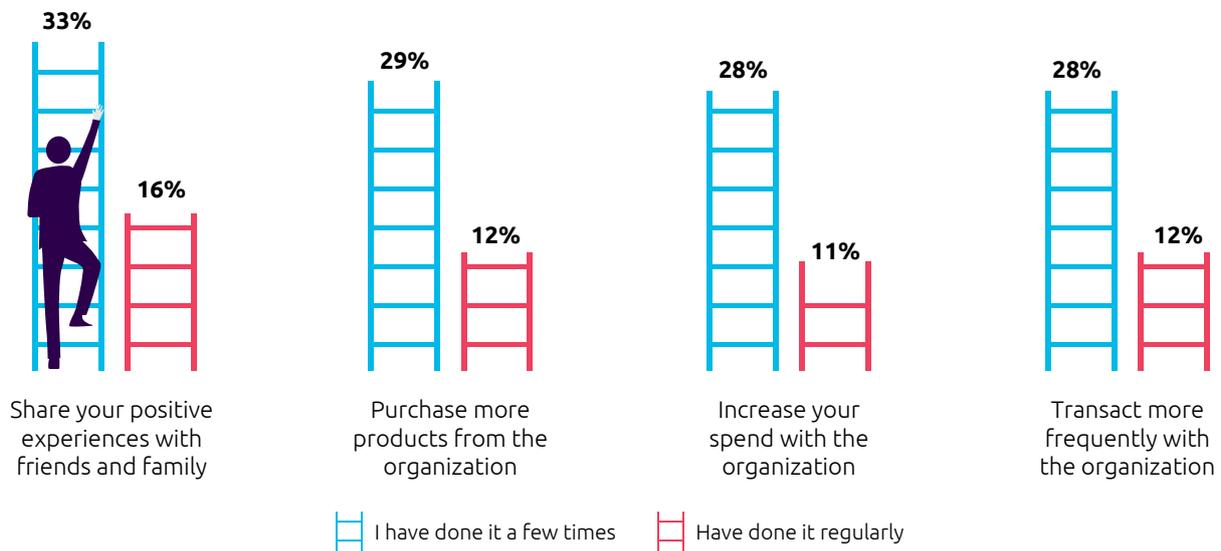
Compliance brings immediate benefits

Our research shows that a narrow approach focused solely on compliance ignores some of the upside. We show that getting the GDPR right:

1. Encourages consumers to spend more, as consumers who trust organizations when it comes to data privacy are willing to spend more
2. Enhances employee loyalty.

Figure 1. Consumers are willing to engage more with GDPR-compliant organizations.

As a consumer, which of the following have you done when you are convinced that the organization you are interacting with is protecting your personal data? (Percentage of individuals)



Source: Capgemini Digital Transformation Institute GDPR Individuals Survey, March–April 2018.

More than one in three consumers **(39%)** will spend more with an organization when convinced that the organization protects their personal data

1. Consumers are more willing to engage with organizations that protect data. When consumers are convinced that an organization is protecting their personal data in line with the GDPR mandate, nearly half (49%) would share their positive experiences with friends and family (see Figure 1). In addition, consumers have already rewarded organizations that have better data protection and are likely to do so again once the GDPR is in effect:

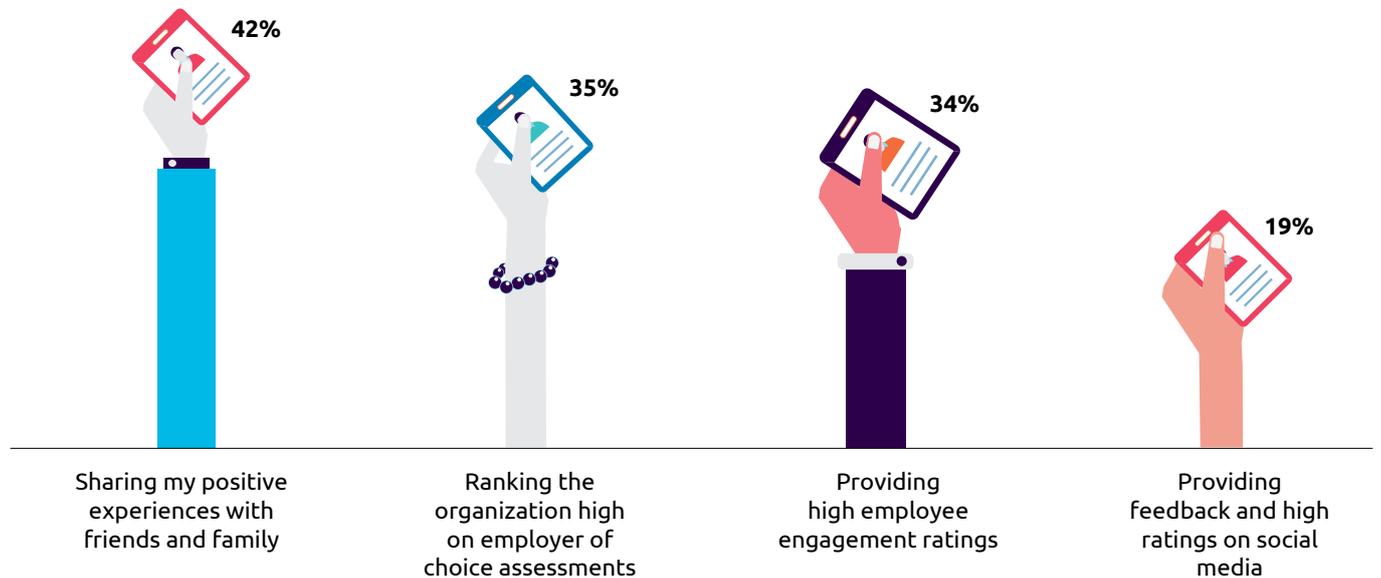
- 40% have transacted more frequently with the organization, either a few times or on a regular basis
- 39% have purchased more products
- 39% have increased spend, with those who have increased it spending as much as 24% more, for instance, on premium or more expensive products and services.

“It [GDPR] will encourage marketers to talk to people when they need something and not simply contact them about something they might want. Rather than pushing products using flaky data, we can handle data in a smart way to create magic moments when people really require help,” says Rupert Bedell, CMO of Unum, a leading insurance firm in the US and UK.

2. GDPR compliance enhances employee loyalty. The positive ripple effects of the GDPR are not just limited to consumers. As Figure 2 shows, employees reward their employers with higher loyalty and positive word-of-mouth when they are convinced that their employer is protecting their personal data.

Figure 2. Employees turn into advocates of their employers when they are convinced that their personal data is protected.

As an employee, what have you done when you are convinced that the organization you are employed with is protecting your personal data? (Percentage of employees who are likely to take these actions based on their past behavior)



Source: Capgemini Digital Transformation Institute GDPR Individuals Survey, March–April 2018.

More than one in three employees **(35%)** are likely to provide high ratings to their employer when convinced that their personal data is protected

Going above and beyond GDPR guidelines brings even greater rewards

While achieving compliance makes good business sense, our research found further untapped opportunity for organizations willing to go one step further. Today's consumers are already thinking far beyond regulatory compliance in how they evaluate organizations and decide which ones receive their business. We find this in a significant set of consumers (over one in five, or 22% of the population), who we call "Data Rights Advocates." These advocates expect organizations to go above and beyond the GDPR mandate and are willing to give more business and loyalty in exchange.

We identified three levels of consumers in terms of GDPR expectations, ranging from those who are satisfied with a basic level of compliance to those who want organizations to go much further:

- Level 1 – **Data-Indifferent consumers (45%)**. These consumers are unaware of what the GDPR means for them or believe that it makes no difference to them. They are also indifferent toward the data privacy standards of the organizations they deal with. For example, they do not expect organizations to have very high security standards that specifically focus on personal data.
- Level 2 – **Data-Engaged consumers (34%)**. These are consumers who expect above-average compliance standards. For example, they want to hear from organizations as GDPR-related changes are rolled out.
- Level 3 – **Data Rights Advocates (22%)**. These are consumers who expect organizations to go the extra mile and provide a state-of-the-art experience when it comes to personal data security and privacy. They will strongly promote organizations that clearly and visibly demonstrate their commitment to personal data privacy.

As Figure 3 shows, Data Rights Advocates provide the richest rewards for organizations, in areas such as average extra spend and willingness to promote the company:

- We asked consumers whether they increase their spend when convinced that an organization is protecting their personal data. Nearly half of Digital Rights Advocates have done so in the past – more than other two categories. They are also willing to increase their spend by an additional 14% – significantly more than consumers in the other two categories.
- Data Rights Advocates are also likely to be strong promoters (45%) of those organizations that demonstrate a commitment to protect data rights. This is significantly more than the Data-Engaged (18%) and Data-Indifferent consumers (8%). The average NPS for organizations from Data Rights Advocates only would be +15. But from Data-Engaged and Data-Indifferent consumers, it would be -26 and -65 respectively.

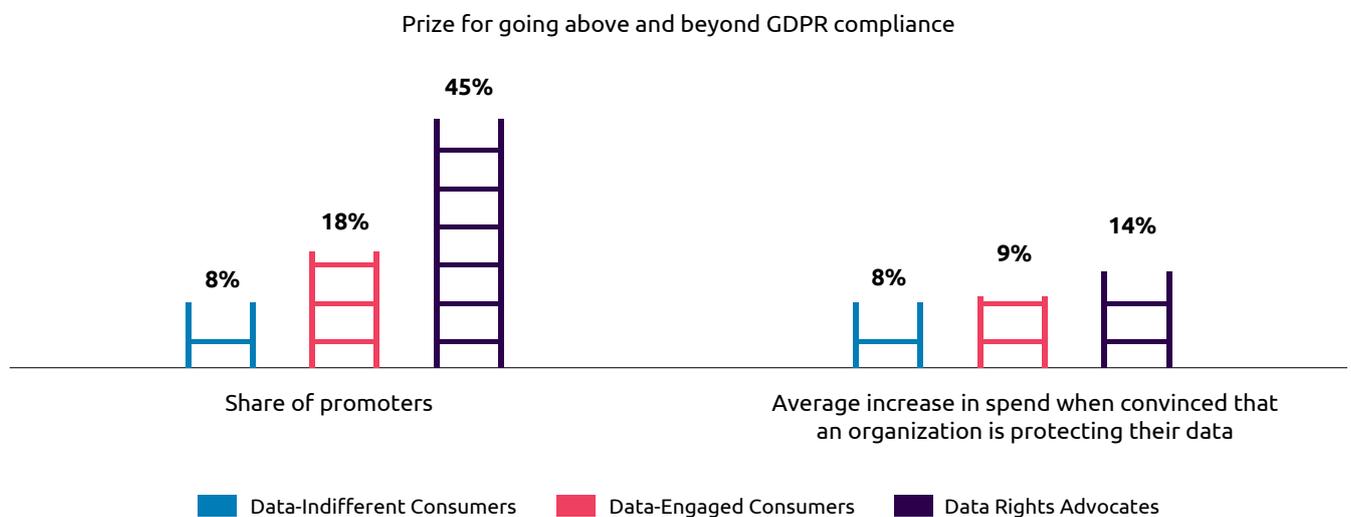
Leading organizations recognize this opportunity and shape their GDPR strategy around it. Marek Pietrzyk, security project manager at the Swiss bank UBS, said: *"Our goal was to have a sophisticated system for protecting customer data that can also be used as a way of differentiating us from our competitors and of attracting new customers."*¹³

45% of Data Rights Advocates will be promoters of organizations that demonstrate a commitment to protect data rights – more than the other two consumer categories

14%

Average increase in spend by Data Rights Advocates when convinced that an organization is protecting their data

Figure 3. Customers reward organizations that go above and beyond.



Data-Indifferent Consumers (45%)

- Unaware of what the GDPR means for them or think that it makes no difference
- Are indifferent to data privacy standards of organizations they deal with
- Do not place a high emphasis on engaging with the organization or hearing from them about how the GDPR will affect them
- Do not desire better control over their data held by organizations



Data-Engaged Consumers (34%)

- Expect an above-average level of GDPR compliance e.g. Simpler privacy policies and a better security standards
- Want to be kept engaged by organizations and be rewarded for their engagement
- Expect offers and promotions in exchange for sharing personal data in conformance with the GDPR



Data Rights Advocates (22%)

- Expect organizations to go above and beyond the GDPR
- Give high importance to: simple and clear privacy policies, innovative ways to manage their personal data, and having best possible controls over their data held by organizations
- Place a very high level of trust in organizations that clearly and visibly demonstrate their commitment to data privacy

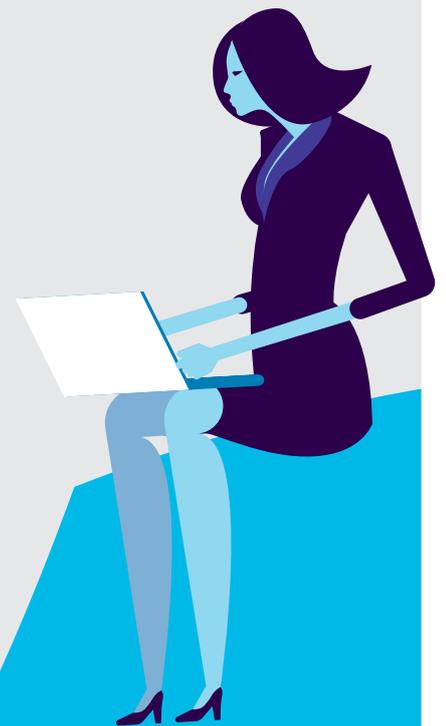
Who are the Data Rights Advocates?

This cohort displays several characteristics that set them apart from others. They are a group who:

- Are aware of the GDPR and what it means for them
- Place higher emphasis on data privacy and security
- Expect organizations to follow the GDPR in word and spirit (see Figure below).

- More than half (53%) are **fully aware of the GDPR** and what it means for them
- About a third (30%) are **millennials** (<32 years of age)
- They **expect very high standards of compliance**
 - 91% expect organizations to go above and beyond GDPR to ensure personal data privacy and security
- They are **likely to take stricter actions** against non-compliant organizations
 - 55% will reduce their spending with organizations they see as non-compliant vs. 37% of all other consumers
- They are also **likely to reward highly** for higher standards of data protection
 - 48% will increase their spending and by upto 18% on average for receiving a better experience with respect to the privacy and security of their data

Source: Capgemini Digital Transformation Institute GDPR Individuals Survey, March–April 2018, Capgemini Digital Transformation Institute Analysis.



The maturity challenge – most organizations are not equipped to seize the GDPR advantage



While the benefits of GDPR compliance are significant, very few organizations are well positioned to seize the opportunity. Reasons include:

- A failure to give the GDPR the attention it deserves, with many taking a perfunctory approach
- Lack of preparedness
- A tendency to be out-of-sync with consumers' data privacy expectations.

One in two organizations has a perfunctory approach to the GDPR

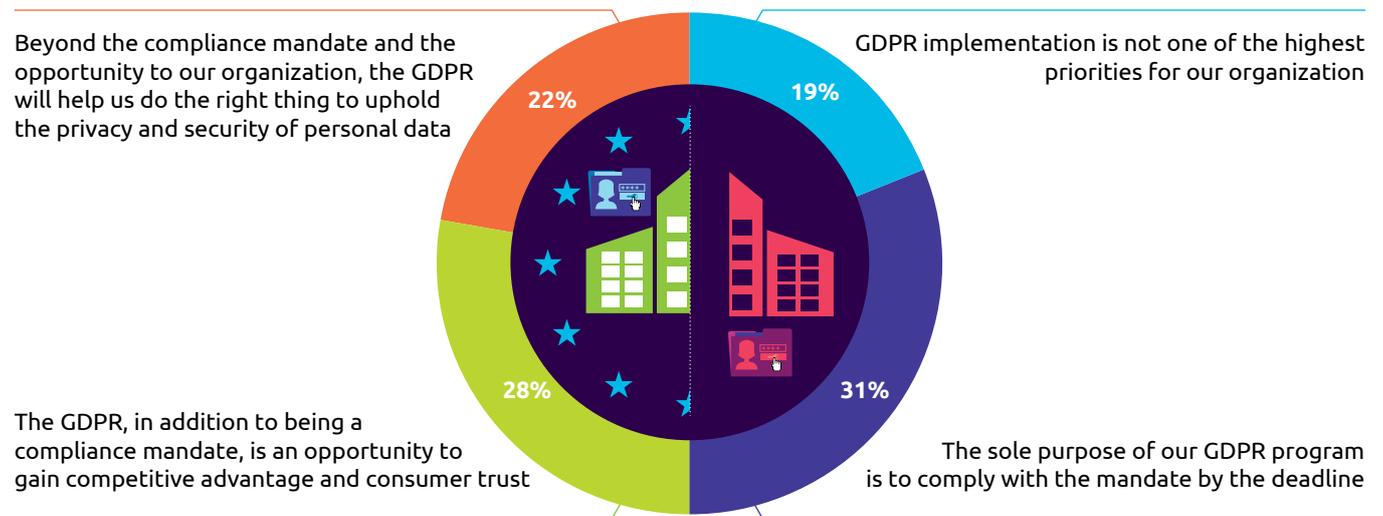
Many organizations fail to give the GDPR the attention it deserves:

- Nearly one in five organizations (19%) fail to make the GDPR a top priority (see Figure 4).

- 31% feel that the sole purpose of their program is to comply with the mandate by the deadline.
- Only around a quarter of organizations (28%) see the GDPR as an opportunity to gain consumer trust and competitive advantage, in addition to being a compliance mandate.

Figure 4. Nearly half of the organizations are taking a perfunctory approach to the GDPR.

Which of the following statements best describes your current approach to GDPR implementation



Numbers may not total to hundred, due to rounding.

Source: Capgemini Digital Transformation Institute GDPR Executive Survey, March–April 2018.

Only about one in four **(28%)** organizations believe that the GDPR is an opportunity in addition to being a compliance mandate

Nearly half of organizations are lagging in terms of compliance

One manifestation of this perfunctory approach is that most organizations are still lagging in terms of compliance. As

Figure 5 shows, 51% of organizations are either lagging or feel they will be only partially compliant by the deadline.

Figure 5. Nearly half of organizations are lagging even as the deadline looms



Source: Capgemini Digital Transformation Institute GDPR Executive Survey, March–April 2018.

When asked how long it would take to reach compliance, 85% said it would take more than three months – beyond the GDPR go-live date. One in four organizations (26%) will not be ready for the GDPR by the end of 2018, as Figure 6 shows. *“A sizeable number of organizations won’t be ready by the deadline and beyond,”* says the Data Protection Officer at a

large UK retailer. *“The key would be to ensure that the basic requirements of the law are adhered to. It also means being able to demonstrate to data protection authorities that the organization has put in place a foundation for the GDPR and is working toward compliance at full speed.”*

Figure 6. 85% of organizations are unprepared for the GDPR deadline.



Source: Capgemini Digital Transformation Institute GDPR Executive Survey, March–April 2018.

It is worth noting that although organizations are working toward compliance, the maturity of the compliance will vary across organizations. While many organizations will at first be compliant using manual processes, some will automate compliance requirements, and a few will likely take a strategic view and set up robust processes and systems to meet regular compliance obligations. As such, organizations would continue to improve their maturity of their compliance processes well beyond the date they become GDPR compliant.

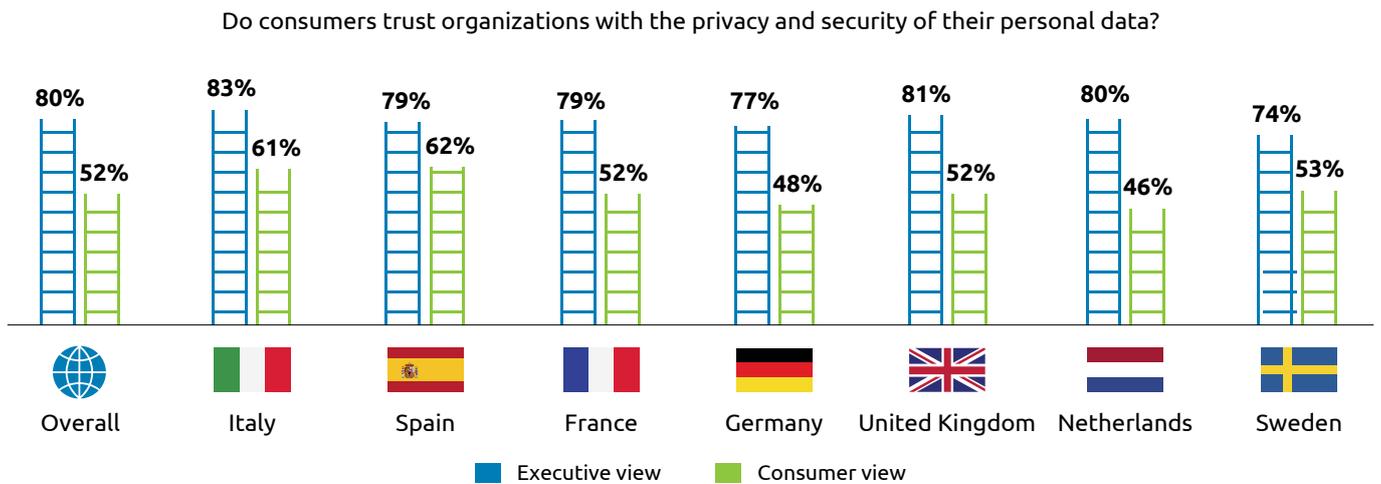
Organizations are out-of-sync with consumers' data privacy expectations

There is a significant perception gap between organizations and consumers around consumer data privacy and security performance:

- On average, 80% of executives believe that consumers trust their organization with the privacy and security of personal data
- But only 52% of consumers agree (see Figure 7).

This overconfidence can blind organizations to the improvements they need to make in data practices and prevent sufficient investment. Such organizations will eventually lose out as consumers increasingly demand a best-in-class data protection experience.

Figure 7. Organizations overestimate consumer trust.



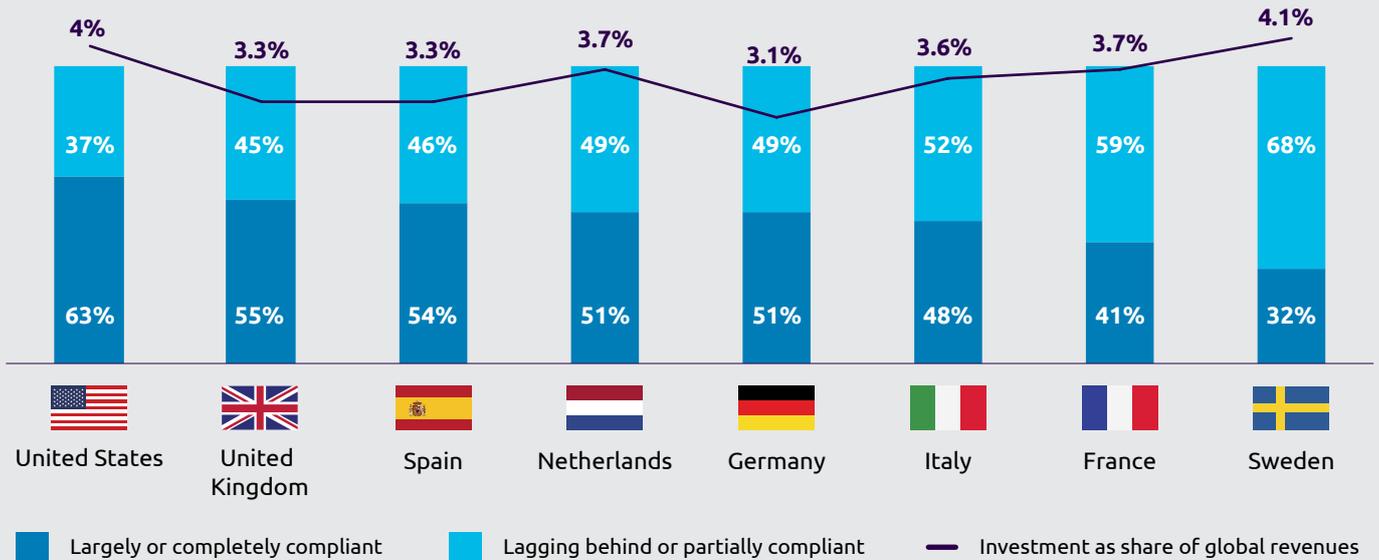
Source: Capgemini Digital Transformation Institute GDPR Executive and Individuals Survey, March–April 2018.

80% of executives believe that consumers trust their organization with data privacy while only **52%** of consumers agree

The state of GDPR compliance

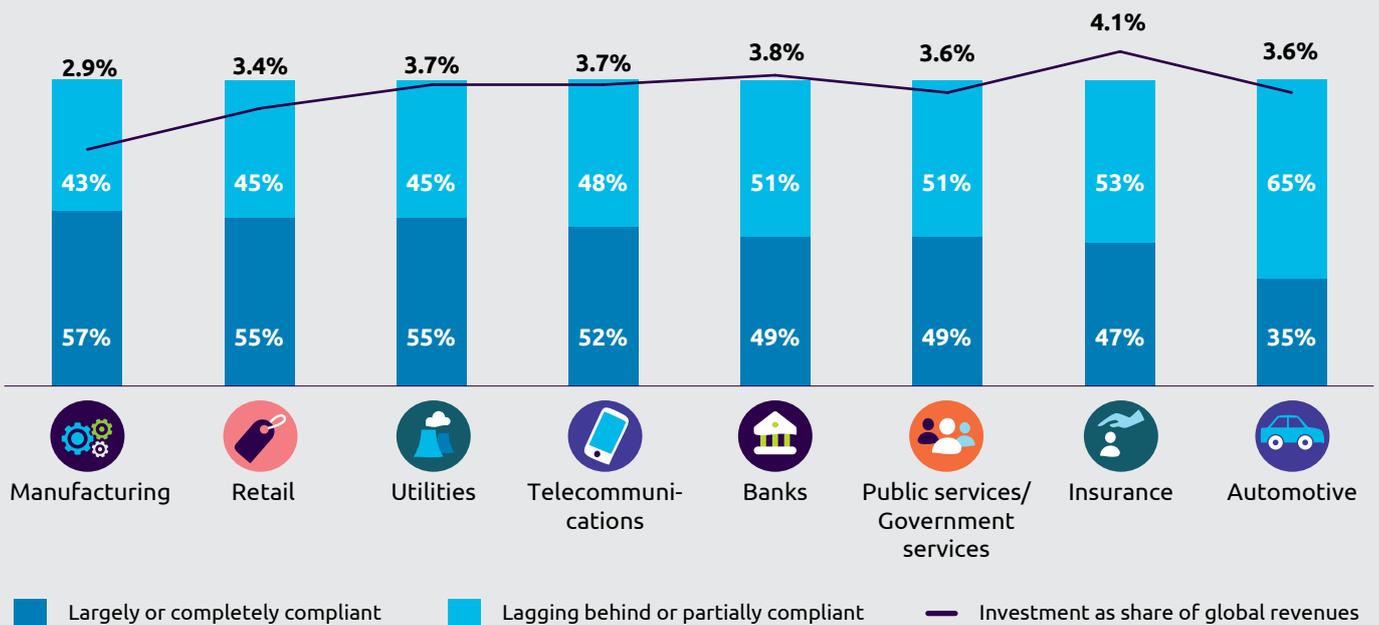
The US, UK, and Spain lead all other countries in GDPR compliance

GDPR compliance, by country



Manufacturing, Retail, and Utilities lead other sectors in GDPR compliance

GDPR compliance, by sector



Based on executive responses to the question: "How ready is your organization for the GDPR? (please select one that applies to your organization) – completely compliant, largely compliant, partially compliant by the deadline, and lagging behind."

Source: Capgemini Digital Transformation Institute GDPR Executive Survey, March–April 2018.

An immature approach will have significant consequences



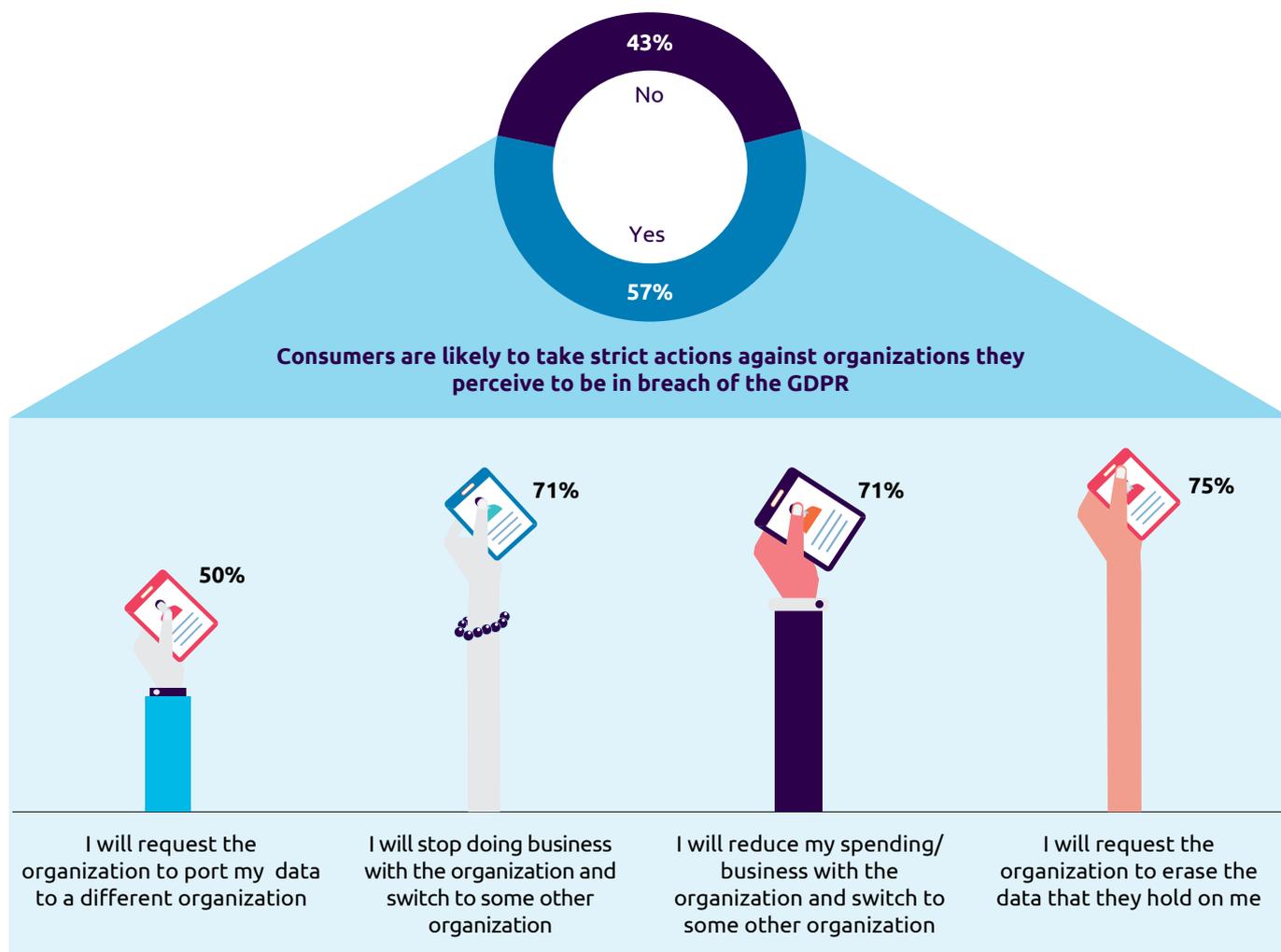
Consumers will take action if they are unhappy with GDPR compliance levels

More than half of consumers (57%) will likely take action when they find out that an organization is in breach of

its GDPR mandate and failing to adequately protect their personal data. We found that more than 70% of those consumers who are likely to take some action (over 39% of the overall population) will take actions such as removing their data and stopping all business with the organization they perceive to be in breach of the GDPR (see Figure 8).

Figure 8. Consumers are likely to take prohibitive action against GDPR offenders.

Will you take action if the organization you are interacting with is not ensuring protection of your personal data?



Source: Capgemini Digital Transformation Institute GDPR Individuals Survey, March–April 2018.

57% of consumers are likely to take action when they find out that an organization is not ensuring data privacy

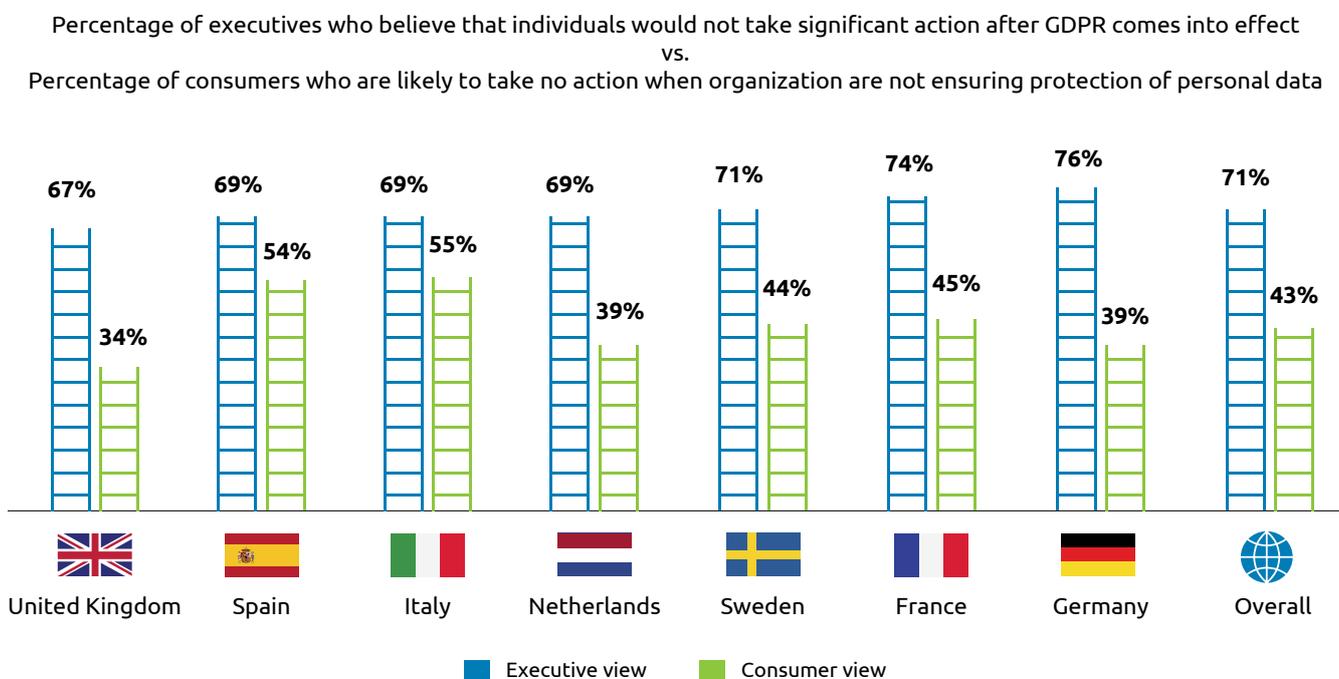
Executives around the world underestimate the extent of consumer activism following GDPR go-live

Overall, 71% of executives believe that consumers will not take significant action around their organization's data privacy and security practices, as Figure 9 shows. *"We haven't seen any substantial increase in consumer interest in matters*

of personal data protection. We don't expect it to change much beyond the GDPR deadline as well, unless there is any event that draws media attention and widespread consumer interest with it," says a senior executive at a large European bank.

However, only 43% of consumers agree that they will likely take no action. If the extent of individual action turns out to be higher than anticipated, a large number of organizations might find themselves underprepared to handle incoming requests related to individual data, further eroding individual trust in organizations' data privacy practices.

Figure 9. Organizations underestimate the extent of individual action.



Source: Capgemini Digital Transformation Institute GDPR Executive and Individuals Survey, March–April 2018.

“

We haven't seen any substantial increase in consumer interest in matters of personal data protection.”

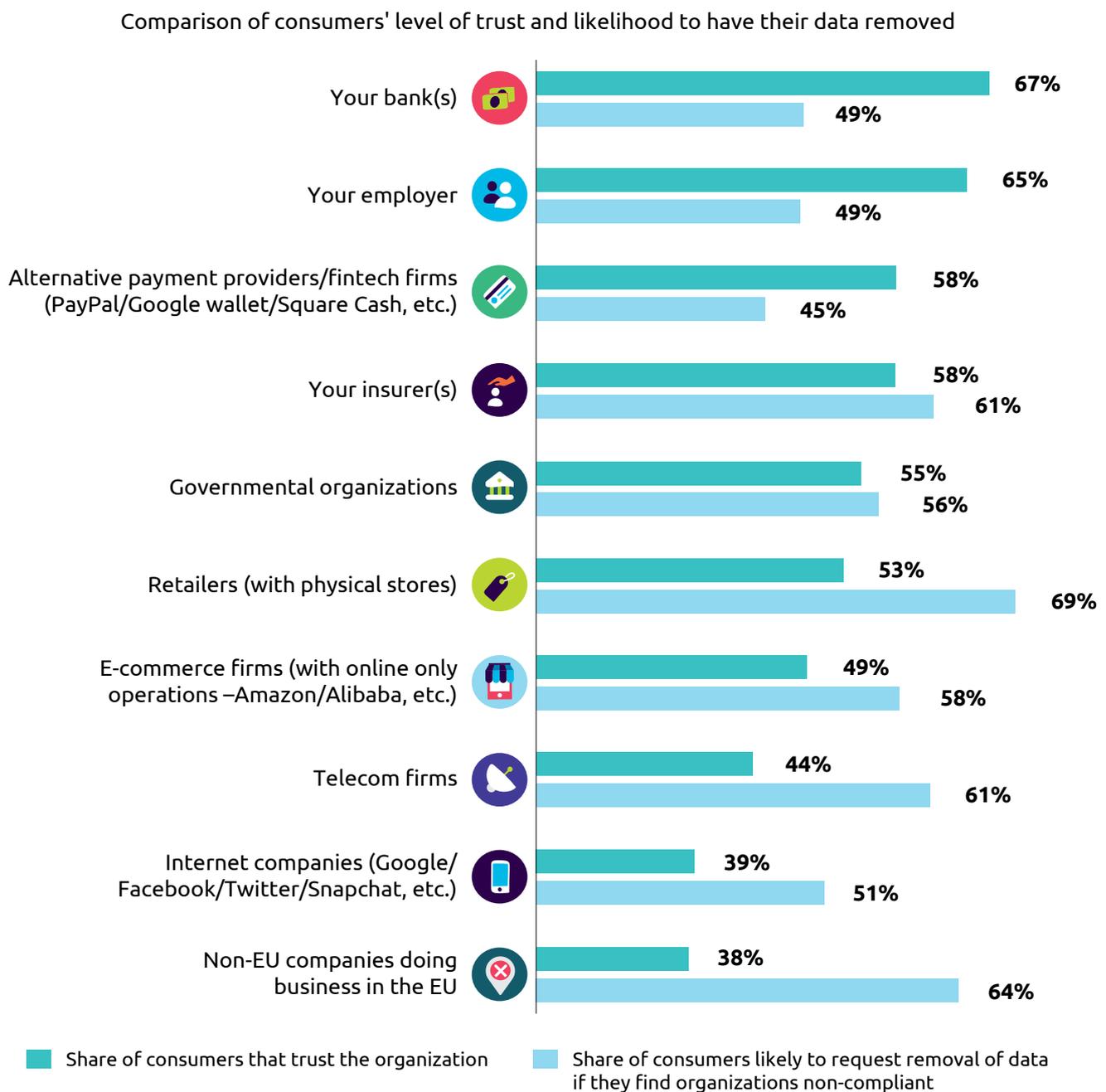
A senior executive at a large European bank.

The action taken will depend on level of trust

Once the GDPR is in effect, organizations that enjoy less trust will receive more individual requests to delete their data. As Figure 10 shows, 64% of consumers are likely to

request non-EU companies to delete their data if they find organizations non-compliant once the GDPR comes into effect, as only about 38% of consumers indicate high levels of trust. But this drops to 49% for banks, which enjoy higher levels of trust.

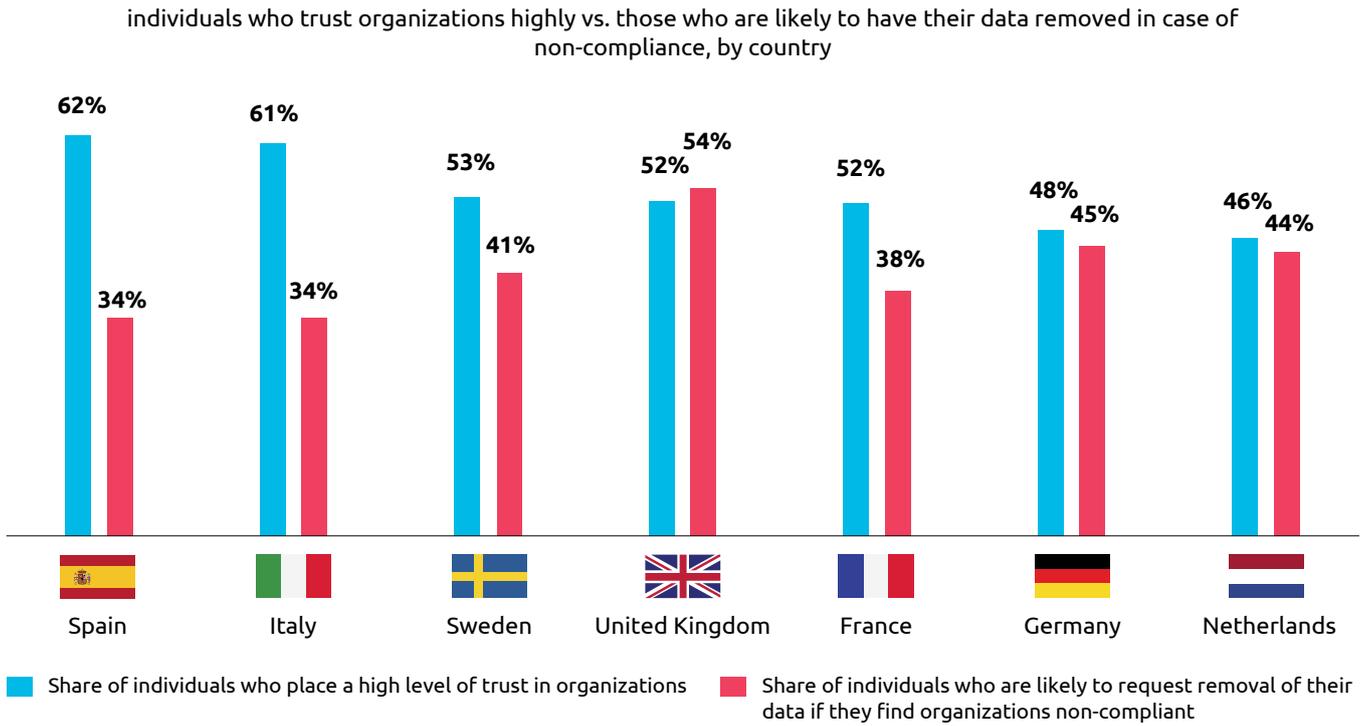
Figure 10. Organizations trusted less by individuals will face more significant action.



Source: Capgemini Digital Transformation Institute GDPR Individuals Survey, March–April 2018.

This trend also holds true at a national level, as Figure 11 shows.

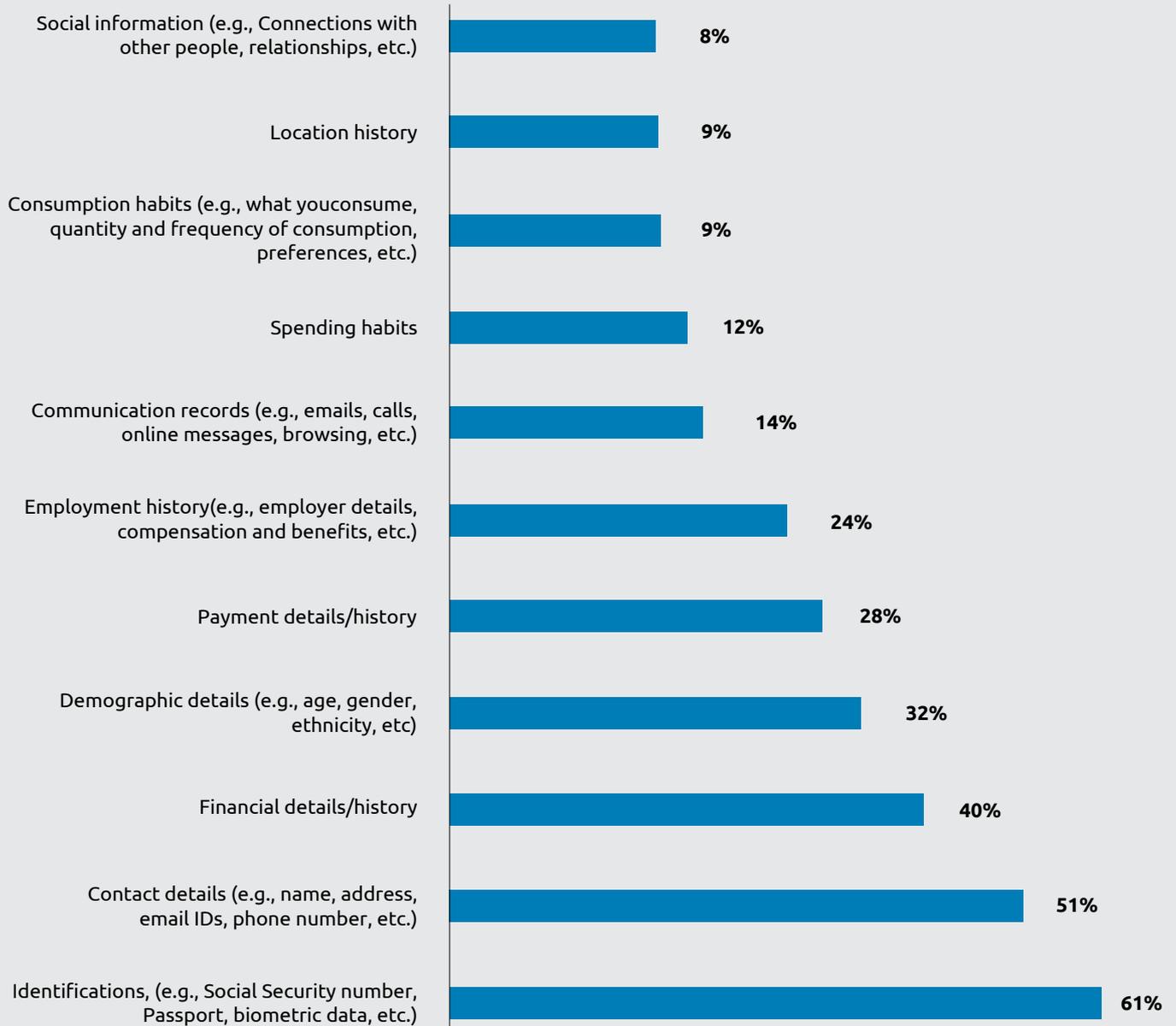
Figure 11. Individuals who trust organizations less are more likely to take action, by country.



Source: Capgemini Digital Transformation Institute GDPR Executive and Individuals Survey, March–April 2018.

Individuals are most sensitive about their identity, contact information, and financial history

Once the GDPR comes into effect, which types of data would you want to have deleted, if you no longer want them to be used by the organization?



Source: Capgemini Digital Transformation Institute GDPR Executive and Individuals Survey, March–April 2018.

What should organizations do to convert the GDPR mandate into an opportunity?



To reap the rewards of the GDPR, organizations must shift their perspective and view the GDPR not just as a compliance mandate, but also as an opportunity to gain competitive advantage and build trust with customers, employees, and citizens. As Figure 12 shows, organizations need to take a

series of external and internal actions. Organizations must accelerate the actions they take with their customer base while rapidly building on a healthy data culture and investing in key technology platforms.

Figure 12. Key actions required to convert the GDPR from mandate to opportunity



Source: Capgemini Digital Transformation Institute Analysis.

Accelerate customer-facing initiatives

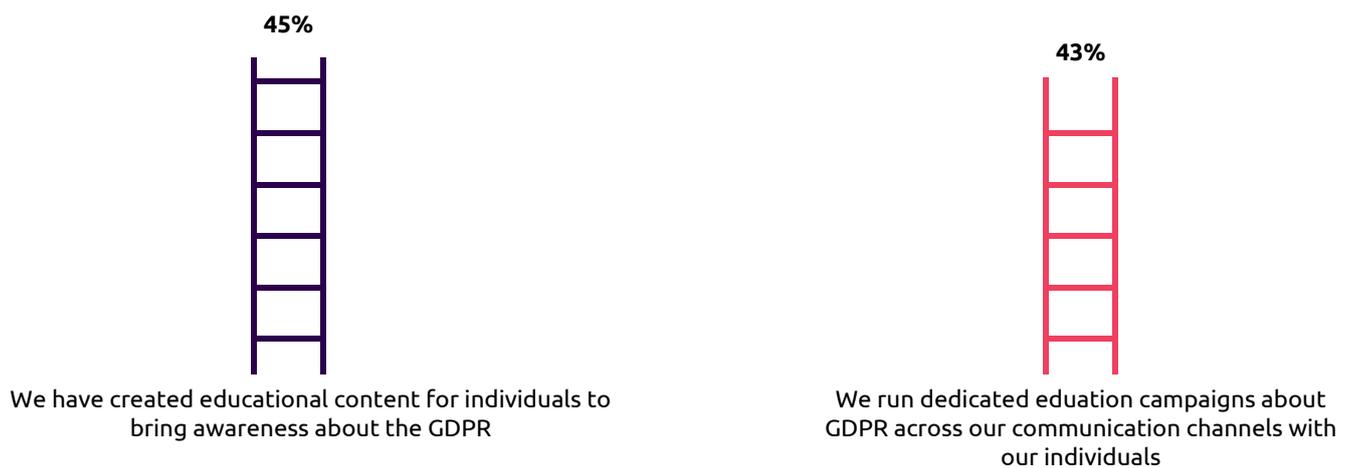
Educate customers and citizens to win their trust

Organizations need to start seeing the GDPR as an opportunity to strengthen trust with customers and citizens. One way to start doing this is to go beyond repurposing existing information and creating basic educational content

and building awareness by running dedicated campaigns with this content. As Figure 13 shows, less than half of organizations have adopted most of these practices. Leading organizations, such as UK retailer John Lewis, put significant efforts into such initiatives. The company worked with a creative agency to help design its communications strategy for the GDPR.⁴ Steve Wright, the company's group data privacy and information security officer, said: *"You're going to need a really good communications program [...] Don't just send people the relevant [GDPR] articles. Create materials they'll understand."*

Figure 13. Leading organizations take consumer and citizen awareness seriously.

To what extent have you taken the following steps to create greater awareness about how your organization's GDPR implementation will impact individuals? (Percentage of executives who regularly do it)



Source: Capgemini Digital Transformation Institute GDPR Executive Survey, March–April 2018.

Organizations can also bolster the trust individuals have in them by demonstrating their commitment to data privacy. Nearly three-quarters (71%) of consumers in our survey said that they are likely to place higher trust in organizations that clearly and visibly demonstrate their commitment to upholding data privacy. The head of regulatory compliance

at a large European insurer echoed the insight: *"We definitely think it can be an advantage if the consumers know that their data is being dealt with in a compliant manner, they would trust us and they would like us more than companies who are not able to show such compliance."*



You're going to need a really good communications program [...] Don't just send people the relevant [GDPR] articles. Create materials they'll understand."

Steve Wright, group data privacy and information security officer, John Lewis

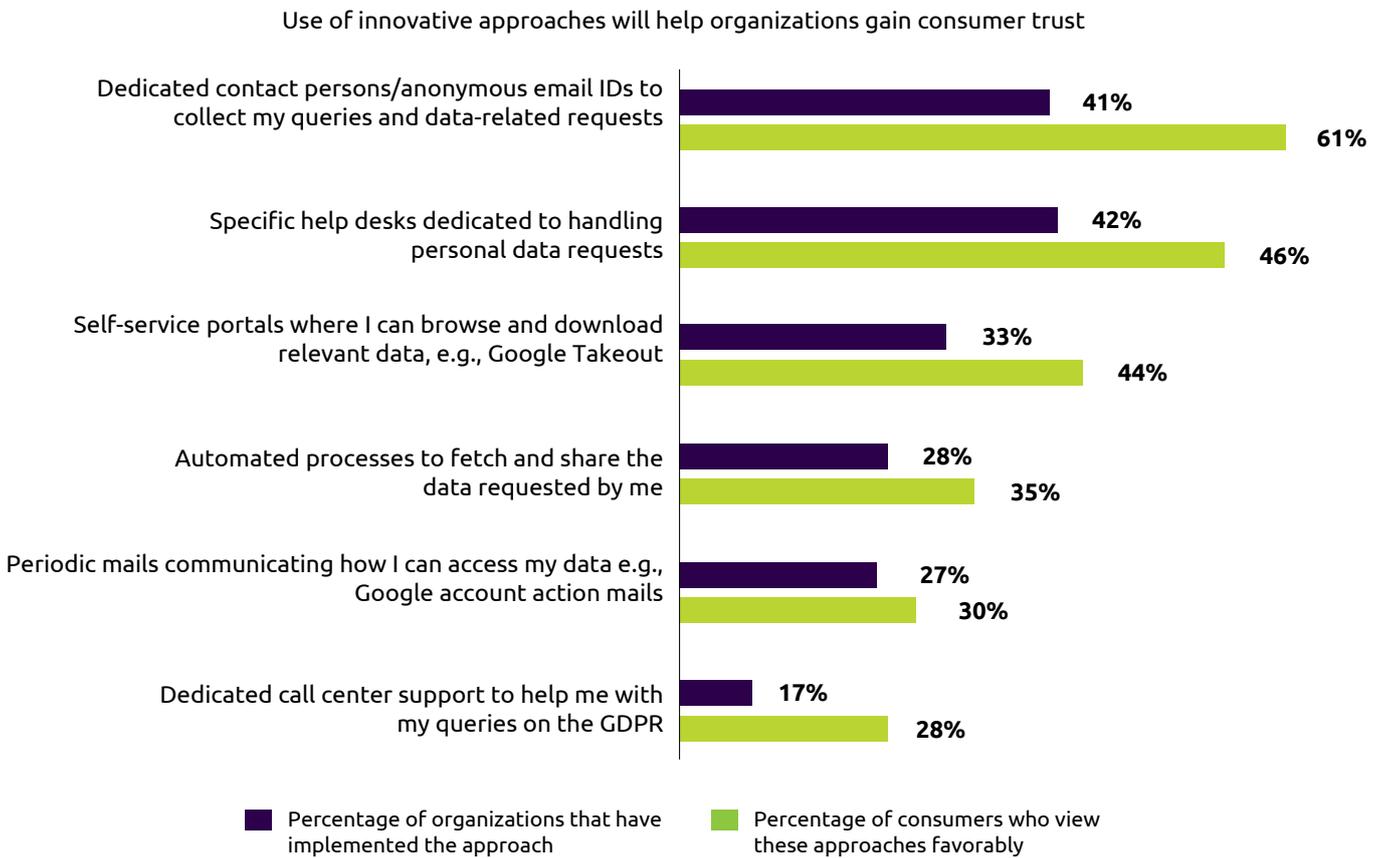
Drive innovation efforts to help individuals exercise greater control over their data

Individuals want organizations to give them simple access to, and control over, data privacy. Although, it is not mandated by the regulatory framework, leading organizations have been adopting innovative approaches to help individuals

exercise more control over their data. In a time of increasing data breaches, individuals see this as a necessity and not the luxury that organizations deem it to be.

As Figure 14 shows, individuals want a range of access vehicles, ranging from data query forms to self-help portals to dedicated call centers. For example, Google Takeout allows users to export and download data from their Google products.

Figure 14. Individuals are looking for innovative approaches to gain control over their data but organizations are lagging.



Source: Capgemini Digital Transformation Institute GDPR Executive and Individuals Survey, March–April 2018.

Identify the Data-Rights Advocates among your customers and convert them into ambassadors

Data Rights Advocates offer significant value if you can meet their expectations. Understanding these individuals better and improving engagement with them leads to positive word of mouth. We found that 60% of these individuals would be willing to share their positive experience of dealing with an organization that protects their personal data with their friends and family.

Organizations need to better understand the profile of this segment and fine tune their marketing and communications approach. This will be key because organizations need to demonstrate high standards of GDPR compliance in order to win over Data Rights Advocates. Organizations can achieve this by showcasing certifications and seals provided by industry associations and consumer rights groups. For example, CNIL in France delivers “privacy seals” that allow users to identify products and processes that assure a high level of protection of personal data.⁵ Organizations would do well to involve them in co-development of their GDPR-related changes. Three in five consumers (61%) in our survey indicated that they highly value being involved by organizations before and during rollout of GDPR-related updates such as providing feedback on privacy and data security measures.

Engage with individuals to understand what matters

A senior GDPR executive at a large online payments company believes individuals’ data privacy expectations have considerably evolved: *“More than ever, individuals are aware of the value their data has for organizations. Therefore, individuals are now much more conscious about the potential abuse of the data if it is not controlled. They believe safeguarding sensitive data is a hygiene factor now and they are looking for more transparency, control, and prevention of abuse of their data.”*

A large banking group in Europe wanted to be more aligned to changing customer expectations and overhauled its CRM strategy to focus more on educating customers on financial matters rather than product marketing. It conducted large-scale research to find out what customers think of the bank’s marketing strategy and how their data is used. As a result of working hand-in-hand with actual customers on this research, the bank got to know what mattered. Although consumers trusted the company with their data, they were looking for more relevant communication and help on topics such as password protection and identity theft. This formed the basis of the group’s new CRM strategy.

60% of Data Rights Advocates would be willing to share their positive experience of dealing with an organization that protects their personal data with their friends and family.

Rapidly Bolster the Enablers

Build a culture of respect for personal data

Several executives we spoke with highlighted the crucial nature of inculcating a culture of respect for personal data among organizational team members. The sensitivity involved in handling personal data must be understood as widely as possible within and beyond organizational boundaries through a concerted effort. As a senior executive at the digital banking arm of a large European bank said: *“We realized early on that employee awareness is the key to data protection in digital banking and have been working toward it*

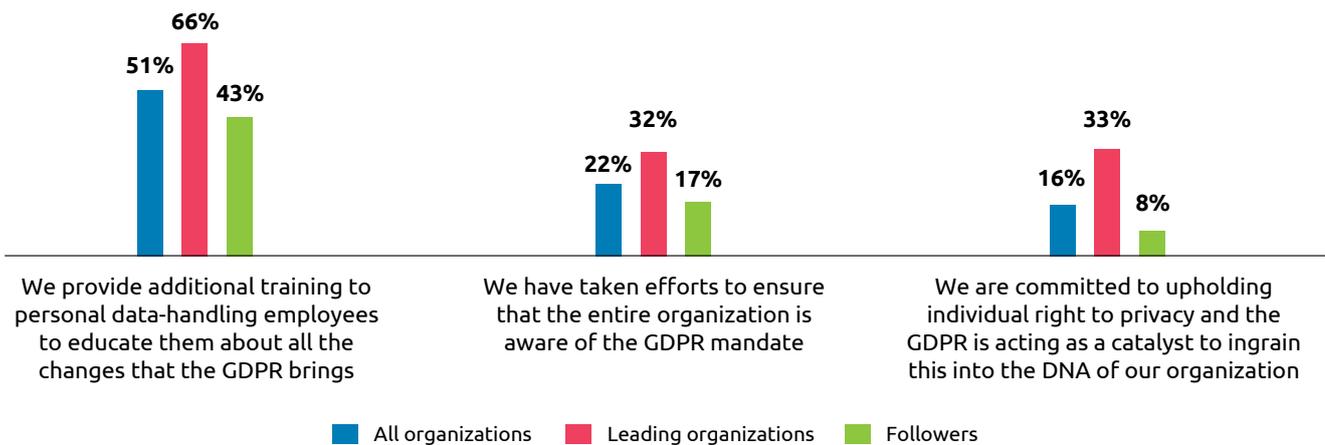
ever since. We have made sure that every employee handling critical data has access to comprehensive documentation and protocols to follow in crisis situations. All our employees undergo mandatory online training that covers technical, legal, and foundational aspects of personal data privacy and security.”

Leading organizations take steps to educate their employees and make data privacy part of their organizational DNA (see Figure 15). We defined leading organizations as organizations:

- That are fully compliant or largely compliant with the GDPR
- That believe the GDPR will help them do the right thing in maintaining privacy and security of personal data.

Figure 15. Leading organizations lead the way in building a culture of respect for personal data.

To what extent have you taken the following steps? (Share of organizations that have implemented these to a great extent)



Source: Capgemini Digital Transformation Institute GDPR Executive Survey, March–April 2018, 341 Leading organizations, 759 followers.

Ensure investments and systems are in place for a smooth GDPR roll-out

Private organizations have stolen a march over public organizations in terms of the core foundations for GDPR

compliance: setting up organization-wide systems and processes and allocating sufficient budgets (see Figure 16). The key foundations of any GDPR program, when done right, they can go a long way in ensuring the success of the initiative.

Two in three (**66%**) leading organizations provide GDPR trainings to personal data-handling employees whereas only **43%** of the other organizations do so

Figure 16. Public organizations need to put in more work on systems and investments to catch up with others.



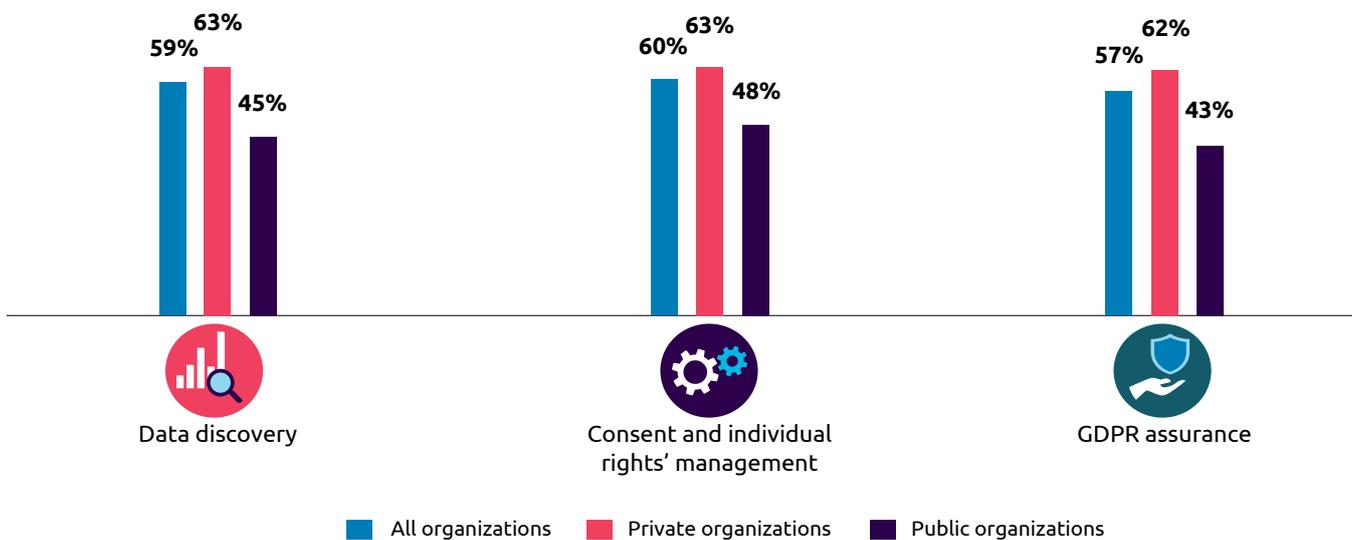
Source: Capgemini Digital Transformation Institute GDPR Executive Survey, March–April 2018.

A large majority of private organizations have implemented key activities related to GDPR compliance (see Figure 17). These include data discovery and consent and individual

rights management. Most government organizations are yet to implement them.

Figure 17. Private organizations have implemented key GDPR activities to a larger extent

How would you rate the level of implementation of your organization with respect to the following activities related to the GDPR? (Share of organizations with a high level of implementation)



Source: Capgemini Digital Transformation Institute GDPR Executive Survey, March–April 2018.

Conclusion

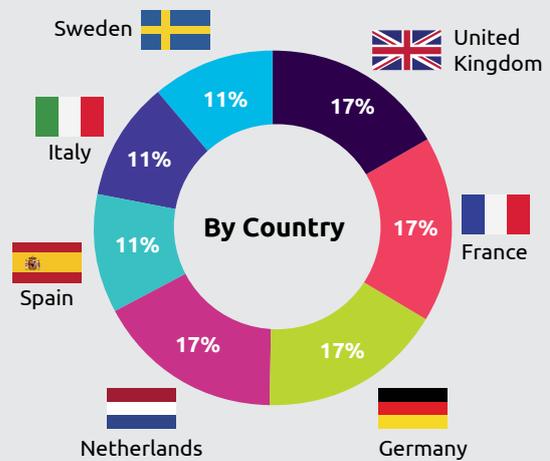
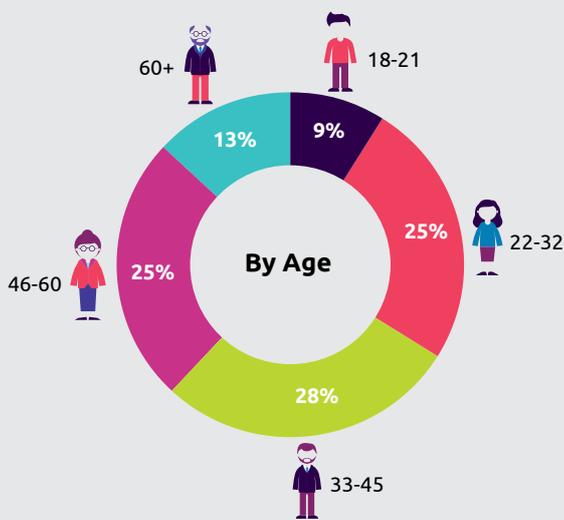
GDPR is an excellent opportunity for organizations to gain consumer trust and competitive advantage. To reap the benefits, organizations now need to weave the key tenets of the GDPR into their organization culture and ensure systems and investments are in place. Working with individuals during this journey will be key to winning their trust and rewards.



Research Methodology

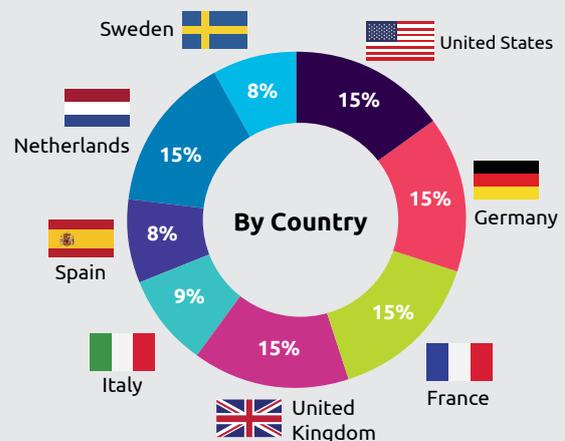
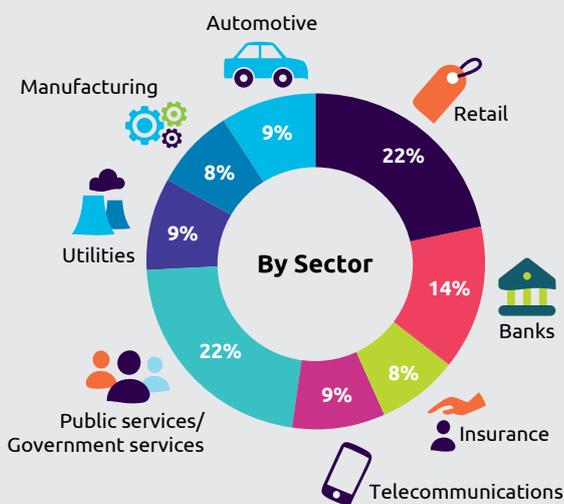
Consumer Survey:

We surveyed 6,000 consumers (aged 18 and above) across seven countries – France, Germany, Italy, Netherlands, the UK, Sweden, and Spain. The survey was conducted in March-April 2018.



Executive Survey:

We surveyed 1,000 executives from organizations spread across eight countries – France, Germany, Italy, Netherlands, the UK, the USA, Sweden, and Spain. The survey was conducted in March-April 2018.



We also conducted in-depth discussions with senior executives from large organizations with more than \$1 billion in annual revenues each.

References

1. Out-Law.com, "Businesses can obtain a 'competitive advantage' if they 'get data protection right,' says watchdog," August 2017.
2. Marketing Week, "Has the data revolution realized its potential?" October 2017.
3. Computerweekly.com, "UBS applies data protection for compliance and competitive advantage," May 2017.
4. Digiday.com, "'Biggest danger is apathy': John Lewis data privacy boss on EU data protection laws," October 2016.
5. Cnil.fr, "Privacy Seals," accessed May 2018.

About the Authors



Willem De Paepe (PhD)

GDPR Global Leader, Capgemini
willem.de.paepe@capgemini.com

Willem is global leader of Capgemini's GDPR Campaign and has held various leadership roles in Capgemini Insights & Data.



Alex Wortmann (PhD)

Executive Vice President, Capgemini Netherlands
alex.wortmann@capgemini.com

Alex is Executive Vice President in Capgemini Insights & Data and Portfolio Manager of the GDPR Campaign.



Pierre-Luc Réfalo

Director Sogeti France
pierre-luc.refalo@sogeti.com

Pierre-Luc is director, Cybersecurity consulting and GDPR services lead at Capgemini. Pierre-Luc is a published author, trainer in Masters degrees and a regularly speaks at international events.



Jerome Buvat

Global Head of Research and Head,
Capgemini Digital Transformation Institute
jerome.buvat@capgemini.com

Jerome is head of Capgemini's Digital Transformation Institute. He works closely with industry leaders and academics to help organizations understand the nature and impact of digital disruptions.



Subrahmanyam KVJ

Program Manager, Digital Transformation Institute
subrahmanyam.kvj@capgemini.com

Subrahmanyam is a senior manager at the Digital Transformation Institute. He loves exploring the impact of technology on business and consumer behaviour across industries in a world being eaten " by software.



Amol Khadikar

Manager, Capgemini Digital Transformation Institute
amol.khadikar@capgemini.com

Amol is a manager at the Digital Transformation Institute. He keenly follows the role played by mobile, software and data science in digitally transforming organizations.



Yashwardhan Khemka

Senior Consultant,
Capgemini Digital Transformation Institute
yashwardhan.khemka@capgemini.com

Yash is a senior consultant at the Digital Transformation Institute. He likes to follow disruption fueled by technology across sectors.

The authors would like to especially thank Aritra Ghosh and Amrita Sengupta from Capgemini Digital Transformation Institute for their contribution to this report.

The authors would also like to thank Laveena Gandhani and Abhyuday Dixit from Capgemini Consulting India, Mieke Van Handenhove from Capgemini Group Marketing, Philippe Kerael from Capgemini France, Graham Hunt and Lee Smith from Capgemini UK, Ron Tolido from Capgemini Netherlands, Balaji Palanidurai from Capgemini India, Fabio Tinetti from Capgemini Italy, and Javier Checa Bermejo and Alejandro Moreno San Vidal from Capgemini Spain.

Digital Transformation Institute



The Digital Transformation 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 the United Kingdom, United States and India.

dti.in@capgemini.com

For more information, please contact:

Global

Willem De Paepe

willem.de.paepe@capgemini.com

Pierre-Luc Réfalo

pierre-luc.refalo@sogeti.com

Isabelle Budor

isabelle.budor@capgemini.com

Alex Wortmann

alex.wortmann@capgemini.com

Philippe Kerael

philippe.kerael@capgemini.com

France

Pierre-Luc Réfalo

pierre-luc.refalo@sogeti.com

United Kingdom

Lee Smith

lee.c.smith@capgemini.com

DACH

Christian Kaupa

christian.kaupa@capgemini.com

Netherlands

Martijn Tack

martijn.tack@capgemini.com

North America

Philip Higginbotham

philip.higginbotham@capgemini.com

Norway

Tor-Ståle Hansen

tor-stale.hansen@capgemini.com

Sweden

Mark Battersby

mark.battersby@capgemini.com

India

Balaji Palanidurai

balaji.palanidurai@capgemini.com

Portugal

Carlos Vidinha

carlos.vidinha@capgemini.com

Spain

Victor Martin Robles

victor.martin-robles@capgemini.com

Belgium

Alexander Vandeneede

alexander.vandeneede@capgemini.com

Australia

Surinder Pal Singh

surinder.p.singh@capgemini.com

Italy

Fabio Tinetti

fabio.tinetti@capgemini.com

FS

Graham Hunt

graham.hunt@capgemini.com

Take full advantage of the unavoidable opportunity with Capgemini's GDPR services

Whatever stage of the journey you're at, we can implement practical solutions to help you meet compliance and use data more strategically to benefit from the many opportunities the GDPR 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 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 moving you towards GDPR compliance and helping you take advantage of the opportunity, is built around the comprehensive portfolio of modular and scalable services below. If you're not quite ready yet, we can accelerate your GDPR journey. 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, GDPR awareness and integrates all internal and external teams.

Program Services: Designs the program to get you moving towards GDPR compliance and allows you to adapt and customize GDPR 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 the GDPR, such as responding to access requests

Data lifecycle services: The GDPR requires organizations to only use as much data as is required to successfully complete a given task. It cannot be reused for another task 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

Discover more about our recent research on digital transformation



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



[Automotive Smart Factories: Putting automotive manufacturers in the digital industrial revolution driving seat](#)



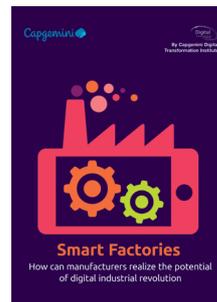
[Unlocking the business value of IoT in operations](#)



[Digital Transformation Review 11: Artificial Intelligence Decoded](#)



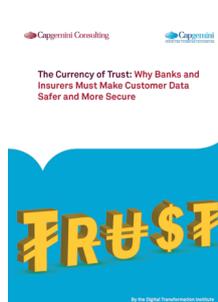
[Turning AI into concrete value: the successful implementers' toolkit](#)



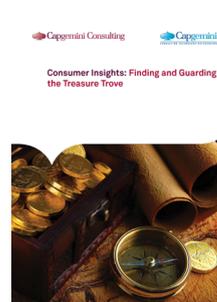
[Smart Factories: How can manufacturers realize the potential of digital industrial revolution](#)



[The Digital Culture Challenge: Closing the Employee-Leadership Gap](#)



[The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure](#)



[Consumer Insights: Finding and Guarding the Treasure Trove](#)



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 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

Visit us at

www.capgemini.com

People matter, results count.

The information contained in this document is proprietary. ©2018 Capgemini.
All rights reserved.