The end of the beginning

Unleashing the transformational power of GDPR

IBM Institute for Business Value

In this report

Executives assess their readiness to comply with GDPR

A leader group we call the "Sparked" sees GDPR preparedness as a business differentiator enabling transformational opportunities

Recommendations for organizations in every phase of their GDPR compliance activities

How IBM can help

IBM Security tackles the world's most challenging security problems. We continually look for new and better ways to protect the faces behind the data — your customers. Our strategy reflects the belief that today's defenses will not suffice tomorrow. It challenges us to approach our work, support our clients and lead the industry with forward-thinking solutions that leverage cloud, AI, orchestration and collaboration.

To get the latest GDPR insights from IBM Security, please visit ibm.biz/PrepareForGDPR. To learn about IBM's GDPR capabilities, from data discovery to unified governance visit ibm.com/gdpr.

A catalyst for change

It is said that innovation and creativity can flourish under intense pressure and constraint – GDPR compliance could present organizations with this type of opportunity. For most, preparations are still in motion, but as we move past the compliance date, a new phase begins. One critical question: can organizations turn a compliance challenge into an occasion to advance their digital efforts? Our research has identified a small group of leaders who say they will be fully compliant with GDPR by the enforcement date and view it as a catalyst for change. This report explores how they are approaching security, privacy, data and analytics, and customer engagement, and how their efforts could drive future success.

The next chapter

Amid a growing global conversation about security, privacy, and choice and control regarding data, the European Union's General Data Protection Regulation (GDPR) is entering its enforcement phase (see sidebar, "What is GDPR?"). Over the years, privacy and security are issues that have moved from back rooms to board rooms and now to dining rooms around the world. Both the threats and responsibilities are greater, as are the potential effects on business and society.

GDPR is significantly impacting organizations and individuals alike – granting data subjects new rights and posing new regulatory challenges for businesses. During the last few years as organizations have been preparing for GDPR, they have been tested by both the effort involved and the cost of compliance. It is estimated that some organizations have spent more than USD 1 million to become GDPR compliant.[1] However, real costs are difficult to estimate since they are often spread across many departments, and actions can leverage existing tools and processes. Organizations have been busy changing processes and developing new ones, creating new roles and building new relationships, training employees, and deploying new tools and technologies.

GDPR is a reality, turning the management of privacy issues, data rights and security breaches into standard business practices. Such transformation triggers a consequential question: *Can organizations turn a compliance challenge into an impetus for broader transformation?*

Only 36%

of surveyed executives say they will be fully compliant with GDPR by the enforcement date

59%

of respondents see GDPR as an occasion for transformation or a spark for new data-led business models

We identified

a group of leaders who see GDPR as a catalyst for longer-term transformation. Compared to the rest of our study sample, 6X as many GDPR leaders report very strong internal collaboration

96%

of GDPR leaders agree that proof of compliance with GDPR will be viewed as a positive differentiator by the public

What is GDPR?[2]

Approved in April 2016, the European Union (EU) General Data Protection Regulation (GDPR) replaces the minimum standards of the Data Protection Directive. Organizations face new, uniform data protection requirements relating to the information of EU subjects.[3] Potential administrative fines can total up to EUR 20 million or up to 4 percent of total worldwide annual turnover/revenue for the preceding financial year, whichever is higher.

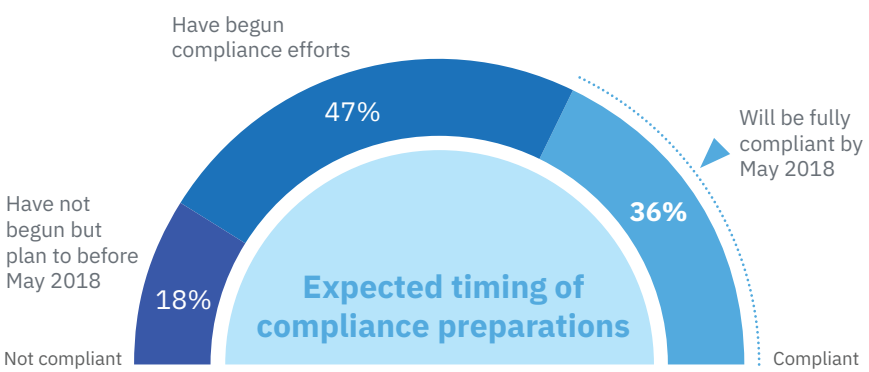
At minimum, the regulation demands:

- Data protection accountability.
- Data subjects' consent, right to access, rectification, erasure and portability.
- Data breach notification.

GDPR – bane or boon?

To test this question, between February and April 2018 we surveyed 1,500 executives responsible for their organizations' GDPR preparations across 15 industries around the world (for more information, see "Demographics and methodology" section). Looking across the entire sample, we discovered interesting insights about the general approach organizations were taking, as well as their overall levels of preparedness. For many, GDPR preparations are still in motion – only 36 percent of respondents told us they will be fully compliant by the enforcement date (see Figure 1).

Figure 1
Preparations for GDPR



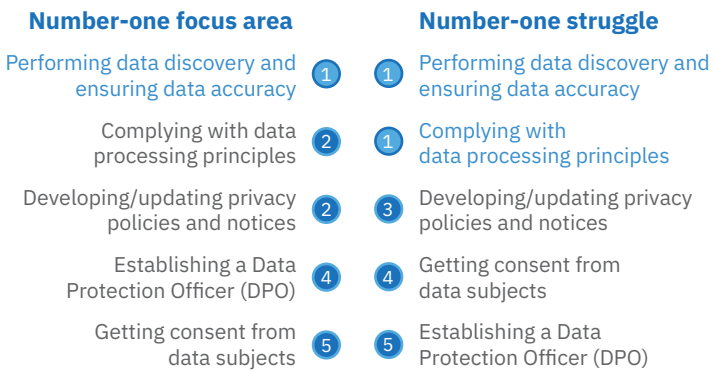
Why are people waiting until the last minute, essentially cramming for a test? There could be many reasons, including a lack of commitment from organizational leadership or a desire to take a wait-and-see approach. It could also be a resource issue or maybe a sense that preparations would disrupt business operations too much.

There is some good news in our respondents' overall view of GDPR. Only 36 percent of respondents regard GDPR as simply a mandatory regulation. The majority had a positive view on the potential of the regulation and what it could do for their organizations. Thirty-nine percent saw GDPR as a chance a transform their security, privacy and data management efforts, and 20 percent said it could be a catalyst for new data-led business models. This could mean that many organizations have finally accepted the regulation as reality and are now looking for ways to benefit from the mandate.

The bad news is, despite focus and effort, overall preparedness is only moderate. What respondents say they are focused on, they are also struggling with. We asked respondents to look at 11 different GDPR-related components and tell us which they were focusing on, which they were struggling with and how prepared they were (see sidebar, "Components of GDPR tested"). One of the principal tasks of GDPR preparation, performing data discovery and ensuring data accuracy, was the component that most of the sample ranked as their number-one focus area. Most of the sample also ranked it as their number-one struggle (tied with complying with data processing principles). In fact, the top five preparation areas were also the top five areas of struggle (see Figure 2).

We can look at it two ways. Perhaps what they are struggling with is what they are putting more effort toward. Or, what they are putting effort toward, they are also struggling with. Either way, the results of their efforts aren't paying off quickly enough. The top two areas of preparedness were performing data discovery and ensuring data accuracy (60 percent

Figure 2
Priorities and struggles in preparation



said they were prepared), and implementing data subject rights, procedures and controls (58 percent said they were prepared). The components with the lowest level of preparedness were getting consent from data subjects (48 percent) and handling cross-border data transfers (47 percent).

Along with their struggles, respondents are also facing several uncertainties and concerns related to GDPR. The top uncertainties for respondents covered both the theoretical and practical – 44 percent worried that GDPR could be modified or replaced in the near future, and 43 percent worried about how much GDPR preparation would cost their organizations. There were also concerns when it came to things like confirming security controls at data processors and how organizations would fulfill an increased number of data access requests.

The "GDPR-erequisites" – Components tested

Data

- Complying with data-processing principles
- Performing data discovery and ensuring data accuracy
- Managing the relationship between data controllers and data processors
- Handling cross-border data transfers

Security

- Enhancing security capabilities
- Improving data incident/breach notifications and response practices

Data subjects

- Getting consent from data subjects
- Developing/updating privacy policy and notices
- Implementing data subject rights procedures and controls

Organizational

- Establishing a Data Protection Officer (DPO)
- Promoting accountability measures

Figure 3
Using GDPR preparations to move beyond compliance

- A strong overall digital strategy and improved cross-organizational collaboration
- Better security through upgraded incident response
- Strong security and privacy, and closer customer relationships as competitive differentiators
- New avenues for data-led business models
- New ways to operate with a streamlined approach to data management

Charging up for the future

To justify the large amount of effort and resource invested in GDPR preparation, organizations want to get something more out of it than simple compliance. We can look to a group of leaders that is taking a mature approach to security and privacy, data and analytics, and customer engagement to propel themselves forward. Taking a comprehensive and holistic approach to GDPR preparations can potentially improve a number of factors in the longer term, including: better cross-organizational collaboration, streamlined operations and data management, improved security and closer customer relationships (see Figure 3).

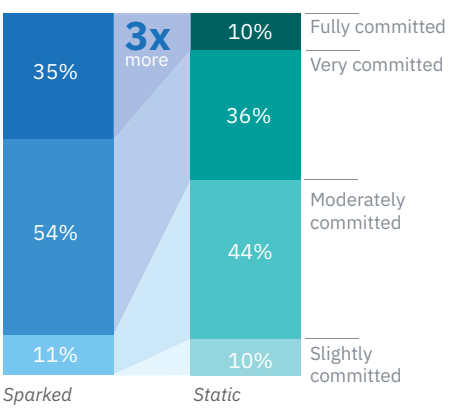
To understand which organizations are best taking advantage of the opportunity, we applied a set of criteria across the sample to identify a leader group. The GDPR leaders who met the criteria comprised 22 percent of our sample – we call them the "Sparked," signifying that these organizations were motivated by their GDPR preparations. The rest of sample, the "Squeezed," are more constrained and less committed, which may be preventing them from realizing their potential. The Sparked:

– State that they will be fully compliant with GDPR by the enforcement date in May 2018
– See GDPR as a chance to transform their privacy, security, and data management efforts, or as a catalyst to create new data-led business models
– View GDPR as an opportunity to reexamine, and improve their security practices and operations
– Say GDPR preparation is enabling them to develop data strategies that will improve their business functions
– Anticipate that GDPR will strengthen relationships with customers/clients.

It is worth noting that Sparked organizations had higher annual revenue – 41 percent of the Sparked were from organizations with an annual revenue of more than USD 5 billion, compared to only 13 percent of the Squeezed.

What makes this group different and what can we learn from how they see GDPR enabling them in the future? First, the Sparked have a greater level of organizational commitment to the process (see Figure 4). Over three times as many of the Sparked than the Squeezed said their organizations were fully committed to comply with the depth and breadth of GDPR. In fact, 89 percent of the Sparked had a high level of commitment.

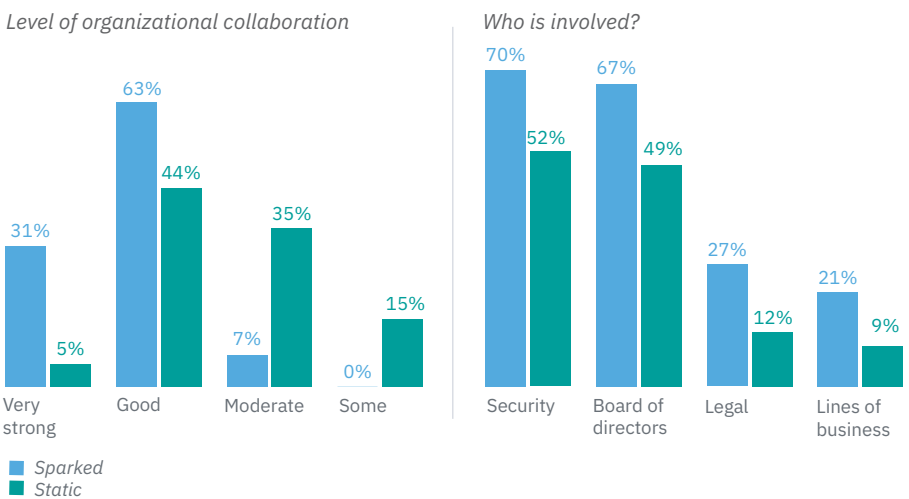
Figure 4
Commitment to providing needed resources and attention



By contrast, those whose organizations were only slightly committed identified several primary barriers to commitment, including a lack of funding, and GDPR being viewed as just a compliance issue or as interfering with their business models.

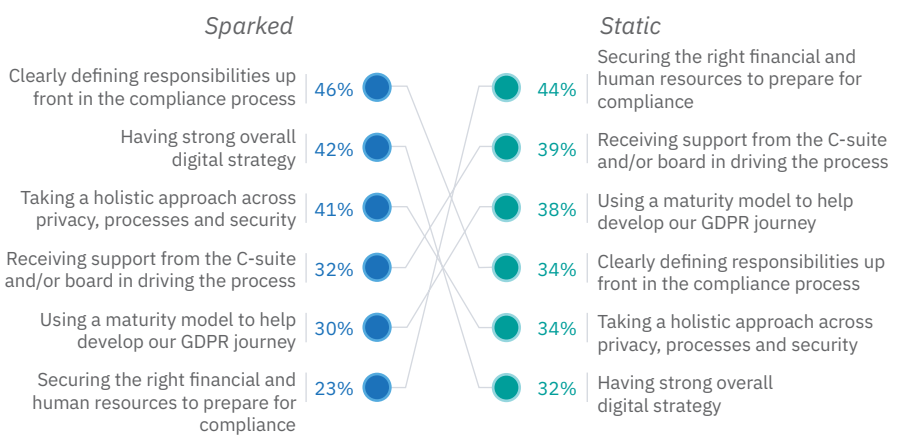
The Sparked also have a higher level of organizational collaboration and they involve other members of their organizations in preparations at a higher rate (see Figure 5). Ninety-four percent of the Sparked report good collaboration (compared to 49 percent of the Squeezed). The Sparked also involve security, their boards of directors, legal departments and lines of business at a greater rate as well, among other enterprise roles.

Figure 5
Organizational collaboration and involvement



What did respondents consider critical to their preparation for GDPR? The Sparked see a broad, strategic approach as key; the rest of the Squeezed were more focused on tactical measures (see Figure 6). The Sparked credited clearly defining responsibilities up front, a strong overall digital strategy and a holistic approach as benefiting them the most. By contrast, the Squeezed had an entirely different set of top enablers: getting the right financial and human resources, receiving top-level executive and board support, and utilizing maturity models or roadmaps.

Figure 6
Top enablers for preparation



As noted earlier, the total sample was only moderately prepared across eleven different components of GDPR preparation. More of the Sparked were prepared across every aspect than the Squeezed in all major areas: data preparedness, security preparedness and data subject preparedness. For example, 79 percent of the Sparked said they were prepared for performing data discovery and ensuring data accuracy, compared to 55 percent of the Squeezed.

This group was also far ahead of others in managing the relationship between data controllers and data processors, handling cross-border data transfers and complying with data-processing principles. In addition, more than two-thirds of them had enhanced security capabilities and improved data incident/breach notifications and response practices. The Sparked were also well ahead of others in getting consent from data subjects and implementing data subject rights procedures and controls.

It is worth noting that even the Sparked have some areas to work on. Only 57 percent of the Sparked said they were prepared for developing and updating privacy policy and notices.

How can all their hard work today enable organizations to realize new value tomorrow through their approaches to security and privacy, data and analytics, and customer engagement?

Sharpening security approaches

GDPR has a number of different security-specific requirements regarding breach notification, data protection and accountability. Ideally, these measures will "lift all boats" when it comes to cybersecurity awareness and preparedness. Our analysis showed that 83 percent of the Sparked see security and privacy as key business differentiators and sources of competitive advantage, compared to just 65 percent of other respondents. Most of the entire sample have modified how they handle incident response because of GDPR (93 percent of the Sparked versus 70 percent of the Squeezed).

A key to longer-term success, seeing security and privacy as key business differentiators and sources of competitive advantage, is also an area of agreement for a vast majority of the Sparked. Finally, roughly three-quarters of the Sparked report that they have fully implemented privacy and security by design for their new products and services. In contrast, less than half of the Squeezed have. By making a leading practice mandatory, GDPR is putting a focus on this important topic that will, optimistically, improve security for all.

To understand how organizations are improving their approaches to incident response and breach notification (as outlined in Article 33 of GDPR) we posed several questions.[4] We found that the majority of the Sparked are engaging their leadership more, practicing their response capabilities and enhancing communications – although, even the leaders could use improvement in these areas. More of the Sparked said they have created new responsibilities for executives related to incident response (63 percent versus 37 percent), run incident response simulations with executives (58 percent versus 38 percent), and built new processes and policies to notify data subjects (53 percent versus 49 percent). As the cybersecurity threat landscape becomes more complex and challenging, improving these practices is essential. Organizations need the confidence to exercise leadership and quick thinking when a security crisis occurs, or risk losing control of an incident response.[5]

Invigorating data strategies

Data is at the core of GDPR – how it is requested, provided, shared, processed and utilized. Most everyone says they are making improvements to their data strategies because of their preparations for GDPR, with the Sparked doing so to a slightly greater extent. A large majority of our respondents have unified their data strategies to improve performance and efficiency (97 percent of the Sparked versus 84 percent of the Squeezed). Most respondents also report that they are treating all their data the same, whether it is from data subjects in the European Union or not (79 percent of the Sparked versus 66 percent of others).

A significant portion of the respondents view GDPR as a chance to streamline their data management approaches. Eighty percent of the sample are cutting down on the amount of personal data they keep, 78 percent are reducing the number of people who have access to personal data and 70 percent are disposing of data that is no longer needed. This “clean-up” process is setting up organizations for longer-term efficiency.

We wanted to understand how GDPR was impacting business models, products and services reliant on data. The Sparked have greater confidence that GDPR will help in the long run – creating new data-led prospects. Almost 30 percent said that GDPR will create new opportunities for data-led business models and data monetization efforts, compared to only 10 percent of the Squeezed. With permission, and following the tenets of GDPR, organizations have the opportunity to create more personalized products and services – fostering deeper relationships with their customers and clients.

Data controllers and data processors must be intimately in sync

The relationship between data controllers and data processors is a critical one that shouldn't be discounted. It is not only critical for compliance, but critical to business' data protection. A data controller determines the means of processing personal data, and the data processor processes personal data on behalf of the controller. This relationship is important for many reasons, the chief one being that under GDPR, controllers and processors must be brought up to the same level of responsibility and duty. Data controllers can't simply outsource their responsibility.

Very few of our entire sample ranked managing the relationship between data controllers and data processors as a key focus area – only 5 percent ranked it as their number one. Like many other areas, the Sparked expressed that they are better prepared for this component (76 percent versus 47 percent for all others).
All surveyed organizations cited challenges with the relationship that need to be addressed. The top concerns included ensuring security (57 percent), developing joint procedures (56 percent) and communication with data processors (51 percent).

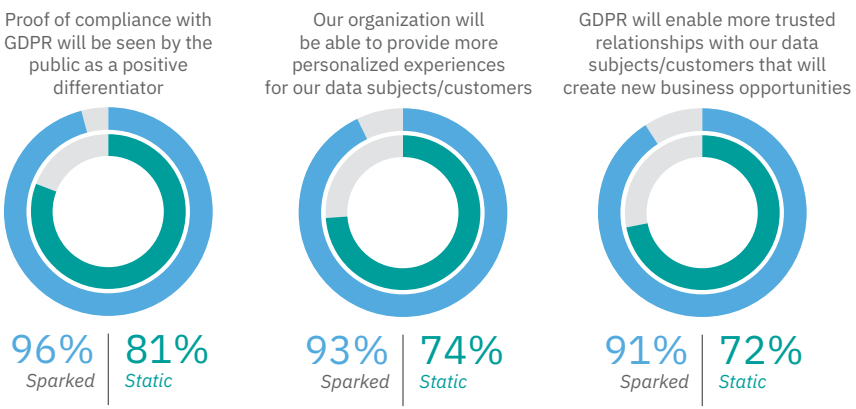
Developing and maintaining transparency and accountability between processors and controllers is not only right for data subjects, but could reduce costs and risk, and improve overall trust in the long run.

Empowering relationships

Earlier, we stated that the majority of respondents held a positive view on the potential of the GDPR and what it could do for their organization (versus just being a compliance challenge). Nowhere is this more evident or important than in how relationships with data subjects could potentially change. In a recent global online survey conducted by The Harris Poll for IBM, they found that 75 percent (of over 8,500 respondents) agreed that if they didn't trust a company to protect their data, they wouldn't buy from them, no matter how great their products were.[6]

The vast majority of those surveyed agree that GDPR will improve their interactions with data subjects and unlock new business opportunities. Over 90 percent of the Sparked agree that proof of compliance will be seen as a positive differentiator, they will be able to create more personalized experiences for data subjects, and that GDPR will enable more trusted relationships and new business opportunities (see Figure 7). Building mutual trust with data subjects through transparency and clear communication is expected to unleash opportunity for organizations that can best take advantage of enhanced reciprocity.

Figure 7
Changes to relationships



Sparking a new beginning

We have crossed a threshold and entered a new era for data, security, privacy and digital customer interactions. While your organization may not have completed all GDPR compliance activities by the enforcement deadline, it is vital to establish efforts to address every aspect with a project plan or other type of roadmap. Those who are prepared may now ask themselves how GDPR can help position them for success by unlocking new opportunities.

No matter how the future unfolds, organizations in every phase of compliance should do a few things to set themselves up for both near- and longer-term success.

Collaboration and commitment are essential for effective preparation and enable you to tackle future challenges:

- Take a holistic approach across privacy, governance, people, processes, data and security
- Expand beyond the “usual suspects” (for example, security, privacy and legal), and involve a broader core team into your preparations – make sure to include lines of business, HR and all groups that touch personal information
- Make everyone accountable for enabling rapid responses to answer inquiries, defend personal data and conduct data processing activities for any regulatory request or investigation
- Look for opportunities to leverage the broader team that you have established for GDPR – including developing new data-led business strategies and products/services.

Advance and leverage your incident response capabilities, building on what you have already started for GDPR:

- Clearly define individual responsibilities for incident response and work to create new responsibilities for key executives, supporting them with pertinent training
- Run incident response simulations and practice sessions with all involved executives and teams
- With the foundations for GDPR established, make "security and privacy by design" priority going forward
- Continue to look for ways to advance security and privacy as key business differentiators and sources of competitive advantage.

Smaller organizations and those challenged by resource constraints should still build a foundation for transformation:

- No matter the level of support or amount of resources you have, understand your data and document related processes – focus your efforts on data mapping and security controls
- Continue to focus on developing awareness and educating key executives, and as enforcement begins, use news stories to start a conversation and spur action
- If you can't invest in new security and privacy tools, look for innovative ways to enhance what you currently have
- Look for opportunities to link to broader digital transformation efforts in your organization.

Demographics and methodology

To better understand how organizations were preparing for GDPR and potentially using it as a transformational opportunity, the IBM Institute for Business Value (IBV) and Oxford Economics surveyed 1,500 GDPR leaders in 34 countries, representing 15 industries between February and April of 2018.

We surveyed Chief Privacy Officers, Chief Data Officers, General Counsels, Chief Information Security Officers and Data Protection Officers. To determine our GDPR leader group, we classified respondents using specific criteria (how they answered a select set of questions) and the GDPR leaders who met the criteria comprised 22 percent of the total sample.

Related IBM publications

"IBM Cybersecurity and Privacy Research." The Harris Poll. April 13, 2018. http://newsroom.ibm.com/2018-04-16-New-Survey-Finds-Deep-Consumer-Anxiety-over-Data-Privacy-and-Security

Kelley, Diana, Vijay Dheap, David Jarvis and Carl Nordman. "Cybersecurity in the cognitive era: Priming your digital immune system." IBM Institute for Business Value. November 2016. https://www-935.ibm.com/services/us/gbs/thoughtleadership/cyberimmunity/

Barlow, Caleb, Christopher Crummey and David Jarvis. "Beyond the boom: Improving decision making in a security crisis." IBM Institute for Business Value. January 2018. https://www-935.ibm.com/services/us/gbs/thoughtleadership/beyondboom/

How can you energize your efforts related to GDPR?

If you are already prepared for GDPR, how can you further advance your digital efforts? If you aren't prepared, how can you urge action within your organization to prepare for both the short and long-term simultaneously?

How are you using your security and privacy efforts to protect your organization, data processors and data subjects from threats? How can you involve your executive team in incident response at a deeper level?

What can you do to enact a streamlined approach toward personal data to create new data-led business opportunities, as well as more personalized products and services?

With GDPR compliance seen as a positive differentiator by the public, how can you empower your organization to build closer relationships with customers and clients?

Going forward, what will be needed to drive a cultural shift that enables both your GDPR and digital transformation efforts concurrently? How can you enable your organization to emphasize security, respect privacy, and responsibly nurture more intimate relationships with customers and clients?

About the authors

Cindy Compert, CIPT/CIPM, is a Distinguished Engineer and the Security CTO, US Public Sector Market, CTO Data Security and Privacy, IBM Security. Cindy is a technical visionary driven by wanting to make a difference around the world, advancing the health, safety and well-being of others. Cindy invented the IBM Security GDPR Framework and is leading IBM Security's GDPR solution strategy across the company. Cindy can be reached on Twitter @CCBigData and at cindycompert@us.ibm.com.

Richard Hogg is the Global GDPR Evangelist at IBM. He has worked over the last three years with heavily regulated organizations on their GDPR journeys. He is responsible for cross-IBM GDPR capabilities and solutions. He is part of the IBM internal GDPR Readiness Program, and a frequent global speaker on GDPR and information governance. Richard can be reached on LinkedIn at linkedin.com/in/rhogg, via Twitter @banjaxx and at rghogg@us.ibm.com.

For more information

To learn more about this IBM Institute for Business Value study, please contact us at iibv@us.ibm.com. Follow @IBMIBV on Twitter, and for a full catalog of our research or to subscribe to our newsletter, visit: **ibm.com**/iibv.

Access IBM Institute for Business Value executive reports on your mobile device by downloading the free "IBM IBV" apps for phone or tablet from your app store.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value

The IBM Institute for Business Value (IBV), part of IBM Services, develops fact-based, strategic insights for senior business executives on critical public and private sector issues.

Contributors

David Chapin, Senior Managing Consultant, Security and Privacy, IBM Security

Jayne Golding, Executive Consultant, European Privacy Lead, IBM Security

Adam Nelson, Associate Partner, Global Privacy Leader, IBM Security

Gant Redmon, Program Director, Cyber Security and Privacy, IBM Security

Lisa Van Deth, Campaign and Thought Leadership Strategy Manager, IBM Security

John Zorabedian, CISO Marketing Manager, IBM Security

Notes and sources

1 Sheridan, Kelly. “Businesses Calculate Cost of GDPR as Deadline Looms.” DarkReading.com. April 12, 2018. https://www.darkreading.com/risk/businesses-calculate-cost-of-gdpr-as-deadline-looms/d/d-id/1331527?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple

2 EUR-Lex: Access to European Union law. Document 32016R0679. Summary of legislation – “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).” http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679

3 “The GDPR: It’s coming – and sooner than you think. Are you prepared?” IBM Security thought leadership white paper. December 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGW03247USEN&&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US

4 EUR-Lex: Access to European Union law. Document 32016R0679. Summary of legislation – “REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL – Article 33, Notification of a personal data breach to the supervisory authority.” https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

5 Barlow, Caleb and Christopher Crummey. “Beyond the boom: Improving decision making in a security crisis.” IBM Institute for Business Value. January 2018. https://www.ibm.com/services/us/gbs/thoughtleadership/beyondboom/

6 IBM News Room. “IBM Cybersecurity and Privacy Research.” The Harris Poll. April 13, 2018. http://newsroom.ibm.com/2018-04-16-New-Survey-Finds-Deep-Consumer-Anxiety-over-Data-Privacy-and-Security

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
May 2018

86015886USEN-01