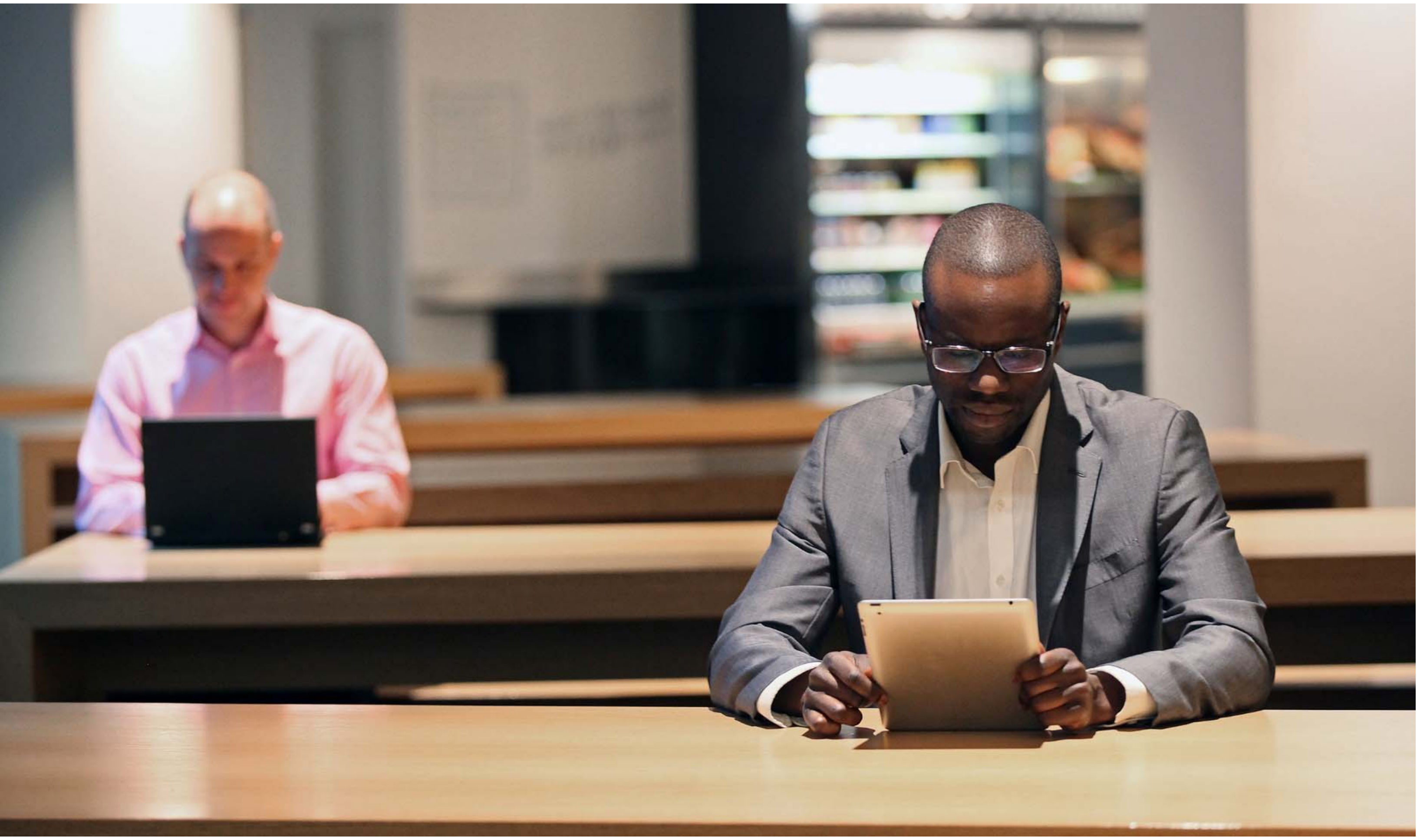
Monetizing data while respecting privacy

How data-use governance can unlock business value and mitigate risk



pwc

Executive summary

In the global digital economy, companies everywhere face a growing challenge: how to use vast amounts of data about individuals they now gather to create greater value for their business and their customers without crossing the line into unethical, unlawful or unwanted use. Indeed, corporate use of data can involve significant risks, including:

- Lack of awareness about data collection and retention activities
- Data being compromised, stolen or misused
- Lack of transparency in how data use affects individuals
- Using data to make decisions that could be perceived as unfair or unethical
- Making wrong decisions because of “bad” data
- Failing to comply with increasingly complex global regulations
- Missing out on opportunities due to an overly cautious approach to data use

In this first installment of a two-part series, we examine some of the major opportunities and risks inherent in data use and the impact on an organization's approach to privacy. We also present a maturity spectrum that illustrates the capabilities and practices that are key to helping companies effectively manage risks and thoroughly leverage the value-creating potential of data use.

For companies to effectively balance opportunity and risk, they must develop strategies that facilitate transparency, empowerment, ethical data use, and overall inclusion with a company’s digital customers. But even more important are strong data-use governance capabilities as part of a stronger privacy program. That’s something many companies currently lack and need to build before increasing their use of data.

We’ve found that progress toward a more sophisticated approach to data-use governance can be tracked on a spectrum that delineates the maturity of an organization’s capabilities and practices. Most companies are at the beginning or in the middle of this spectrum. They typically have basic to intermediate privacy practices and do not fully understand what data they hold and how it is used and protected. In addition, they’ve generally taken only small steps, if any, toward enabling the use of data to create greater value while managing the associated risks. Very few have achieved an advanced stage on the spectrum. These select companies have a holistic view of data-use governance and have put sophisticated data-use governance capabilities in place that effectively balance opportunity and risk.

As the opportunities to use data for growth and competitive advantage expand, so do related risks. That’s why a sophisticated approach to data-use governance is no longer an option – it’s a prerequisite for success in today’s global digital economy.

The data-use challenge: Balancing opportunities and risk

68%

of CEOs see data and analytics technologies as generating the greatest return for stakeholder engagement

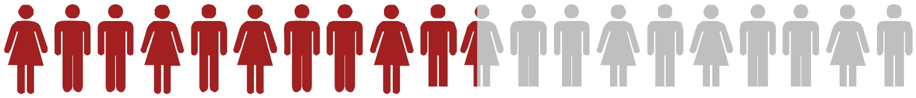
Source: PwC, 2016 Global CEO Survey, January 2016

Thanks to the ever-increasing amounts of data generated on or by individuals and more powerful analytics capabilities, organizations can use and monetize data in ways they couldn't three to five years ago. According to a recent PwC survey, 68% of CEOs see data and analytics technologies as generating the greatest return for stakeholder engagement.[1] These are, however, tricky waters to navigate. Using data in innovative ways can have a substantial upside for an organization and its customers -- but it also comes with greater risks than ever before. Seven such risks are most common:

- *Lack of data awareness:* Organizations are not always fully aware how much data they are collecting by default; what types of data they are collecting and why, how the data is protected, and even where all the data lies. In fact, only 51% of respondents to a recent information security survey reported having an accurate inventory of where personal data for employees and customers is collected, transmitted and stored.[2] Having only a partial understanding of these key issues can lead to missed business opportunities, but also unnecessary risks -- particularly given the evolving state of standards and rules on privacy protections in the United States and around the globe.

51%

of organizations report having an accurate inventory of data



Source: PwC, CSO, CIO, The Global State of Information Security® Survey 2016, October 2015

[1] 19th Annual Global CEO Survey "Redefining business success in a changing world" Jan. 2016 - https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2016.html

[2] "Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security® Survey 2016" - http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/key-findings.html

- *Data being compromised, stolen, or misused.* High-profile data breaches in the past few years affecting billions of records have made organizations painfully aware of what can happen when they don't properly secure and protect their data. The fallout from a breach can be much worse when a victimized company has not previously developed a thorough understanding of its own data collection, retention and use activities and used that understanding to tailor those activities to mitigate privacy and security risks.
- *Lack of transparency*. It's not always clear to individuals or groups of individuals how an organization's use of data affects them. A typical example is the long, complex and often convoluted privacy policy companies use today. Few people can truly understand them and fewer actually even read them. This can lead to unpleasant surprises for individuals when they discover what they really gave companies permission to do with their data when they accepted their privacy terms.

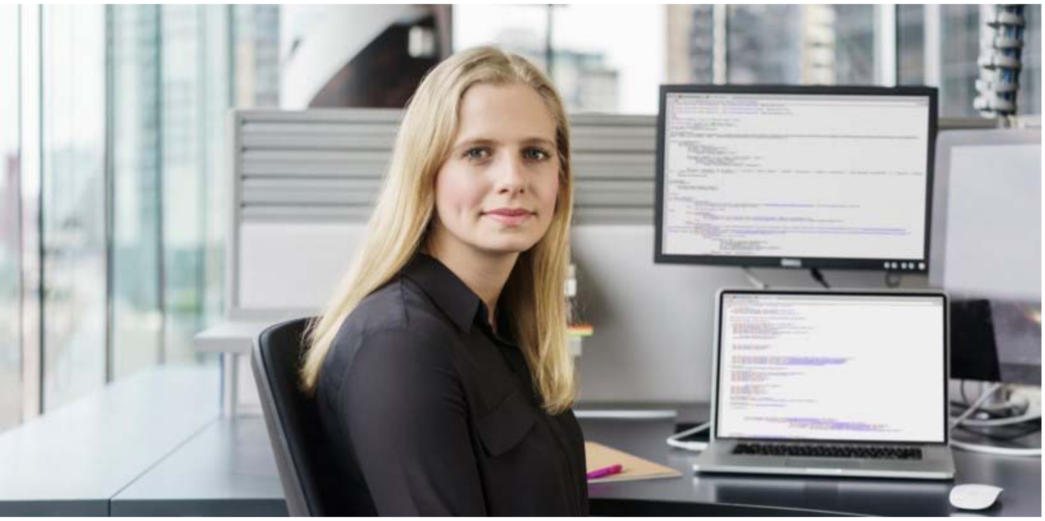
- *Using data to make decisions that could be perceived as unfair or unethical.* In Europe, the new General Data Protection Regulation (GDPR) looks at “data protection” more broadly than how other regions regulate privacy, covering a larger set of individual rights. Many others are also extending the privacy and data protection discussion to include ethical considerations of data processing.[3] In the United States, the Federal Trade Commission (FTC) is questioning the growing complexity of information flows and uses, and is suggesting processing needs to be “fair.”[4]
- *Making wrong decisions because data is inaccurate or not what the company thought it was*. The data could be old or its source unclear. This could put a company in a precarious position if it decides to use that data in a high-impact or high-profile way. The result could be relatively benign, such as mild embarrassment. Or it could be extremely serious, where decisions affect someone’s health or life.

[3] European Data Protection Supervisor “Towards a new digital ethics: Data, Dignity and Technology” - https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf and “Meeting the Challenges of Big Data” - https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

[4] United States Federal Trade Commission (FTC) Staff Report, “Internet of Things: Privacy & Security in a Connected World” Jan. 2015 - https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

- *Failing to comply with increasingly complex global regulations*. Regulatory strength is growing as governments step up their response to concerns over data privacy and how data is used. In fact, relatively minor gaps in privacy controls now can result in substantial monetary damages. For instance, in the European Union, the new GDPR provides fines of up to 4% of a company's global revenue for violating this law.[5] Policymakers in other regions are also looking to increase their regulators' power and courts are becoming more activist. Further, approaches to regulating privacy vary significantly across the globe.

  Unlike the EU's approach, most U.S. data privacy statutes only apply to specific sectors such as healthcare, education, communications and financial services.[6] The Federal Communications Commission (FCC), for instance, recently issued a rulemaking proposal on privacy and data security for internet service providers.[7] In addition, the Federal Trade Commission (FTC) has urged industry to consider data minimization – in other words, limiting the collection of consumer data, and retaining that data only for a set period of time rather than indefinitely.[8]



- *The "reticence risk."* Some organizations are overly cautious and simply choose not to use their data. Whether that's because they have an unclear vision of how to safely use data or they fear possible major negative consequences associated with data collection and use, the result is the same: missed opportunities to create value and gain competitive advantage.

The key challenge for organizations is finding the right balance between using data to create greater value while mitigating the risks inherent in doing so.

[5] © European Union, 1998-2016; "Regulation (EU) 2016/679 of the European Parliament and of the Council" - http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

[6] White House report, "National Privacy Research Strategy" - June 2016 https://www.whitehouse.gov/sites/default/files/nprs_nstc_review_final.pdf

[7] "3 things to know about: The FCC's proposed Broadband Privacy Rule" April 5, 2016 - https://www.pwc.com/us/en/industry/communications/publications/3-things-fcc-broadband-privacy-rule.html

[8] United States Federal trade Commission (FTC) Staff Report "Internet of Things: Privacy & Security in a Connected World" Jan. 2015 - https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

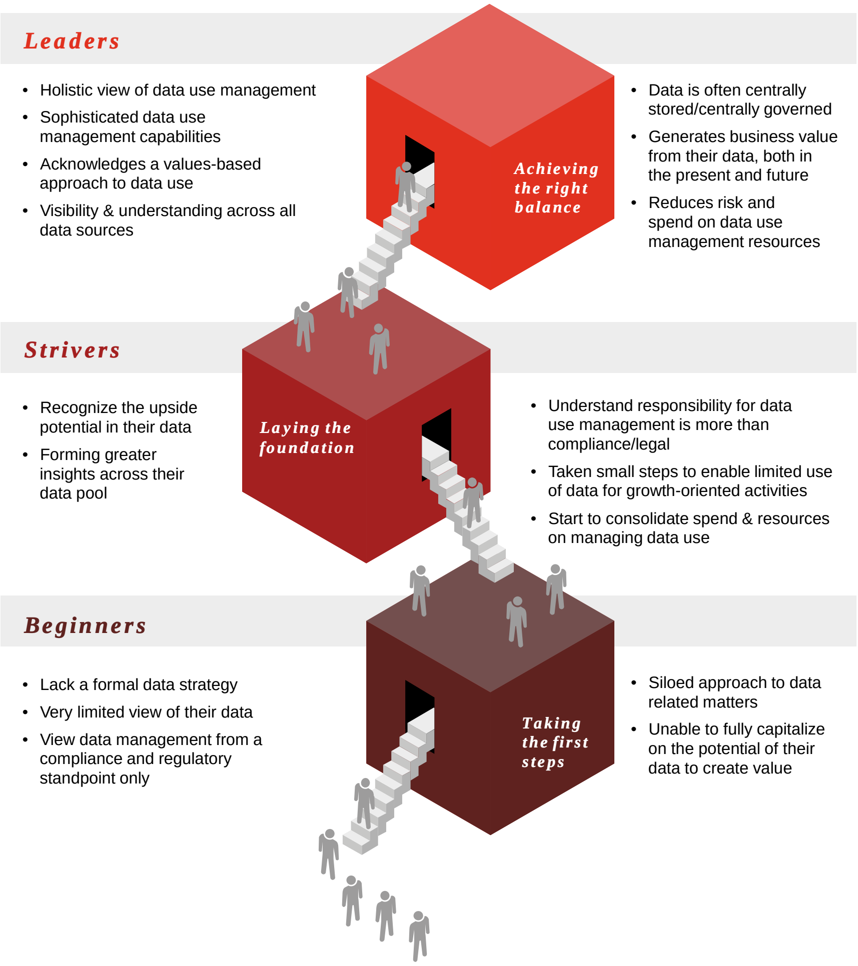
Data-use governance maturity spectrum

Many companies struggle to achieve this balance and put in place appropriate systems to maintain it. In some cases, organizations are just now implementing basic privacy practices and capabilities to protect data, and have yet to consider how to use data better to create greater value. In only rare instances have organizations built the right capabilities that enable them to effectively use their data to create significant business value while safeguarding it from risk.

We've found that organizations' progress in embracing a more sophisticated approach to data-use governance can be tracked on a spectrum as illustrated in Figure 1.

Figure 1

Data Use Governance Maturity Spectrum



Leaders

- Holistic view of data use management
- Sophisticated data use management capabilities
- Acknowledges a values-based approach to data use
- Visibility & understanding across all data sources

Achieving the right balance

- Data is often centrally stored/centrally governed
- Generates business value from their data, both in the present and future
- Reduces risk and spend on data use management resources

Strivers

- Recognize the upside potential in their data
- Forming greater insights across their data pool

Laying the foundation

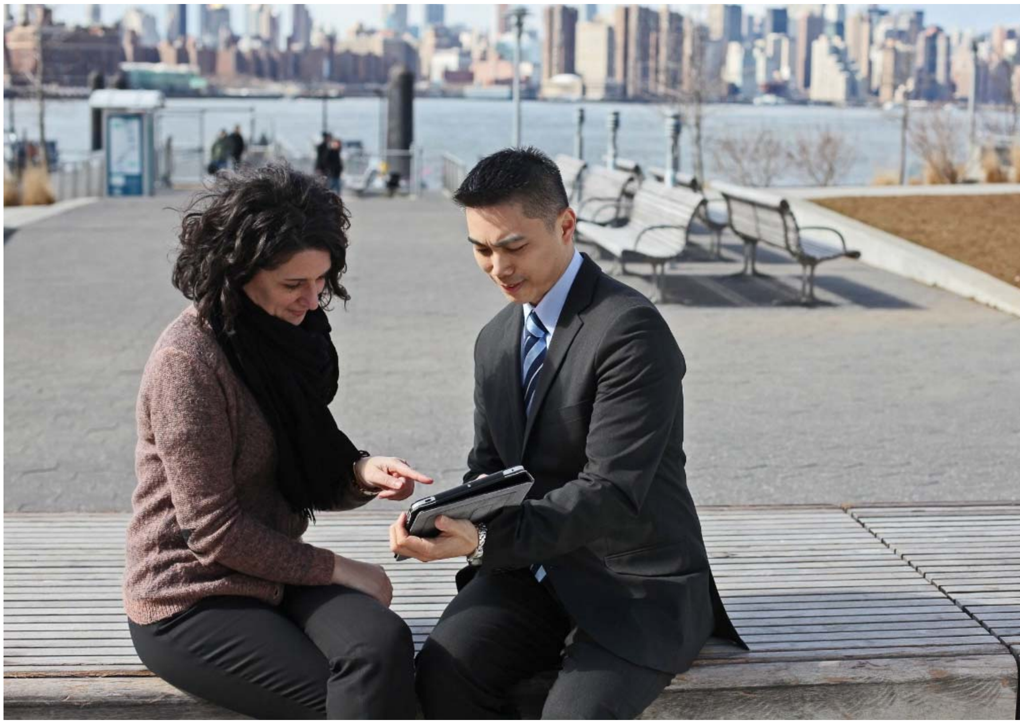
- Understand responsibility for data use management is more than compliance/legal
- Taken small steps to enable limited use of data for growth-oriented activities
- Start to consolidate spend & resources on managing data use

Beginners

- Lack a formal data strategy
- Very limited view of their data
- View data management from a compliance and regulatory standpoint only

Taking the first steps

- Siloed approach to data related matters
- Unable to fully capitalize on the potential of their data to create value



Beginners: Taking the first steps

At the far left of the spectrum are Beginners, which are the least mature in their approach. These companies may have effective data security practices, but they tend to lack a formal strategy for how data is used, both within their organization and outside it. They typically view privacy and data-use governance primarily from a compliance and regulatory standpoint and therefore focus on locking down data as securely as possible.

However, because they also have a very limited view of their data, they don't always know if they're thoroughly protecting their data. As a result, these organizations take a double hit. They can't fully capitalize on the potential of the data to create value, and they leave their data vulnerable to compromise or misuse that could lead to brand, financial, and legal repercussions. Further, by collecting and retaining data by default instead of by design, these companies are missing an opportunity to tailor their data collection and retention activities to avoid unnecessary privacy and security risks.

Strivers: Laying the foundation

In the middle are Strivers. These companies have recognized the upside potential in their data; they understand that responsibility for data-use governance should not be viewed solely from a compliance or legal perspective. And they encourage the owners of various types of data to become part of the data-use governance conversation. But they have taken only small steps to enable limited use of certain types of data for growth-oriented activities, such as improving product development and customer engagement.

Strivers tend to have a largely complete view of where their data resides and how it's used, and have applied common tools that enable them to secure, manage, and properly dispose of it. But they tend to still approach data-use governance mostly in terms of silos rather than in an integrated, coordinated way. The silo approach can result in one part of the business aggressively using data and putting the company at increased risk. Overall, while Strivers have a basic and functional data-use governance infrastructure in place, they are unnecessarily expending resources on managing data use and not capitalizing on data's potential or properly managing data-use risk.

Leaders: Achieving the right balance

A select group of companies could be categorized as Leaders. They take a holistic view of data-use governance and have put in place sophisticated data-use governance capabilities. Leaders have a well-developed and well-understood enterprise-level data-use governance strategy that acknowledges the equal importance of a values- or ethical-based approach to innovative data use and strong data security. They also know how data-use governance differs from but is related to data-protection governance and data-management governance—and how all three are vital components of overall information governance (Figure 2).

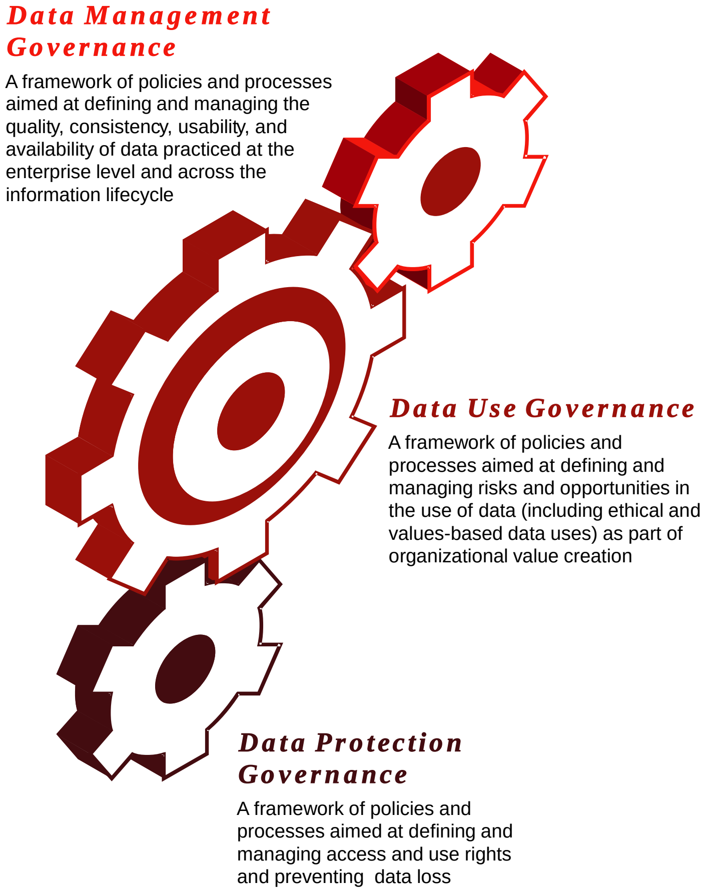
For Leaders, data is often centralized or centrally governed, which makes governance of data use more effective, easier, and less expensive. Owners of data—such as heads of marketing, sales, and product development—collaborate with compliance and legal professionals on two critical initiatives: 1) defining the rules and guidelines for data use and protection; and 2) developing and implementing a flexible enterprise-wide governance structure to enforce their internal policies.

Finally, Leaders have established top-to-bottom roles with clear accountability and responsibility as part of the governance infrastructure. And they use advanced tools to automate many security functions while providing the most robust protection possible.

The bottom line: Leaders' sophisticated approach to data-use governance makes them far more adept at generating business value from their data while reducing risk and their spend on data-use governance resources.

Figure 2

The Semantics of Governance


Data Management Governance
A framework of policies and processes aimed at defining and managing the quality, consistency, usability, and availability of data practiced at the enterprise level and across the information lifecycle
Data Use Governance
A framework of policies and processes aimed at defining and managing risks and opportunities in the use of data (including ethical and values-based data uses) as part of organizational value creation
Data Protection Governance
A framework of policies and processes aimed at defining and managing access and use rights and preventing data loss

Responsible data use in an era of big data

When it comes to data about individuals, companies today have a dual responsibility: to use that data to create more value for the company and its customers, and to do so in the most privacy-centric, ethical, fair, and transparent way possible. Most companies know this. But many have been slow to develop the capabilities that are critical to achieving it. As a result, they are failing to make the most of their data. Perhaps even worse, they could be making themselves vulnerable to questionable data use that puts them in hot water with customers, regulators or legal authorities.

As our maturity spectrum illustrates, the practices and capabilities embodied by data-use governance Leaders should be the desired goal. It's the state companies should strive for and ultimately achieve to effectively balance opportunity and risk. Even more to the point: it's where customers and regulators *expect* them to be.

To begin this journey, companies should first assess where they are on the maturity spectrum. For example:

- Do they have a complete view of the data they hold and its use?
- Do they have a robust privacy policy with appropriate corresponding controls in place?
- How have they begun to integrate the various information governance capabilities across their organization?
- How well are controls being developed that enable data use for value creation and also manage the current and emerging risks?

This preliminary assessment can start a path forward and create cross-organization recognition of the need to approach this space differently and cohesively.

In the second installment of this series, we will detail the main pillars that companies must get right to make the data-use governance structure effective, sustainable, and responsive to the company's business drivers. These are the capabilities we help organizations build to provide competitive differentiation while leveraging the full value creation of data use and managing an organization's risks.

For a deeper conversation about data-use governance, please contact us:

Jay Cline
Principal, PwC
jay.cline@pwc.com

Joe DiVito
Principal, PwC
joseph.v.divito@pwc.com

Carolyn Holcomb
Partner, PwC
carolyn.c.holcomb@pwc.com

Jacky Wagner
Managing Director, PwC
jacqueline.t.wagner@pwc.com

Peter Cullen
Privacy Innovation Strategist, PwC
peter.cullen@pwc.com