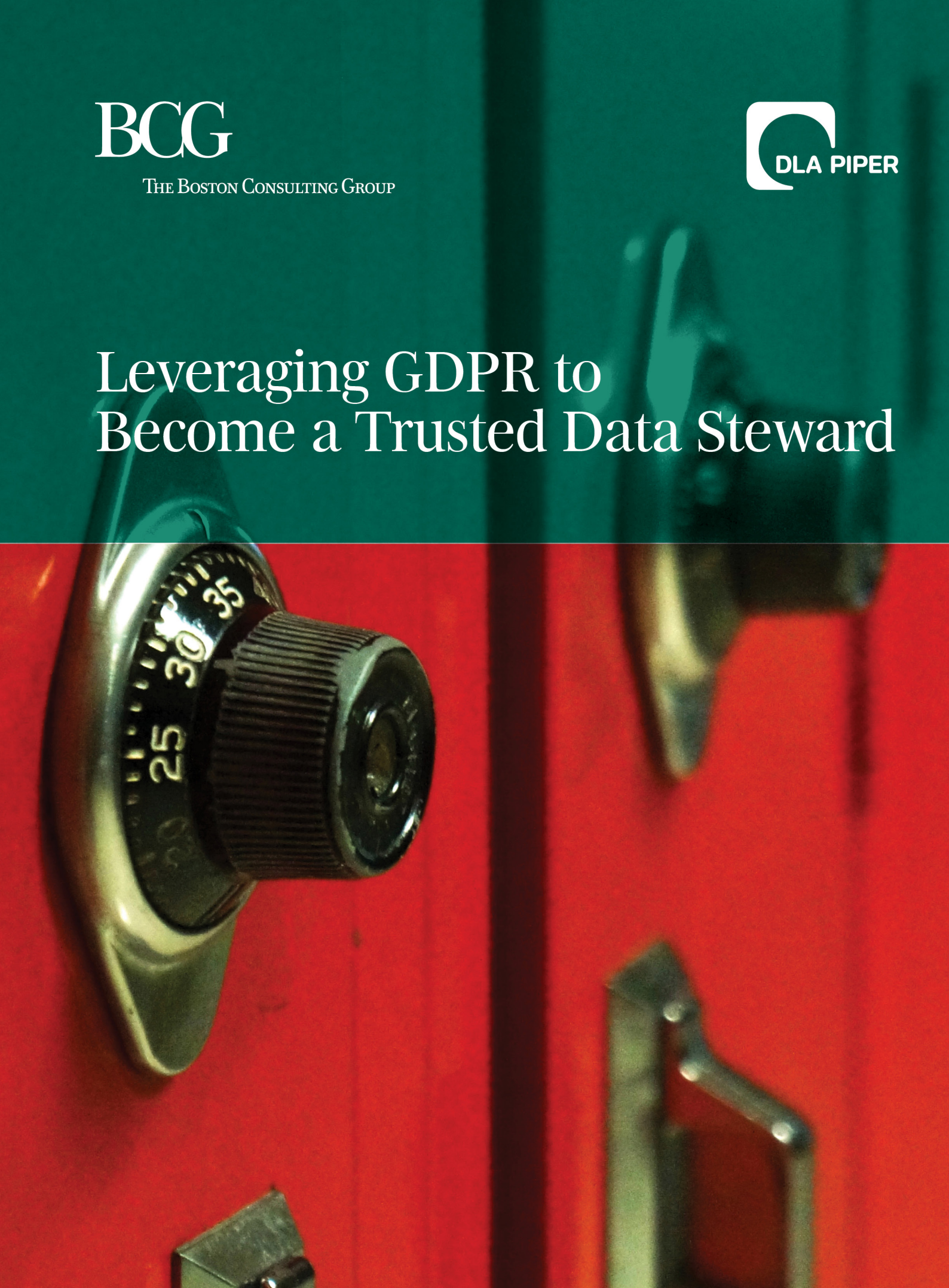
BCG

THE BOSTON CONSULTING GROUP

DLA PIPER

Leveraging GDPR to Become a Trusted Data Steward



The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with offices in more than 90 cities in 50 countries. For more information, please visit bcg.com.

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help clients with their legal needs around the world.

We strive to be the leading global business law firm by delivering quality and value to our clients. We achieve this through practical and innovative legal solutions that help our clients succeed. We deliver consistent services across our platform of practices and sectors in all matters we undertake.

Our clients range from multinational, Global 1000, and Fortune 500 enterprises to emerging companies developing industry-leading technologies. They include more than half of the Fortune 250 and nearly half of the FTSE 350 or their subsidiaries. We also advise governments and public sector bodies.

BCG

THE BOSTON CONSULTING GROUP

DLA PIPER

Leveraging GDPR to Become a Trusted Data Steward

Patrick Van Eecke, Ross McKean, Denise Lebeau-Marianna, Jeanne Dauzier: **DLA Piper**
Elias Baltassis, John Rose, Antoine Gourevitch, Alexander Lawrence: **BCG**

March 2018

AT A GLANCE

The European Union's new General Data Protection Regulation, which aims to strengthen protections for consumers' data privacy, creates an opportunity for companies to establish themselves as trusted stewards of consumer data. But a substantial mismatch exists between what companies think consumers care about in the realm of data privacy and what consumers actually want.

Preparing for the GDPR

The new regulation sets detailed standards for the collection, handling, and sharing of consumer data. It requires that consumer consent be explicit, and it stipulates that consumers have the "right to be forgotten" and the "right to data portability," making companies more accountable for how they process personal data under "privacy by design" and "privacy by default" principles.

From Compliance to Stewardship

Consumers are increasingly uneasy about sharing financial, familial, locational, or use-based personal data. But many companies fail to grasp the aspects of data sharing that especially concern consumers. By aligning their data privacy policies with consumer wishes, companies can go beyond GDPR compliance to gain a valuable competitive advantage as trusted data stewards.

Data-driven transformation is a reality, and companies are increasingly eager to take advantage of it and to scale up their efforts in this area.[1] Arguably, leveraging data represents the most promising source of business and value creation of the early 21st century. As the data-driven transformation of companies and society continues to create data ever more rapidly, in new ways and from new sources, business opportunities based on data will continue to proliferate rapidly.

However, recent BCG consumer research has uncovered a previously hidden obstacle to successfully unleashing this enormous opportunity: data misuse. Data misuse occurs when consumers are unpleasantly surprised to learn that data about them has been collected or has been used in ways outside the original purpose for which it was gathered—and when they perceive such practices to be potentially harmful and feel that the company should not engage in them.

The EU's response to these concerns is the General Data Protection Regulation (GDPR), which will become applicable in May 2018.[2] This regulation sets new and more restrictive standards for data use, and it requires companies to put in place sophisticated approaches and tools to ensure that consumer data is used in an appropriate way. Further, it applies not just to EU companies, but to every organization that handles data on EU citizens.

Even so, DLA Piper and BCG remain convinced that legal and technical approaches are not sufficient to develop the level of consumer trust that companies need. In our view, companies that wish to become trusted data stewards must go beyond mandatory regulatory compliance and the adoption of necessary technical steps relative to data handling. They must, in addition, take a series of proactive measures to increase consumer trust—and they have good reasons to do so.

Companies that wish to become trusted data stewards must take a series of proactive measures to increase consumer trust.

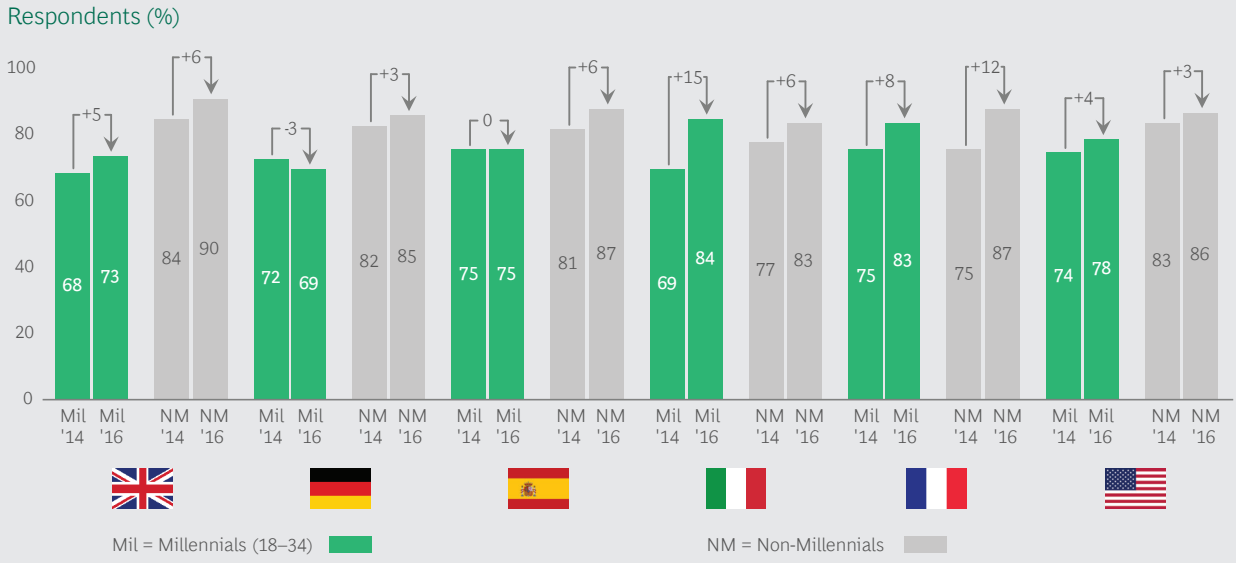
Consumer Attitudes Continue to Vary

BCG research conducted on two different occasions in five European countries (France, Germany, Italy, Spain, and the United Kingdom) and in the US found that concern about the privacy of personal data is a priority among consumers and is on the rise.[3] Consumers in almost every country and age group believe that one must be more concerned or cautious about sharing personal data today than they did just two years earlier. More importantly, the already small gap between Millennials and non-Millennials in this area is closing. Now, overall, at least four out of five European consumers, regardless of their age, are worried about sharing their data. (See Exhibit 1.)

Moreover, BCG found that consumer attitudes about privacy vary depending on the type of data at issue. In the EU countries surveyed, more than 80% of respondents still consider financial data and data with regard to payment card use to be private. Seven out of ten think that information about children, spouses, health status, and taxes is inherently private. Consumers are somewhat less sensitive about the privacy of their location, phone communication, internet use, and email, although 50% of consumers consider such data private, too. (See Exhibit 2.) And whereas most consumers do not consider information such as a consumer's name, age, gender, hobbies and interests, important dates, and brand preferences to be especially private, the percentage of respondents who do view these pieces of information as moderately or extremely private has risen. Part of the reason for this change is that consumers are becoming savvier about data collection and analysis, and less trusting of companies. Consumers are beginning to understand that a company may use these seemingly innocuous pieces of

EXHIBIT 1 | Consumer Caution Is Generally Increasing Across Age Groups and Countries

"You have to be cautious about sharing your personal data online"

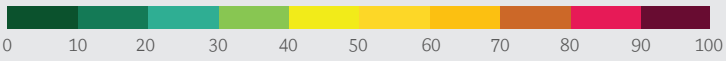


Source: BCG Big Data & Analytics Survey 2014 and 2016.
Note: Survey question: "Please indicate how much you agree with the following statement." Answers using a scale from 1 ("strongly disagree") to 10 ("strongly agree"). The charts shows respondents who answered 8, 9, or 10.

Exhibit 2 | Data Type Is Critical to Understanding and Contextualizing Consumer Sentiment

% who consider the data type moderately or extremely private

Data type	Italy	UK	US	Spain	France	Germany
Credit card	84	79	79	81	89	85
Financial information	83	78	78	79	87	86
Tax information	70	72	77	72	83	83
Information about children	74	70	70	75	81	77
Health or genetic information	68	65	67	71	78	77
Information about spouse	67	59	63	69	78	78
Exact location	46	54	59	58	67	67
Dialed phone numbers	65	60	58	66	77	76
Email	42	50	53	45	54	48
Surfing history	50	48	47	52	64	66
Planned purchases	33	46	45	41	44	47
Important dates	34	45	44	43	48	55
Purchase history	32	42	43	40	53	52
Social network activity	40	38	40	43	54	53
Media usage	32	35	35	38	42	50
Products viewed online	26	33	32	32	39	42
Name	28	26	32	32	46	40
Interests	32	29	30	47	32	43
Age and gender	22	29	30	29	31	37
Brand preferences	15	24	23	22	22	34
Frustrations with products	25	26	22	32	32	32



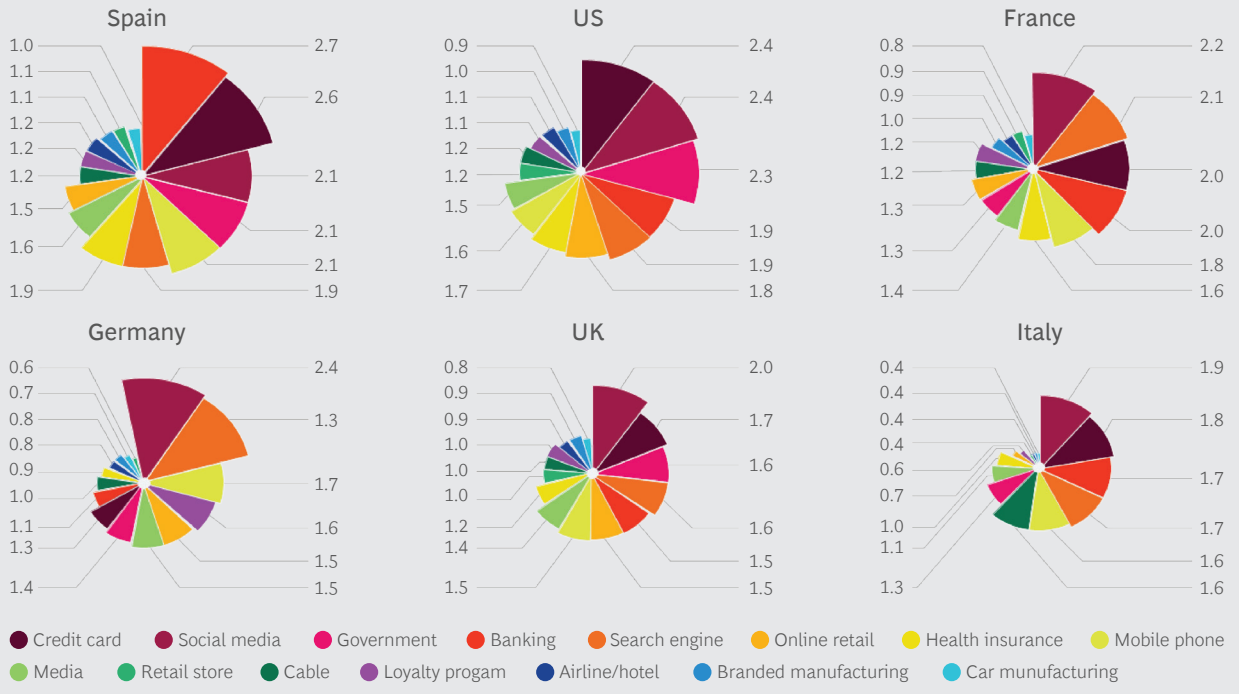
Source: BCG Big Data & Analytics Survey 2016.
Note: Survey question: "How private do you consider the following types of personal data?" Answers using a scale from 1 ("not at all private") to 5 ("extremely private"); multiple answers allowed.

information to de-anonymize other, more sensitive types of collected data to help it build a robust profile of them.

The variations in consumer concern depending on the type of data involved are echoed in consumers' concerns about companies in different industries. (See Exhibit 3.) Consumers are most concerned about online companies (social media, search engines, and online retailers), financial companies (credit card companies and banks), and governments—because these entities handle the type of information that consumers consider most sensitive or because they are the types of companies that most visibly collect consumers' data. Exhibit 3 is particularly important for companies involved in data analytics, as it shows the starting point from which they are working today. Companies in a high-concern industry have an especially high hurdle to clear in attempting to build consumer trust and gain access to consumer data.

EXHIBIT 3 | Consumer Concern Varies Widely by Industry

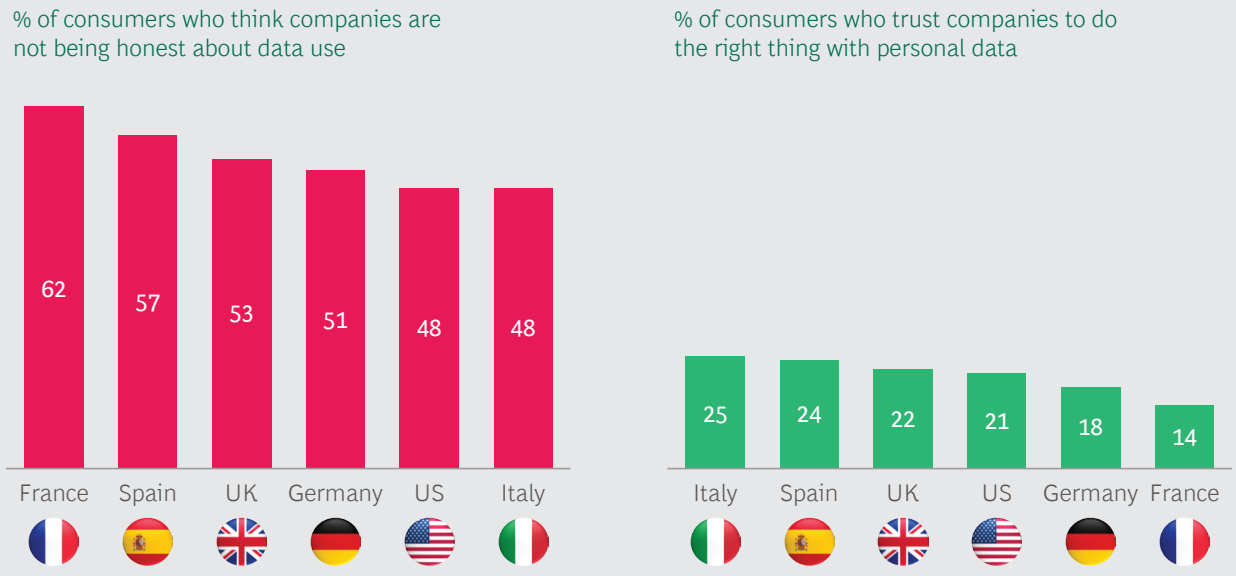
Indexed level of concern (1.0 = 25% of consumers express concern about an industry)



Source: BCG Big Data & Analytics Survey 2016.
Note: Survey question: "Are you concerned about any of the following types of companies or organizations sharing your private data?"

The varying levels of concern that consumers have about companies in different industries are only the tip of the iceberg, however, when it comes to building consumer trust. BCG research shows that between 48% and 62% of consumers do not believe that companies are honest about how they use consumers' data. (See Exhibit 4.) And only 14% to 25% of consumers actively trust companies to do the right thing with their personal data.

EXHIBIT 4 | Consumers Are Primed to Suspect Companies of Misusing Their Data

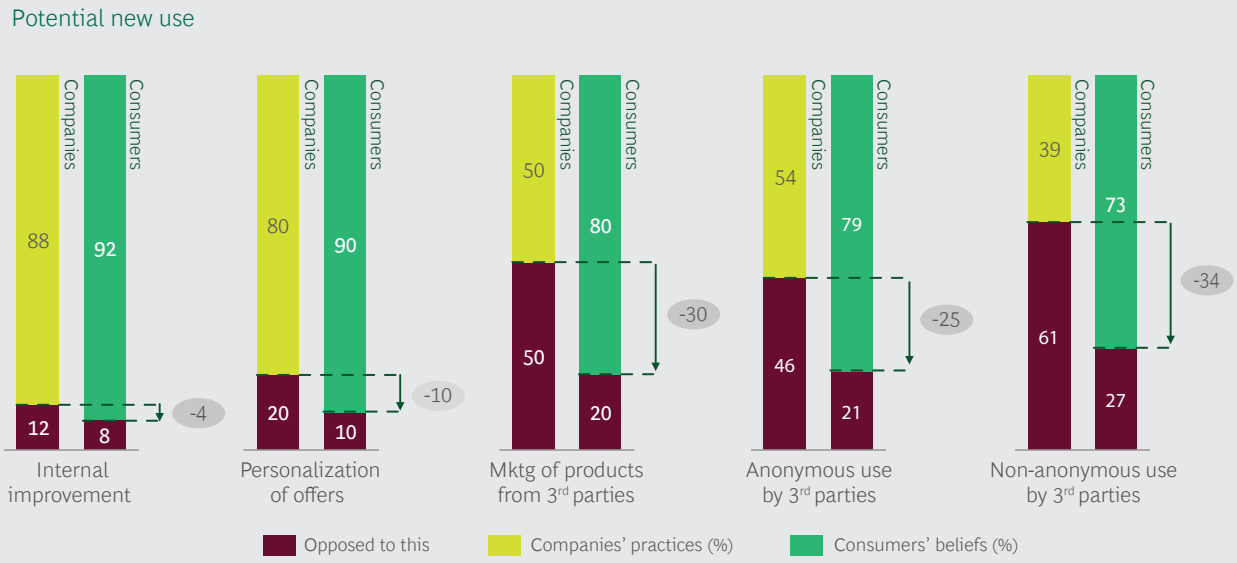


Source: BCG Big Data & Analytics Survey 2016.
Note: Survey question: "How much do you agree or disagree with each of the following statements?" Answers using a scale from 1 ("do not agree at all") to 10 ("agree completely") The charts show respondents who answered 8, 9, or 10 to the following prompts: "Companies don't tell you how they really use your personal data they collect" (left) and "I trust companies and organizations to do the right thing with the data they collect" (right).

Recklessly Conservative Companies

A good way to understand the difficulties that currently exist between companies and their customers with regard to data analytics is to examine what BCG has termed the "recklessly conservative" behavior of companies in collecting and using customer data.[4] Companies are failing to pursue new uses of data that customers are more open to, and when they do pursue a new use, they typically don't inform or educate their customers or ask their permission—although this is something consumers clearly want. We asked consumers and companies about five uses of data and how they thought companies should notify or seek permission for each use: internal improvement of products and services, personalization of offers, marketing of products from third parties, anonymous use by third parties, and non-anonymous use by third parties. (See Exhibit 5.) In each case, we asked companies and consumers to specify whether they thought data should not be used for that purpose, or to select one of five permission and notification methods that companies should use to engage their consumers: opt-in permission, opt-out permission, notification, payment for access to data, or no notification or permission required.

Exhibit 5 | Companies Are Failing to Use Data for New Purposes That Most Consumers Find Acceptable



Source: BCG Big Data & Analytics Survey 2016.
Note: Survey questions: "For each of these new uses, what do you believe your company must do to gain customer consent to use the data?" and "Which approval should an organization have from you for the following uses?"

Overall, companies were 25 to 34 percentage points less likely than consumers to think that third-party use of consumer data is acceptable (consumers and companies were generally in line with each other on internal uses). For example, 50% of companies approve of using consumer data to market products from third parties, while 80% of consumers find this use acceptable. In view of these results, we believe that companies are being unduly conservative in their pursuit of new data uses in the hope that their caution will insulate them from risk. Ultimately, their caution is misguided relative to consumers' actual concerns because, while consumers care less than companies imagine about how the data is used, they care deeply about being informed of its use.

Of the companies in our survey, 28% to 55% thought that they did not need to take any action before using data for each of the five types of use. Only 6% to 15% of consumers agreed with this view. Indeed, the vast majority of consumers want companies to take active steps to secure notification or permission for any use of personal data. More specifically, consumers want to have the choice to opt in or opt out of a data use: more than 60% of consumers believed that opt-in or opt-out permissions should be required for all five types of use. Only two uses of data—internal improvement and personalization of offers—were acceptable to more than 10% of consumers in the absence of action by the company to obtain the consumer's permission.

The active, explicit consent framework defined in the GDPR represents a positive step toward resolving this problem, as it will require companies to get the type of consent that consumer want. But addressing the issue of consent via regulation amounts to treating a symptom instead of the underlying disease. Widespread practice of reckless conservatism suggests that many companies think that operating within the relevant laws and regulations and being cautious about which uses they pursue will safeguard them from customer opprobrium.

In reality, however, a company must do more than simply comply with regulations. It must be open and transparent with its customers in order to build their trust and avoid unpleasant surprises. We believe that the GDPR provides companies an invaluable opportunity in this regard. As they adjust their activities and practices to comply with the GDPR, companies will begin taking steps in the right direction. But in our view they should strive to go beyond simple compliance with the letter of the regulation and take the modest extra steps needed to implement a "smart compliance" program that includes a broader suite of best practices designed to foster consumer trust, thereby achieving a significant competitive advantage moving forward.

Changes Brought About by the GDPR

Privacy issues arising from the data transformation of companies and the growing popularity of web services have pushed the EU to entirely rethink its data protection legislation. The current EU Data Protection Directive, valid until May 2018, was adopted in 1995.[5] EU member states have integrated this directive into their respective national jurisdictions in different ways, resulting in fragmented and inconsistent national legislation on data protection within the EU. The GDPR will replace the Data Protection Directive and, being a regulation rather than a directive, will apply directly in every EU member state, eliminating the current tangle of national data protection laws.

The GDPR provides companies an invaluable opportunity to be open and transparent with their customers and to build trust.

The GDPR retains the key privacy principles defined in the 1995 Directive, which we discussed extensively in our previous DLA Piper and BCG co-authored paper.[6] At the same time, it has brought some important changes, summarized herein.[7]

Harmonization. With a few exceptions, a single set of rules on data protection will be directly applicable in all EU member states, ending the fragmentation of national data protection laws. Although each member state has implemented data protection laws locally that transpose the EU Data Protection Directive, the approaches taken by various national legislators have differed materially, resulting in inconsistent compliance requirements across member states.

The new GDPR institutes a harmonized approach to compliance across all member states, although they will still have the opportunity to adopt local legislation to regulate specific privacy-related aspects such as protection of employment-related data.

Stronger Enforcement. Non-compliance by companies could lead to heavier sanctions under the new regulation. GDPR introduces a revised enforcement regime in which regulators have the power to levy heavy financial sanctions of up to 4% of the annual worldwide revenue of the company and its affiliates worldwide, or up to €20 million, whichever is higher. Each national supervisory authority will have the power to impose these sanctions. This major change from the patchwork regulatory framework currently in force across the EU will dramatically increase the risk associated with privacy non-compliance.

Extraterritoriality. The GDPR's territorial scope will be broader because its provisions will apply both to EU-based companies and to non-EU organizations that target the EU market either by offering their goods or services to EU citizens or by monitoring their behavior.

Regulators have the power under the GDPR to levy sanctions of up to 4% of a company's annual worldwide revenue or up to €20 million.

Governance. The GDPR will replace the current requirement to notify the national Data Protection Authority (DPA) about data processing operations with a more general obligation requiring data controllers to keep extensive internal records of their data protection activities. Controllers must ensure that the processing of all personal data complies with the GDPR and must be able to demonstrate compliance to a supervisory authority upon request. Minimum measures to be taken include the following:

- **Increased Responsibility and Accountability**. Organizations must accept increased responsibility and accountability in managing how they control and process personal data.

- **Performing Data Protection Impact Assessments (DPIAs) for High-Risk Data Initiatives**. Organizations must perform a DPIA before processing personal data in operations that are likely to increase specific privacy risks to individuals due to the nature or scope of the processing operation. We expect DPIAs to become a routine governance tool in managing privacy risk across organizations.

- **Designating a Data Protection Officer (DPO)**. Both data controllers and data processors—whose core activities include regular and systematic monitoring of people (the GDPR calls people whose data is processed "data subjects") on a large scale and large-scale processing of special categories of data or data relating to criminal convictions—must appoint a DPO, who will report to the highest management level. The DPO's tasks will include informing and advising the controller/processor (and the organization's employees) of their obligations, monitoring compliance with the GDPR, advising on data protection impact assessments (DPIAs), and cooperating and acting as point of contact with the supervisory authority.

- **Notifying the Regulator of Data Breaches**. When a significant data breach occurs, controllers must notify the local supervisory authority and (in some cases) the data subjects involved. In most EU member states, such notification is not currently mandatory, so this measure represents a significant departure from current practice.

Unambiguous Consent. The GDPR requires the adoption of a more active consent-based model to support lawful processing of personal data. By established legal principle, a controller can process personal data only for fair and lawful purposes. Under the 1995 Directive, a controller can lawfully process data with the express or implied consent of the data subject or in situations where the processing is necessary for the controller's "legitimate interests" and does not cause undue prejudice to the individual. During the regulatory reform process, many EU legislators felt that the 1995 Directive's regime gives controllers too much flexibility in determining how data is used and that the new regulation should do more to protect consumers' privacy rights. This was particularly true with regard to social media networking and consumer profiling—areas where individuals often have limited ability to control the way their data is shared and where consent often takes the form of implied consent or a broad interpretation of "legitimate interests."

Further, the GDPR significantly refines the definition of "consent." Consent should be freely given, specific, informed, and unambiguous. Implied or implicit consent (inferred, for example, from a person's decision to stay on a website or not to respond to a request) will not be sufficient, as the GDPR states that the consent should be given "by a statement or clear affirmative action." Requiring consent from an end user prior to giving that person access to a service, where the personal data is not necessary to perform the contract, will no longer be allowed. Under the new regulation, controllers must take into consideration in their working practices what the data subject would like and expect his or her data to be used for, and must give each individual the right to change preferences from time to time if, for instance, the person wishes to withdraw consent previously given, or objects to continued processing on grounds of "legitimate interests."

Consent should be freely given, specific, informed, and unambiguous. Implied or implicit consent will not be sufficient.

This flexibility is enshrined in new rights to data erasure ("the right to be forgotten") and will require organizations to adopt a more dynamic consent model/preference type approach to consumer interactions.

Transparency. Companies will have increased transparency obligations and, with a few exceptions (mainly for smaller companies), should maintain a record of processing activities for which they are responsible. The GDPR introduces a new obligation requiring the controller to develop "transparent and easily accessible" policies explaining to data subjects how their personal data will be processed, what their individual rights are, and how those rights may be exercised.

Companies must provide this information in an intelligible form, using clear and plain language that the target audience will understand—ensuring, for example, that they address the topic of data to be collected from children in a manner that children will understand.

Data Breaches. Under the GDPR, organizations must notify the local Data Protection Authority (DPA) and, in some cases, data subjects of significant data breaches.

Data Portability. Companies must ensure that personal data is readily identifiable and extractable so that data subjects can easily transfer their data files to a different service provider.

A new right to data portability introduced by the GDPR empowers each data subject to receive personal data that concerns him or her, and that he or she has provided to a controller, in a structured, commonly used, machine-readable format. The data subject is also entitled to have the data transmitted directly from one controller to another, where this is technically feasible.

Right to Be Forgotten. The GDPR confirms the "right to be forgotten," meaning that data subjects can require a controller to delete data files relating to them if there are no legitimate grounds for retaining those files. The 1995 Directive already includes a right for data subjects to seek a court order forcing a controller to cease data processing in circumstances that might result in damage to the data subjects, as recently recognized by the European Court of Justice's landmark Google Spain ruling.[8]

The GDPR sets rules that permit data subjects to raise objections, force erasure of data files, and prevent further disclosures.

The GDPR builds on this principle with a new statutory right to raise objections directly with the controller, force erasure of data files, and prevent further disclosures in any of the following specific circumstances:

- Where the data is no longer necessary for the purposes for which it was originally collected or processed
- Where the data was originally collected from the data subject based on consent, but where the individual has indicated that he or she wishes to withdraw that consent
- Where the data was originally collected from the data subject based on the legitimate interests of the controller, but where the individual has indicated that he or she objects to personal data being processed for those purposes
- Where the data has been processed unlawfully
- Where the data must be erased in order for the controller to comply with a legal obligation to which the controller is subject
- Where the data has been collected in relation to the offering of information society services to children

Exceptions to the erasure requirement may apply in instances where the controller demonstrates an overriding justification for maintaining the processing of the data—for example, the need to retain records in order to comply with a legal obligation (for example, banking obligations regarding financial and account management data records covering a certain number of years).

In each case where a data subject raises an objection, the controller must take all reasonable steps to inform any third parties to whom the data has been disclosed of the erasure request. This means that the controller must take reasonable measures to manage the way in which any third party makes use of personal data passed on to it.

Data Processors. Organizations that process data on behalf of other companies (that is, "data processors") must comply with a number of specific data protection obliga-

tions, and they will be liable to sanctions if they fail to meet these criteria. The GDPR directly regulates data processors for the first time.

The 1995 Directive generally regulates controllers (organizations responsible for determining the manner and purposes for which any personal data is processed) rather than data processors (organizations that a controller may engage to process personal data on the controller's behalf). Under the GDPR, processors will be required to meet a number of specific obligations, including requirements to maintain adequate documentation, implement appropriate security standards, carry out routine data protection impact assessments, appoint a data protection officer, comply with rules on international data transfers, and cooperate with national supervisory authorities.

These obligations exist in addition to the requirement that the controller must engage processors under a data processing agreement that includes terms mandated by the GDPR. Processors will be liable to sanctions at the same level as controllers if they fail to meet these criteria.

Data Protection Impact Assessment. An organization must conduct a Data Protection Impact Assessment (DPIA) before processing personal data for operations that are likely to present higher privacy risks to data subjects due to the nature or scope of the processing operation. The EU regulatory authorities have issued guidelines for assessing when a new data processing activity or data technology might put people's rights and freedoms at higher risk.

One-Stop Shop. The GDPR offers the possibility that an organization may nominate a single national data protection authority as the lead regulator for all compliance issues in the EU, in instances where the organization has multiple points of presence across the EU.

The GDPR introduces a "one-stop-shop" principle under which the supervisory authority in the country of the controller's (or processor's) main establishment in the EU may be responsible for decisions relating to the controller (or processor) across its EU operations. A company's main establishment is typically the place of its central administration in the EU. Although subject to some significant exceptions, this one-stop-shop principle should reduce the administrative burden of compliance for organizations that have an international footprint and currently must interact with supervisory authorities in each member state where they are present.

Under the GDPR, data processors must maintain adequate documentation, carry out impact assessments, and cooperate with authorities.

Data Protection Officer (**DPO**). The DPO will play an important role within an organization, ensuring that privacy compliance becomes part of the company's DNA. With a few exceptions, companies must appoint a DPO who has the necessary resources, authority in the company, and expertise to fulfill his or her strategy-setting and monitoring obligations.

Privacy by Design and Privacy by Default. The GDPR introduces the concepts of "privacy by design" and "privacy by default." "Privacy by design" means taking privacy risk into account throughout the process of designing a new product or service, rather than treating it as an afterthought. An organization must carefully assess and implement appropriate technical and organizational measures and policies from the outset

to ensure that its processing complies with the regulation and protects the rights of data subjects. "Privacy by default" means establishing mechanisms within the organization to ensure that, by default, only as much personal data as needed is collected, used, and retained for each task, and only for as long as needed.

The Route to GDPR Compliance

This section highlights the key steps leading to a comprehensive compliance plan. Depending on their size, the types of data they handle, and their aspirations, different companies can opt for different levels of complexity to ensure GDPR compliance. Even so, some common steps exist:

Companies can opt for different levels of complexity to ensure GDPR compliance, depending on size, data handled, and company aspirations.

Review the GDPR and assess its applicability to your company. The GDPR will apply to most EU-based companies that handle personal data (such as employee data, consumer data, and prospects data). Non-EU-based entities should make strategic decisions about their approach to the GDPR's requirements and designate a representative to the EU to deal with the regulation.

Conduct an assessment of the current state of personal data. The assessment can be done by questionnaire, interviews with relevant stakeholders, or—if time is of essence—in-the-field work by a dedicated team. It should identify the following types of information:

- All personal data handled by the organization, classified by origin/channel and vintage
- All declared purposes for the collection of this data and associated customer consents
- All producers and consumers of personal data
- All uses of personal data

Conduct a gap analysis and prepare a list of readiness actions. Companies should leverage the outcome of the previous step to analyze legal and technical gaps between the current state and the desired fully compliant situation. Companies should draw up a comprehensive list of remediation actions, prioritize them, and include them in a compliance roadmap. Larger organizations should consider adopting a formal program for change management.

Develop the elements necessary for compliance. This step includes developing a record of processing activities (required by regulation) that includes all elements necessary to fully describe the company's data usage. Depending on the size and complexity of the organization, other elements, such as a data flow map describing the lineage and life cycle of personal data, may also be necessary. This map may be needed to prove that the company can respond appropriately to data subjects' exercising of their new rights (such as data transferability and data erasure).

Implement the remediation plan, and prepare for privacy by design and privacy by default. In the short term, the remediation plan should address all legal and technical compliance gaps (privacy principles and frameworks, accountability, documentation, IT changes if required, and so on). For the middle to long term, the company needs to prepare for such eventualities as regular audits, data protection impact assessments, continuous monitoring against legislative and regulatory updates, and training of staff.

Moving from Simple Compliance to Smart Compliance

BCG is convinced that trust will be a key competitive advantage in a data-driven world. Analytics capabilities, platforms, tools, and other capabilities are necessary but not sufficient to differentiate a company from its rivals, as these things will eventually become commodities. The significance of customer trust, on the other hand, will continue to grow, driven by increasing concerns about data privacy, broadening regulatory oversight, and growing public awareness that companies use data to trigger and direct their actions.

Therefore, organizations must go beyond simple regulatory compliance, no matter how extensive or comprehensive the regulations and laws may be. Consumers want to know that their data is being protected and not used for harmful or offensive purposes; but few consumers are extensively familiar with how regulations like the GDPR protect them and their data. So, in order to ensure continued access to their data, companies must take additional steps to implement a "smart compliance" program that educates their customers and builds trust.

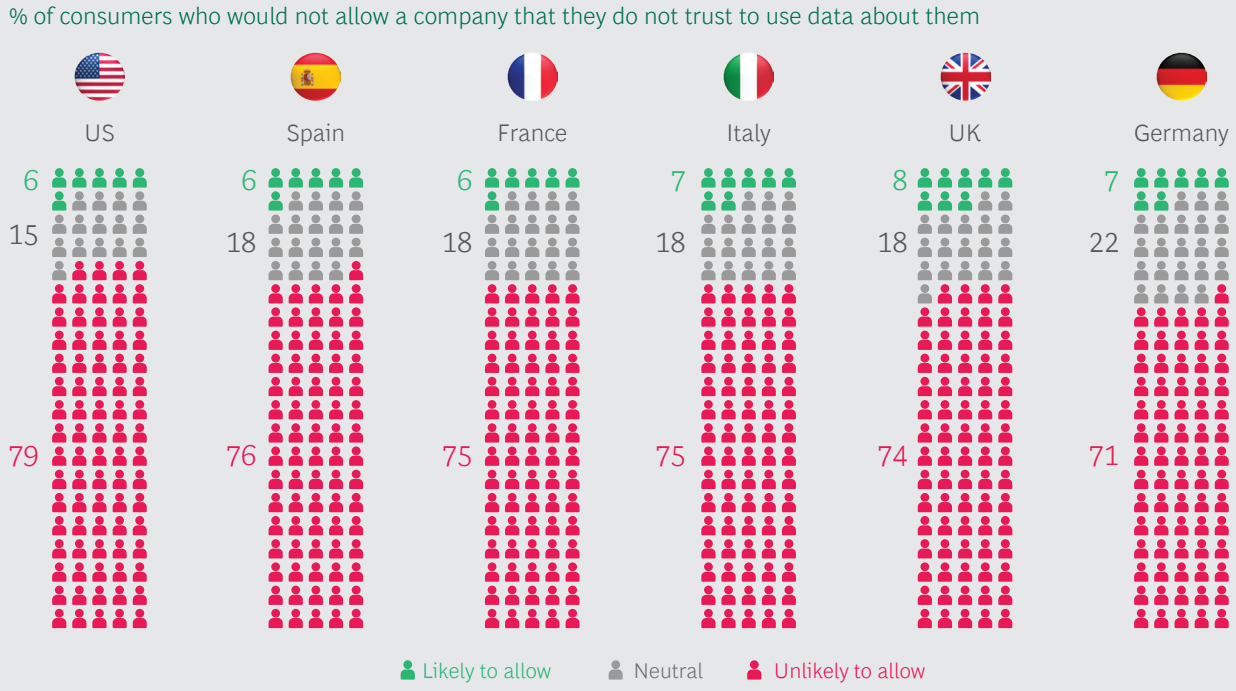
Trust will be a key competitive advantage in a data-driven world, owing to increasing concerns about data privacy.

As discussed earlier, consumers are becoming more aware that their data is being collected, and they see more clearly how it is being used, for purposes ranging from targeted advertisements to customized promotions. But at the same time, consumers are much more wary about sharing their data and are thinking about how companies will use and protect it.

Although the GDPR establishes a legal and economic framework for punishing bad actors, the existence of this new regulation—and companies' adherence to it—will not be enough to build or restore consumer trust. Companies must think about how to become trusted data stewards—companies viewed by their consumers as being law abiding, responsible, safe, transparent, and proactive in data security and customer outreach.

BCG research has shown that failing to engender consumers' trust will lead to drastically decreased access to data, which can cripple a company's data strategy for years to come. (See Exhibit 6.) Further, misuse of data causes companies to lose, on average, one-third of revenues from affected consumers in the first year following the misuse.[9]

EXHIBIT 6 | Distrust Radically Reduces the Amount of Data Consumers Are Willing to Share with a Company



Source: BCG Big Data & Analytics Survey 2014 and 2016.
Note: Survey question: "How much do you agree or disagree with each of the following statements?" Answers using a scale from 1 ("strongly disagree") to 10 ("strongly agree"). The chart shows respondents who answered 8, 9, and 10 (likely to allow), 4, 5, 6, and 7 (neutral) and 1, 2, and 3 (unlikely to allow).

The GDPR's consent-based approval structure shows that regulators recognize the importance of active consumer engagement and trust to a robust data ecosystem. But as companies comply with the GDPR, they must adopt new methods to foster consumer trust beyond the baseline expectation set by the regulation.

Moving from Smart Compliance to Trusted Data Stewardship

Although few companies have attained the status of trusted data steward, building trust is not a herculean task. Fundamentally, it involves leveraging a set of best practices and working to embed a new mindset about customer data usage, premised on the idea that companies are responsible for ensuring that all stakeholders (customers, prospects, and regulators) fully understand the collection and use of customer data. By going the extra mile to become fully compliant with the GDPR, companies can give themselves a sustainable competitive advantage. For this to happen, their data strategy must embrace both internal and external best practices.

Internal Best Practices. Becoming a trusted data steward begins at home. Companies can establish or enhance a number of best practices internally:

- **Ensure engagement by senior executives**. In most companies, senior executives are not substantially engaged in data-related decisions and policies; instead, they delegate responsibility to the company's legal and IT teams. These teams should be involved, of course, because they have crucial expertise. However, personal data use can affect brand value, market share, and revenue growth through consumer and stakeholder perceptions of such use—and these are senior management issues, not just legal or IT ones.

- **Establish company-wide data policies, and make business owners responsible for enforcing them**. A BCG survey of 140 companies worldwide found that at least one-third of them don't have specific data use policies.[10] Among those that do, policies are often fragmented by business line or corporate function into multiple, sometimes incompatible standards. Best-practice companies establish a single set of data policies, governed by a chief data officer (or equivalent) who uses customer interests and business needs as decision criteria.

- **Create robust protocols for data access and use**. Many companies (71%, according to BCG survey results) have protocols in place that govern data access, defining which individuals have access to which types of data—the "who" and "what" aspects. But to truly steward data and avoid the pitfalls of unapproved use, companies must also proactively manage the "why" aspect: the permissible ways in which employees and internal teams (such as analytics teams) may use the data they are authorized to access.

- **Leverage tools for monitoring data quality and data usage**. In a perfect world, data would always be clean and everyone would follow purpose-based access protocols that were compatible with both corporate and GDPR guidelines. In the real world, companies need to ensure that violations of access or customer consent do not occur. Monitoring approaches must focus on the same who-what-why elements that data access protocols should address, with support from appropriate off-the-shelf or company-specific tools.

In the real world, companies need to ensure that violations of access protocols or customer consent do not occur.

This list is not exhaustive. Other internally focused practices, such as the establishment of a company-wide organization focusing on data quality and led by a chief data officer (CDO), are characteristic of a modern data governance organization and operating model.

External Best Practices. In addition to taking internal actions, companies must actively engage with customers and other stakeholders through external practices. Examples of such practices include the following:

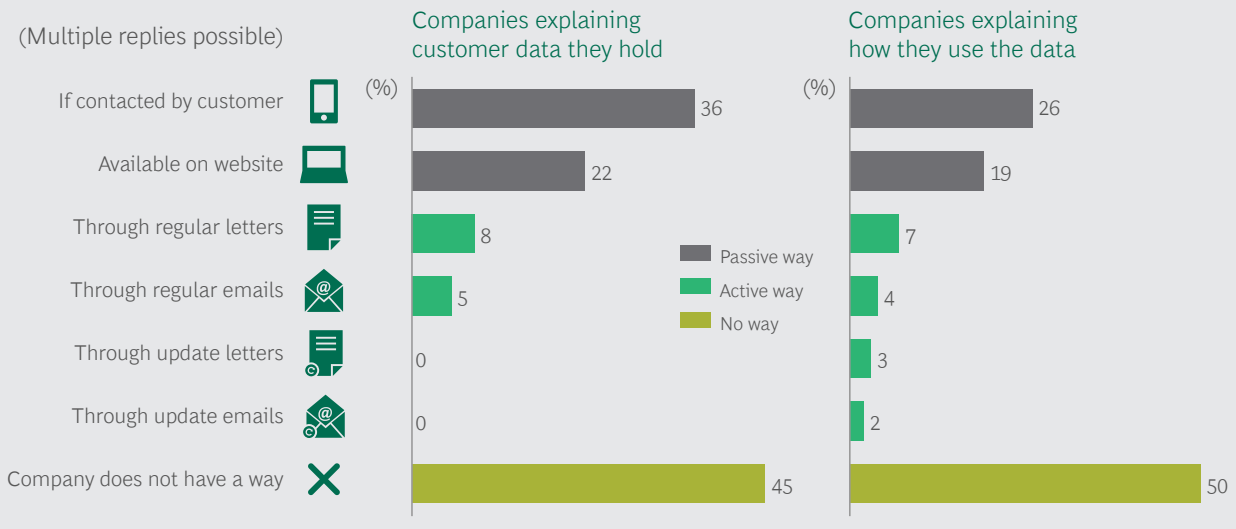
- **Be on time for GDPR compliance** (**and let it be known that you are**). A recent survey by DLA Piper found that the average alignment of companies to the GDPR's challenges is just 34%, meaning that many organizations have numerous compliance gaps in relation to the new regulation.[11] BCG's work with several leading companies leads us to believe that this figure may underestimate the extent of noncompliance—but either way, a large percentage of companies will probably not be ready when the GDPR takes effect. Hence, the few companies that are compliant

will have bragging rights that reinforce their image as data stewards with consumers and stakeholders.

- **Be more transparent and proactive in your data-related communication.** For most companies, ensuring a high degree of transparency calls for a major shift in mindset and culture—from making information available and adhering to regulatory requirements for disclosure (such as the ones contained in the GDPR), to being responsible for ensuring that customers and other stakeholders understand what a company is doing with their personal data. To make the transition from opaqueness to transparency, a company must adopt a new set of engagement practices, moving from pull communication to push communication. Today, communication practices are overwhelmingly designed to support customers who take the initiative to investigate and understand data use practices. (See Exhibit 7.) But few consumers currently do so, leaving the majority primed for distress when they are unpleasantly surprised by data activities whose details or implications they had not fully understood. BCG's survey also found that a large proportion of companies have no way to explain to their customers what data they hold on them or how they use this data.

- **Go public with your key data use principles.** Companies should use their corporate website or another suitable platform to make widely available the key principles that guide their use of customer data. This information can take the form of a data charter—a concise, easy-to-read document written with the customer in mind. Companies may want to create two versions of this document: a short version to publish on the company's website, and a longer, more detailed version for internal

EXHIBIT 7 | Many Companies Either Use Passive Methods of Data-Related Communication or Have No Way to Communicate



Source: BCG Big Data & Trust Consumer Survey 2016.
Note: Survey questions: "With regard to engaging with customers about the data your company holds about them, which of the following statements are true?" and "With regard to engaging with customers about how you use their data, which of the following statements are true?"

communication. A few BCG clients in the EU have already published data charters, which typically affirm five company commitments:

1. Protect customer data and ensure data security and integrity.
2. Proactively restore control of data to customers.
3. Share data for the common good.
4. Use data to create value for the customer.
5. Enter a continuous process that guarantees these commitments.

- **Measure and publish metrics about customer trust.** As with all key corporate activities, a company cannot make progress toward becoming a trusted data steward without active measurement. And in the context of data transparency, key metrics should be shared with customers and other stakeholders. At present, few companies actively monitor their customers' trust, let alone communicate with them on these metrics. Doing so is therefore a way to differentiate and start building a data-use-related competitive advantage. Best-in-class companies have created metrics that monitor trust by regularly and routinely tracking stakeholders' perceptions. These metrics should, of course, be tailored to a company's unique situation, but they should generally cover the following issues:
  - Overall trust in a company's data stewardship
  - Understanding of a company's data practices
  - Areas of significant sensitivity and concern
  - Consumers' willingness to allow the company to pursue new uses of data (with their consent)

Top companies have created metrics that monitor trust by regularly and routinely tracking stakeholders' perceptions.

COMPANIES THAT CHOOSE this track and earn the trust of well-informed customers will be able to create more value from consumer data. As BCG research has shown, consumers are at least five times as likely to share data with a company they trust as with a company they do not trust. Trusted companies will therefore be able to access more data for current uses and will be able to obtain the consent of their customers for new uses unavailable to less-trusted competitors.

Organizations, especially those operating within the EU, should leverage the work that they have already invested and will continue to invest in GDPR compliance to move closer to becoming truly trusted data stewards.

NOTES:

[1] See "Data-Driven Transformation: Accelerate at Scale Now," BCG article, May 2017.
[2] European Union Regulation EU/2016/679.
[3] BCG Big Data & Trust Consumer Survey, 2014 and 2016.
[4] See "Bridging the Trust Gap: Why Companies are Poised to Fail with Big Data," BCG article, October 2016.
[5] European Directive EC/1995/46.
[6] DLA Piper & BCG, "Earning Consumer Trust in Big Data: A European Perspective," March 2015.
[7] A brief glossary of GDPR-related terms used is included in the appendix.
[8] See *Google Spain SL, Google Inc. v Agencia Española de Proteccion de Datos*, Case C-131/12, May 2014.
[9] See "Bridging the Trust Gap: The Hidden Landmine in Big Data," BCG article, June 2016.
[10] BCG Data Enablement Survey, 2016.
[11] See "Global Data Privacy Snapshot 2018," DLA Piper, January 2018.

Appendix: Glossary of Key GDPR Terms

Consent: Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Controller (or Data Controller): The natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Breach: A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

Data Filing System: Any structured set of personal data that is accessible according to specific criteria, whether centralized, decentralized, or dispersed on a functional or geographical basis.

Data Processing: Any operation or set of operations that are performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure (by transmission, dissemination, or otherwise making available), alignment, combination, restriction, erasure, or destruction.

Data Protection Authority (DPA): A national and independent administrative regulatory body whose mission is to ensure that data privacy law principles are applied to any processing of personal data, within its territory. Each authority has powers of investigation, intervention, sanction, and engagement in legal proceedings.

Data Protection Impact Assessment (DPIA): A tool designed to enable organizations to work out the risks that are inherent in proposed data processing activities before those activities commence, in order to address and mitigate the risks before the processing begins. Also, a systematic process that identifies and evaluates, from the perspective of all stakeholders, the potential effects on privacy of a project, initiative, proposed system, or scheme and that includes a search for ways to avoid or mitigate negative impacts on privacy.

Data Protection Officer (DPO): A person who is formally tasked with ensuring that an organization is aware of and complies with its data protection responsibilities.

Data Subject: A natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity.

EDPB: The European Data Protection Board, an EU body made up of representatives from national DPAs and the EDPS.

EDPS: The European Data Protection Supervisor, a body responsible for ensuring that EU institutions comply with EU data protection law.

Information Society Service: A service as defined in point (b) of Article 1(1) of EU Directive 2015/1535 of the European Parliament and of the Council—namely, any service provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of such service.

Opt In: Express consent by a data subject to the processing of personal data for a stated purpose (such as for the purpose of sending him or her electronic marketing communications).

Opt Out: Consent by a data subject that may be implicit or may be obtained in the form of acceptance of a negative sentence, such as "I do not object to the processing…."

Personal Data: Any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier—such as a name, an identification number, location data, an online identifier—or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Processing: Any operation or set of operations that are performed on personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure (by transmission, dissemination, or otherwise making available), alignment, combination, blocking, erasure, or destruction.

Processor (or Data Processor): A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

Profiling: Any form of automated processing of personal data consisting of evaluating certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Pseudonymization: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

Purpose: The goal for which personal data is especially collected.

Record of Processing Activities: An electronic or paper list of all data processing activities for which a data controller or, in some cases, a data processor is responsible.

Third Country: A state outside the European Economic Area (EEA), which currently consists of the 28 EU member states plus Iceland, Lichtenstein, and Norway. *Following the UK's submission of a notice of withdrawal under Article 50 of the Treaty of Lisbon, the United Kingdom will remain an EU member state until midnight (Brussels time) on 29 March 2019, unless the European Council decides unanimously to extend the two-year negotiating period. On the date of withdrawal, the United Kingdom will become a third country.*

Third Party: Any natural or legal person, public authority, agency, or body other than the data subject, the controller, the processor, and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

WP29: The Article 29 Working Party, an EU-level advisory body composed of representatives of the 28 EU DPAs and the EDPS, created under Article 29 of the 1995 Data Protection Directive. Under the GDPR, the EDPB effectively replaces the WP29.

Authors

DLA Piper

Patrick Van Eecke
Partner
patrick.vaneecke@dlapiper.com

Ross McKean
Partner
ross.mckean@dlapiper.com

Denise Lebeau-Marianna
Partner
denise.lebeau-marianna@dlapiper.com

Jeanne Dauzier
Senior Associate
jeanne.dauzier@dlapiper.com

The Boston Consulting Group

Elias Baltassis
Director, Data & Analytics
baltassis.elias@bcg.com

John Rose
Senior Partner, Managing Director and BCG Fellow
rose.john@bcg.com

Antoine Gourevitch
Senior Partner and Managing Director
gourevitch.antoine@bcg.com

Alexander Lawrence
Project Leader
lawrence.alexander@bcg.com

To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com.

Follow bcg on Facebook and Twitter.

03/2018


BCG
THE BOSTON CONSULTING GROUP


DLA PIPER