BCG
THE BOSTON CONSULTING GROUP

DLA PIPER

Earning Consumer Trust in Big Data: A European Perspective

Carol Umhoefer, Jonathan Rofé, Stéphane Lemarchand - DLA Piper
Elias Baltassis, François Stragier, Nicolas Telle - The Boston Consulting Group
March 2015

Big Data represents a promising source of business value creation. The exponential growth of available data is creating an environment well suited to companies looking to generate new opportunities, improve their operating model, or construct new business models. A granular understanding of consumer behaviors and habits will be fertile ground for developing new products and services, improving existing offerings, reinforcing relationships with consumers, and boosting revenue.

The use of Big Data is nonetheless sensitive by nature, as it often relies on the processing of personal data in a constantly changing technological environment. The relatively new areas of data protection and data privacy are governed by numerous and complex regulations that are permanently mutating.

Moreover, the approaches to privacy are fundamentally different in the world's three-largest markets. Data privacy in the U.S. varies depending on the sector, such as health, telecommunications, or financial services; China's laws focus on consumers and trade secrets; and the EU takes a holistic approach. Consequently, exploiting personal data may expose businesses to risks that are underestimated or even unknown. These risks are most obviously legal, but also reputational.

Consumers need to be convinced that their personal data is adequately protected and used fairly; trust is the key to maintaining a fruitful relationship. It is therefore necessary to clearly understand the legal implications of Big Data to allow consumer confidence to grow and prosper.

The Big Value of Big Data

Big Data is a misleading term. It rightly puts emphasis on data but conceals other important aspects. For BCG, Big Data is the transformational impact on businesses of being able to economically capture, analyze, and interpret ever larger and more complex data in order to drive a step change in value creation and model change. Big Data refers to three components: massive volumes of multisourced, multistructured data that are growing exponentially owing to the digitization of society and the development of the Internet of Things; new technology ecosystems that offer quasi-infinite scalability and that facilitate the storage, processing, and analysis of data at an ever-diminishing cost; and finally, advanced analytics—mathematical and statistical techniques often referred to as machine learning—that are vastly superior to previous approaches and provide insights that are not merely observational (or descriptive) but also predictive.

Understand What Was Incomprehensible ; Anticipate the Unknown. Big Data's potential for businesses is huge, provided that the right practices, organization, and tools are put in place to extract the value hidden in the data. The digitization of commercial transactions and consumer interactions, the advent of social networks, the increasing mobility of communications, and the Internet of Things all create data that encompasses a far larger realm of consumer behavior than the data existing and used only a few years ago. Traditional data sources—such as payment cards, loyalty programs, Internet purchases, after-sales service, and requests for information—can be further refined by data originating from social networks, online behavior, mobile devices, and connected objects. Data from all of these sources can be combined to provide rich insights into consumer preferences, purchasing habits, and interests. Traditional marketing methods, including consumer surveys and *in situ* panels, are rapidly becoming obsolete.

Big Data's big opportunity resides in the diversity, quality, and granularity of the data processed. The huge volume of data, its processing, and the algorithms that permit the creation of personalized purchasing profiles enable businesses to understand—in real time—the detailed evolution of consumer behavior. With increasingly sophisticated technologies, businesses can predict, or even anticipate, purchasing decisions and consumer behavior.

Consumer Trust Is The Key to Unlocking Big Data's Full Value Potential

Consumers' awareness of their personal data continues to grow, in no small part because of the media's increasing coverage of data breaches and personal data surveillance. Dominant Internet actors, such as Google and Facebook, have been heavily criticized—indeed, sanctioned by regulators in both the U.S. and the EU—for changes to their data-privacy policies.

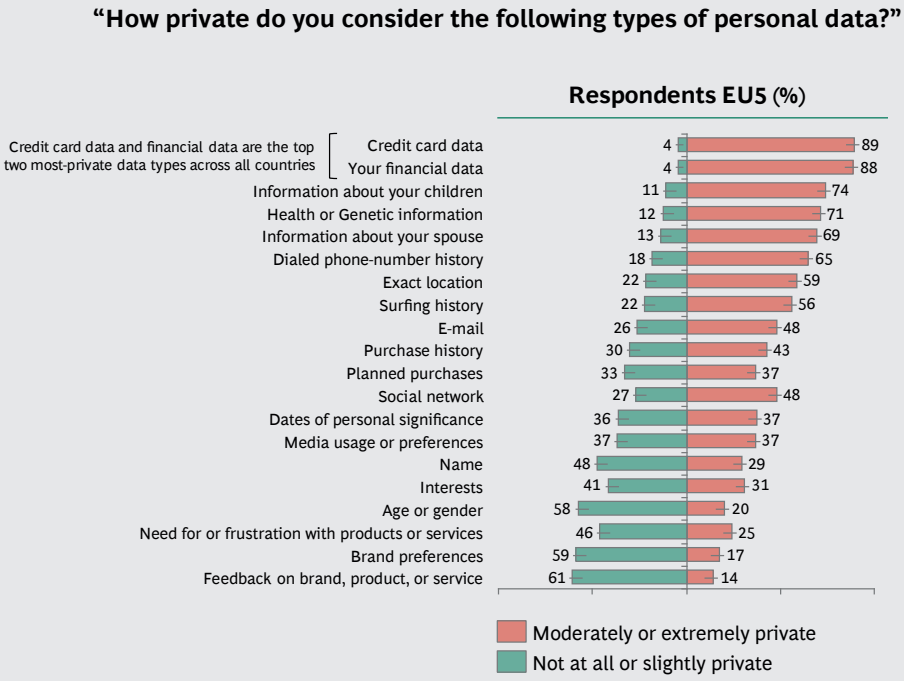
It takes time to gain a consumer's trust, but only an instant to lose it. BCG's research has shown that consumer trust is the key factor that determines the opportunities companies can reasonably pursue. Consumers need to feel confident that their data will be used in a fair, honest, and controlled manner. The economic impact of consumer trust is considerable: a business that builds such confidence can expand the data it can access and use tenfold. Not all companies will be able to create—and maintain long term—trust of this type. Without such confidence, however, the billions of Euros in future economic and social value that Big Data represents might be lost.

Consumer Attitudes Vary. BCG researched 10,000 consumers in 20 countries and found that consumer attitudes about confidentiality vary according to the type of data at issue.[1] In the EU countries surveyed, almost nine people out of ten consider financial data and data regarding payment card use private. Seven out of ten think that information about children, spouses, health status, and telephone communications is inherently private. Consumers are somewhat less sensitive about the privacy of their location, Internet use, e-mail, purchasing history, and use of social networks, although 50 percent of consumers consider such data private as well. Family name, age, gender, hobbies and interests, and brand preferences are considered private by a minority of the consumers surveyed. (See Exhibits 1 and 2.)

Exhibit 1 | Consumers Are Cautious About Sharing Personal Information Online

Source: BCG Global Consumer Sentiment Survey 2013.
Note: Respondents were asked, "Please indicate how much you agree with the following statement."

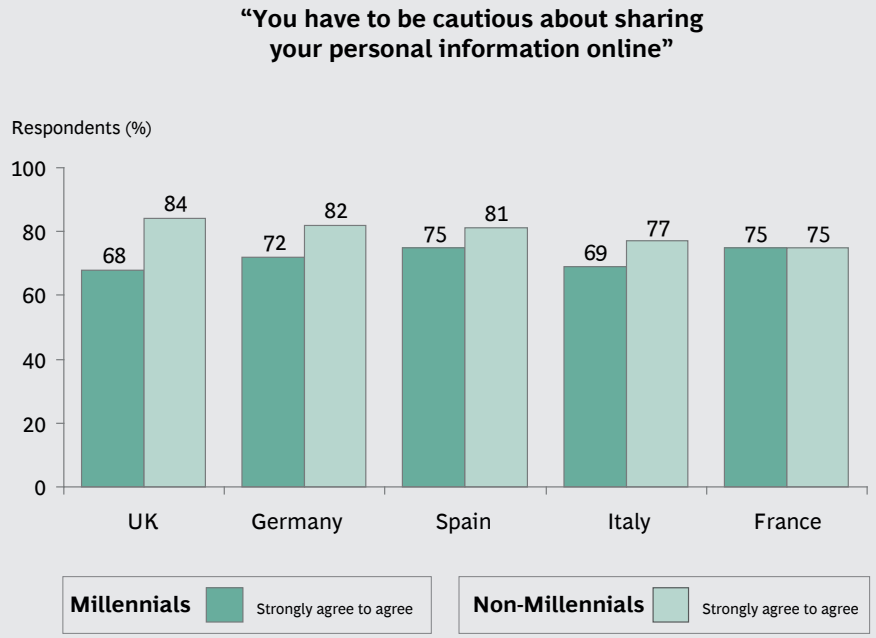
Exhibit 2 | Feelings About Privacy Vary Depending on Data Types



Source: BCG Global Consumer Sentiment Survey 2013.
Note: EU5 (European Union 5) includes Germany, France, Italy, Spain, and the U.K.

Overall, 75 percent of the consumers surveyed in most countries consider that the privacy of personal data is a priority issue. It is interesting to note that this attitude is shared across all age groups, refuting the conventional wisdom that only the baby boomer generation is focused on privacy issues. Younger generations (for example, Millennials) share the concerns of their elders. (See Exhibit 3.)

EXHIBIT 3 | Millennials and Non-Millennials Show Similar Caution About Sharing Personal Information Online



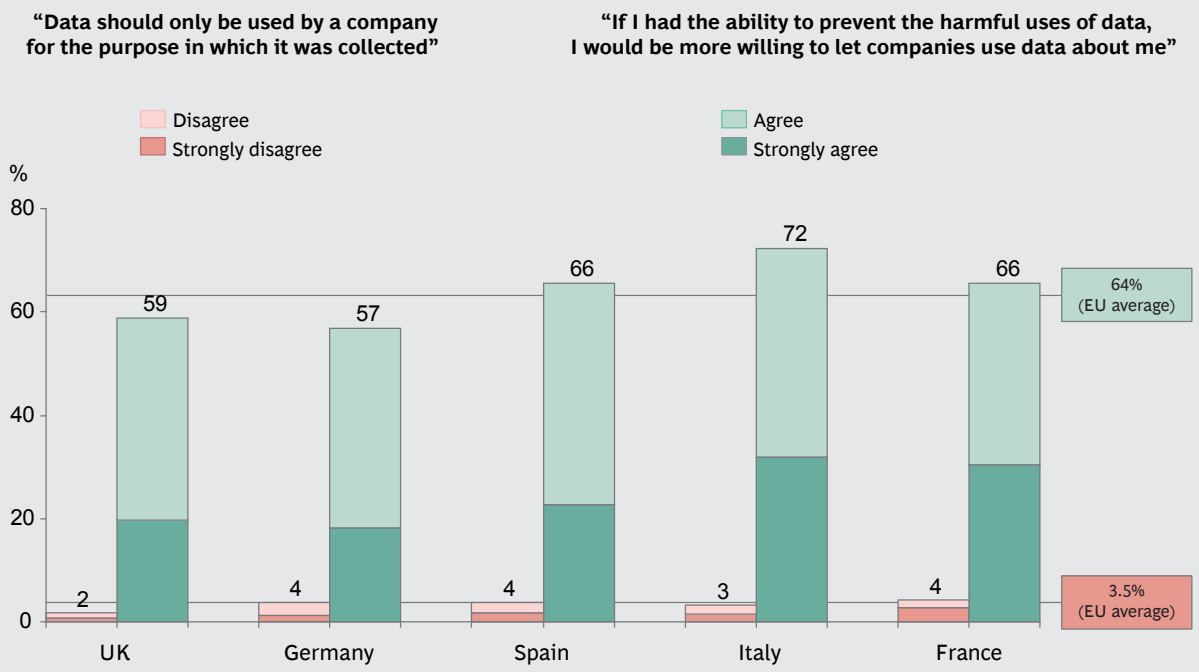
Source: BCG Global Consumer Sentiment Survey 2013.
Note: Millennials are defined as 18 to 34 year olds; non-Millennials are age 35 or older.

BCG's research also shows that in most of the countries surveyed, more than half of consumers accept the use of their personal data by companies, provided consumers are confident that no harmful consequences will ensue. Sixty-six percent of French respondents shared this view, compared with 57 percent in Germany and 53 percent in the U.S.

There are dozens of recent examples of significant loss of consumer trust. In some cases, companies insufficiently protected personal data, leaving it vulnerable to a data breach. In other cases, companies intentionally shared consumer data with third parties, violating consumers' trust.

The experience of two major European telecom operators is instructive. Both provided data on their consumers' location and movements to retailers. However, one operator had invested in advanced anonymization techniques; the other did not. When revelations surfaced of consumer data sharing, the telco that did not take sufficient steps to protect consumer data received significant criticism, while the company that was proactive did not. In sum, two companies operating in the same sector, processing similar data, and using the same analytic approaches had divergent market experiences owing to the trust of consumers and regulators.

EXHIBIT 4 | Preventing Harmful Uses Can Increase Access to Consumer Data by At Least Five to Ten Times in Most Countries



Source: BCG Global Consumer Sentiment Survey 2013.

In the current environment, consumers are concerned about the potential use (and abuse) of their personal data. Only companies that convince consumers that their personal information will be used fairly and honestly will be able to widen the scope, variety, and volume of accessible data. (See Exhibit 4.)

Reasonable Use of Personal Data. It can be difficult to reconcile what are sometimes competing if not conflicting interests in Big Data:

- Businesses want access to the maximum volume and variety of data possible in order to better understand their customers and improve their products, services, and revenues.
- Governments may seek to regulate and to limit as much as possible access to data and its processing.
- Consumers are willing to trade their data for personalized and free services, but within certain limits that are difficult to predict.

Only a fair and reasonable use of personal data that creates consumer and regulator trust can reconcile these interests.

A Complex Legal Environment

The legal approach to data protection and privacy in the U.S. and the EU is at odds on many points. The U.S. takes a sector approach, with strict requirements for health and financial data in particular. There is no single privacy regulator. And in some cases, there's no federal privacy law but rather dozens of state laws. The EU, under the 1995 Data Protection Directive (officially Directive 95/46/EC), has a harmonized, transversal approach, imposing a standard set of principles on the processing of personal data across all 28 member states. The EU Directive is soon to be revised by the Data Protection Regulation. (See the sidebar "The Forthcoming EU Data Protection Regulation.")

In Asia-Pacific, countries such as Singapore, Malaysia, and the Philippines are adopting privacy laws modeled on those in the EU. Some countries, such as Australia, have strengthened their laws. And other countries, notably China, have focused on protecting consumer data and do not have broadly applicable privacy laws.

Looking at the EU, national laws in each of the member states have transposed the Directive's principles and created a single data-protection authority for each country. These authorities have varying powers to investigate violations and to set and impose sanctions under their respective national data-protection laws. To cite a few examples, in Romania, administrative sanctions are up to €11,200, compared with €150,000 in France (€300,000 for a repeat violation) and €600,000 in Spain.

The Current EU Data-Protection Directive

The principles set forth in the Directive are pivotal to understanding the legal risks of Big Data processing in the EU.

The Data Controller. The data controller is defined as "the natural or legal person, public authority, agency or any other body which alone, or jointly with others, determines the purposes and means of personal data processing."[2] The data controller assumes most of the legal obligations for personal data under the Directive. Regardless of whether the data controller entrusts a third party with responsibility for data processing, the data controller remains liable. Moreover, the location of the data controller *and* the means of processing it controls will determine which national data-protection law applies. Therefore, a data controller established in the UK, or established outside the EU but using means of processing in the UK, will be subject to the UK's 1998 Data Protection Act (DPA). Similarly, a U.S. company acting as data controller that is not present in the EU but is using servers in the UK will also be subject to the DPA. Likewise, the DPA will apply to a UK company acting as data controller and using servers in India to process personal data relating to the activity of the UK company.

The Purpose of Processing. This is a key issue surrounding Big Data, as one of the most frequent practices is using data collected for one purpose (for example, after-sales service) for a different purpose (for example, consumer segmentation for marketing campaigns). Under the EU Directive, personal data must be collected for specified, explicit, and legitimate purposes, and the individual must have been informed of those purposes.

There is an exception: if the personal data was not collected from an individual but, for example, was provided by the data controller that originally collected the data, the subsequent data controller is not required to inform the individual if disproportional efforts would be required to do so. One challenge however is that data protection authorities across the EU have varying ideas about what constitutes a "disproportional effort." A telephone directory service in France was sanctioned by the French data-protection authority (CNIL) for having failed to notify social network users that their data posted on the network might be used by the directory.[3]

The 28 EU data-protection authorities, assembled under Article 29 Working Party and referred to as the "G29," consider that informing individuals of very broad purposes—such as "improving users' experience," "marketing functions," or even "IT security purposes"—does not meet the requirements of the Directive.[4] Although this view is not binding, the trend in the EU is clearly toward providing more and clearer information to individuals.

CASE EXAMPLE

A bank owns and operates an insurance subsidiary, with which it shares the same branch network. The bank wants to use bank customer data to target those customers when promoting the insurance subsidiary's products.

Practical Considerations

- The bank's customers may need to have expressly consented to receiving commercial solicitations for services that are not banking services.
- Bank secrecy laws may require customers to expressly consent to sharing of customer data between the bank and the insurance subsidiary.
- In principle, an unsubscribe link must be included in commercial e-mail solicitations, even when the customer has consented to receive such solicitations.

Changing the Purpose of Processing. As noted earlier, the Directive states that personal data must be collected for specified, explicit, and legitimate purposes and not be further processed in a way incompatible with those purposes. The data controller must provide, at the time the data is collected, information about the purposes of processing, and, in some cases, must also obtain the individual's consent to processing.

To further protect personal data, registration with the relevant national data-protection authority may be required. In France, this requirement means, in practice, that *each type of purpose* must be registered. In Spain, each database must be registered with the Spanish data-protection authority (AEDP). In the UK, the data controller must be registered with the Information Commissioner's Office (ICO). However, in Germany, there is generally no registration requirement.

Said differently, in some EU countries, any alteration of the purposes for which data is processed can trigger new notice requirements and possibly cause a new registration with the data protection authority, as well as other obligations in terms of confidentiality and security.

CASE EXAMPLE

An insurance company offers a car insurance policy at an attractive price, provided it can collect, through onboard measurement devices, data on the car's location and data on the driver's behavior (such as acceleration, speed, and so forth) in order to encourage safe driving practices.

Practical Considerations

- Some data-protection authorities may consider that collecting data on traffic offenses is incompatible with restrictions in the Data Protection Directive on the collection of criminal-record data.

Fair and Lawful Data Collection. With so much data available on the Internet, it may seem that data is accessible and free for harvesting. But freely available data is still covered by the EU Directive, and the data controller is still responsible for collecting it in a fair and lawful manner.

Data protection laws also apply when data is made available in the public domain—even when individuals make their personal data publicly available. In particular, notice requirements will still apply as will obligations to allow the individual to object to the processing of his or her data.[5]

Freely Given and Informed Consent. In principle, personal data can be processed only with the individual's consent, unless an exception applies. Depending on the local law and the type of data collected, implicit consent may be sufficient, or consent may have to be unambiguous, and in some cases it has to be explicit.[6]

In all cases, consent must be freely given and informed. The data controller is responsible for ensuring that the individual can understand the key aspects of personal data collection and processing, including the type of data collected, the purposes of data processing, the recipients of the data, the rights of the individual to correct and delete data, and the conditions under which the data could potentially be transferred outside the EU.

This point might be a source of potential conflict between companies and their consumers. A 2013 study conducted by 20 national data-protection authorities concluded that information given to individuals on websites is often insufficient: 20 percent of the leading global websites, and 50 percent of mobile apps, do not provide information on the type of personal data processing they conduct, meaning that informed consent from users is not possible.[7] The G29 reached a similar conclusion regarding mobile apps for phones and tablets, finding that a majority of apps do not provide adequate information to individuals about the processing of their personal data.

All in all, regulators in six European countries—France, Germany, Britain, Italy, Spain, and the Netherlands—have opened investigations into Google after the consolidation of its 60 privacy policies into one and after it started combining data collected on individual users across its various services (Gmail, Google Maps, YouTube, and so forth). Two EU data-protection authorities fined Google for insufficiently informing users about how it combines data from its different services. Google later modified its privacy notice.[8]

CASE EXAMPLE

To improve targeting, a French retailer credits a customer's loyalty card with purchases made using the payment card associated with the loyalty account, even if the customer does not use the loyalty card at checkout. The customer's loyalty points are therefore increased.

Practical Considerations

- The French data-protection authority, the CNIL, issued a recommendation on November 14, 2013, related to the processing of payment card data in connection with distance sales. The CNIL's recommendations on the lawful use of payment card data are very restrictive and do *not* include the use of a payment card number as a commercial identifier.

CASE EXAMPLE

A telecom operator creates an advertising agency to sell to third parties its customer contact data (such as name and address) as well as aggregated profiling data (such as location, minutes used, and frequency of calls). Having such sociodemographic data will enable third parties to more precisely target their advertising and marketing campaigns.

Practical Considerations

- In addition to general data-protection rules, the telecom operator is subject to specific rules deriving from EU Directives applying to the processing of location data and traffic data.
- Location data may be processed by the telecom operator and transferred to third parties offering value-added services, provided that (i) location data has been anonymized or (ii) the telecom operator obtained prior express and informed consent from the customers.
- Traffic data may be processed by the telecom operator to allow it to provide value-added services, provided that it obtained prior express and informed consent of the customers. However, such traffic data must be anonymized before it is transferred to third parties.
- For the EU data-protection authorities, anonymization implies that there is no possibility of re-identification. Simple aggregation is not enough.
- Customers must be given the option to withdraw their consent to processing traffic and location data at any time, easily, and free of charge.

The Data Retention Period. The EU Directive requires that data be retained only for so long as is necessary given the purposes for which it was collected. Data retention should, therefore, be limited. In addition, each country may impose legal provisions that specify

minimum or maximum retention periods for certain types of data. Local data-protection authorities also make recommendations as to the proper retention periods.

Anonymization. Data protection laws govern only data (such as name, identification number, or a series of characteristics that are unique to an individual) that can directly or indirectly identify a natural person. Therefore, if the data processed is genuinely anonymous, data protection laws do not apply.

However, there is no single legal definition of anonymous data, and data protection authorities across the EU have differing views of when data can be considered anonymous.

- The EU Directive states that all the means "likely reasonably to be used either by the data controller or by any other person" to identify an individual must be taken into consideration to determine if the data is anonymous.

- For the G29, if, after taking into account all the means of anonymization, the possibility of identifying a person does not exist or is *negligible*, the person should not be considered as identifiable.[9]

- The UK's Data Protection Act of 1998 states that personal data relates to a living individual who can be identified from the data and other information that is in the possession of, or is *likely* to come into the possession of, the data controller.

- In France, CNIL does not consider whether means are "likely reasonable" to be used to identify individuals. Instead, the data controller must examine whether it is theoretically possible (even if highly improbable) that an individual can be directly or indirectly identified using other data or means anywhere in the world. Accordingly, only irreversible anonymization is sufficient to take data out of the purview of French data-protection law. However, irreversible anonymization is not always feasible, particularly with the onset of massive databases from a wide variety of sources.

Consequently, in many instances anonymization depends on very specific circumstances. In the UK, it is possible to identify an individual on the basis of only a postal code, as some codes correspond to a sole resident, whereas in France, a postal code might be shared by more than 200,000 people.

The G29 has proposed the following three criteria for determining whether an anonymization method is sufficient:[10]

- *Singling out*, which corresponds to the possibility of isolating some or all records that identify an individual in a dataset

- *Linkability*, which is the ability to link at least two records concerning the same individual or a group of individuals (either in the same database or in two databases)

- *Inference*, which is the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes

If one of these three criteria is not satisfied, the G29 advises that the data controller undertakes a detailed analysis of the risk of re-identification of the individuals.

CASE EXAMPLE

A mobile phone operator wants to promote a new offer for international calls. It launches a marketing campaign that targets all of its customers who make frequent international calls over a period of three months.

Practical Considerations

- Customers of the mobile phone operator must be informed, for example, through their subscription terms or the operator's privacy policy, that they may receive commercial solicitations from their operator.
- In addition, the mobile phone operator is subject to specific rules applying to processing of traffic data for the purpose of marketing electronic communications services.
- The mobile phone operator may process customers' traffic data in order to determine which customers are likely to be interested by this offer, provided that it has obtained customers' express and duly informed consent and that traffic data is processed only to the extent and for the period necessary for the marketing of this offer.
- Customers must be given the possibility to withdraw their consent to processing traffic data at any time, easily, and free of charge.

CASE EXAMPLE

An e-commerce website engages in a partnership with an insurance company, in which the site sends a real-time alert to the insurer when a customer purchases a good that may need to be insured (for example, a high-tech product).

Practical Considerations

- The express and informed consent of the website's customers must be obtained before any personal data is shared with the insurer.
- The website needs to ensure that the data shared with the insurer is relevant, appropriate, and nonexcessive.
- In principle, an unsubscribe link must be included in commercial e-mail solicitations, even when the customer has consented to receive such solicitations.

Security. Security obligations weigh on data controllers and their processors. Security is increasingly as critical for business as it is for governments. The EU Directive requires data controllers to implement technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access (particularly when the processing involves the transmission of data over a network), and against all other unlawful forms of processing. Processors acting on behalf of data controllers must offer sufficient guarantees to ensure data security.

CASE EXAMPLE

A mobile phone operator wants to analyze the data of its former customers and target those who may be interested in a new commercial offer (for example, customers who, according to the analysis, may have terminated their subscriptions because they exceeded their minutes too often and may be interested in unlimited minutes).

Practical Considerations

- The mobile phone operator is subject to specific rules applying to processing traffic data for the purpose of marketing electronic communications services. The mobile phone operator will need to make sure that (i) it has obtained customers' express and informed consent to process their traffic data and (ii) traffic data is processed only to the extent and for the period necessary for the marketing of the new commercial offer.
- In addition, the operator will have to verify that targeted customers have terminated their subscriptions with the operator less than three years ago.

In addition to these general-security requirements of the EU Directive, many countries (notably Spain, Italy, and Germany) have adopted specific data-security requirements in their national data-protection laws. Violations may be met with specific criminal-law sanctions.

Furthermore, some specific laws and security requirements apply to certain industries, such as telecom operators, banks, and those that process health data.

For example, telecom operators and their personnel are bound to respect the confidentiality of subscriber communications. Data concerning telecom traffic (for example, Internet protocol addresses or other data related to telecom connections) can be used only by operators to market their own services, prepare invoices, and, with the subscriber's consent, provide value-added services. Localization data can only be used to transmit communications; once the communication has ended, the use of localization data requires the subscriber's consent.

Similarly, banks and their employees may be bound by bank secrecy laws—for example, laws that prohibit any disclosure of a customer's account data to third parties, except where express consent is obtained.[12]

Database Protection. In addition to data privacy concerns, laws protecting the use of databases may also come into play. Database creators may find their work protected not only by copyright but also by *sui generis* rights in a database. When the compiling, verification, and presentation of a database attest to a substantial qualitative or quantitative investment,[11] the database is protected by law. The person claiming the protection must demonstrate, for example, an investment in purchasing or leasing servers to process the database content, in data processing and storage capacity, and in hiring personnel to build, develop, and maintain the database.

The creator of a database can bring a claim against any third party that substantially extracts database content or reuses it in any form. Whether an extraction is "substantial" will depend on the exact circumstances of each case, but typically a court will look to whether the parties are competitors, the nature of the extracted data, the availability of the extracted data from other sources, and so forth. The notion of data reuse can be quite broad, covering any nonauthorized use that is intended to disclose to the public any or all of the content included in the database. For Big Data actors, the takeaway is that obtaining explicit authorization before using a third party's database is paramount.

THE FORTHCOMING EU DATA PROTECTION REGULATION

As we go to press, the new EU Data Protection Regulation, which will replace the Directive, has not yet been finalized.

Some of the main points being reviewed are the following:

- The formal definition of personal data will be broadened to include an individual's identification number, location data, and online identifier.
- The Regulation will have broader application, adopting a consumer-law approach so that EU data-protection laws will apply to businesses that sell online to EU residents.
- When consent from an individual is required, it will have to be explicit; implicit consent will no longer be considered as unambiguous and thus will not be sufficient.
- The right to be forgotten, already recognized by the European Court of Justice in its May 13, 2014, decision in the Google case, will be enshrined in a legislative act.
- Naming a data protection officer will become mandatory for a defined class of businesses.
- Data breaches will need to be notified to the data protection authority.
- Data processing that may pose particular risks to individuals' privacy must be analyzed—by conducting a privacy impact assessment—before being implemented.
- Sanctions will be similar to those imposed in antitrust cases—that is, a percentage of worldwide revenue.

The Regulation will affect all data controllers and processors, but certain provisions could have an outsized impact on organizations dealing with Big Data. For example, the requirement for explicit consent may multiply requests for consent. This in turn could lead to constant notices and requests for consent, thus overwhelming users, or to an impoverishment of available data, thus impacting the value created by analysis, or to both. Any of these phenomena will increase administrative burden for data controllers and reduce innovation and future business opportunities.

Appointing an experienced data-protection officer, or conducting privacy

impact assessments, will mean increased costs for some data controllers but may also encourage practices that help build consumer trust. The forthcoming Regulation could therefore threaten certain data monetization strategies but, simultaneously, encourage processing methods that enhance consumer trust.

Earning Consumer Trust with Win-Win Propositions

Innovating within the boundaries of the regulatory and legislative environment is not always easy. Gaining consumer trust is a necessary condition; it may not be a sufficient one. Finding a win-win proposition with a fair value exchange between the consumer and business will be the key to success.

Sharing value can be explicit, such as providing data in exchange for payment, as already happens on some data-purchasing websites. Sharing value can also be implicit, which happens when businesses rely on in-kind advantages, such as loyalty cards or reduction coupons. And the value exchange may be nuanced; Facebook, for example, provides free services in exchange for massive monetization of user data, without explicit acknowledgment.

Guaranteeing confidentiality and data security, ensuring transparency, and allowing consumer control over data are clearly an important part of this value exchange.

The pace of technological development and the increased awareness on consumer privacy will have a significant impact on Big Data's perception, at least until it reaches maturity. The winning strategy for businesses using Big Data will be to regularly monitor legal and cultural changes as well as adapt to new behaviors and consumer practices, all while encouraging technological innovation.

Ten Risk-Mitigation Practices for a Big-Data Project

1. Use anonymous data whenever possible.
2. Obtain informed consumer consent when collecting personal data.
3. Ensure that profiling does not create any discrimination among consumers.
4. Be transparent about the reasons for collecting data.
5. Ensure data is correct—and secure—at all times.
6. Make tools available to consumers, offering control over their data.
7. Abide by data-retention rules if data is not anonymous.
8. Do not use data that seems freely available without analyzing the legal risks.
9. Communicate the value proposition for consumers.
10. Do not use third-party database content without authorization.

NOTES

1. *The Trust Advantage: How to Win with Big Data*, BCG Focus, November 2013.
2. Source: EU Directive 95/46/EC
3. CNIL decision No. 2011-203, dated September 21, 2011, ordered the publication of an official warning to the directory.
4. G29's "Opinion 03/2013 on Purpose Limitation." The G29 was created by the EU Directive. The G29 has no direct enforcement authority, but its opinions may carry weight with national data-protection authorities and national courts.
5. CNIL decision No. 2009-148, dated February 26, 2009, is instructive in this regard; a company collecting public real-estate announcements was ordered to pay a fine.
6. G29's "Opinion 15/2011 on Consent."
7. "Internet Sweep Day: The First World-wide Evaluation of Privacy Notices for Internet Users," CNIL, August 13, 2013, http://www.cnil.fr/linstitution/actualite/article/article/operation-internet-sweep-day-une-premiere-mondiale-visant-a-apprecier-le-niveau-dinformat/.
8. The changes were effective on March 31, 2014, http://www.google.fr/intl/fr/policies/privacy/.
9. G29's "Opinion 4/2007 on the Concept of Personal Data."
10. G29's "Opinion 5/2014 on Anonymization Techniques."
11. Compare with French Monetary and Financial Code, Article L. 511-33.
12. Article 7 of Directive 96/9/CE, dated March 11, 1996.

Authors

DLA Piper
Carol Umhoefer, Partner
carol.umhoefer@dlapiper.com

Jonathan Rofé, Counsel
jonathan.rofe@dlapiper.com

Stéphane Lemarchand, Partner
stephane.lemarchand@dlapiper.com

The Boston Consulting Group
Elias Baltassis, Director
baltassis.elias@bcg.com

François Stragier, Associate Director
stragier.francois@bcg.com

Nicolas Telle, Project Leader
telle.nicolas@bcg.com

DLA Piper

With 4,200 lawyers in more than 30 countries spanning all regions of the globe, DLA Piper is your partner of choice wherever in the world you do business. In France, DLA Piper has more than 140 lawyers, including 40 partners. We advise multinationals, banks, and investment funds on all legal issues that businesses face, including corporate, tax, finance, employment, litigation, regulatory, and real estate matters.

DLA Piper's Intellectual Property & Technology practice in France has 22 lawyers, 7 of whom are partners. The practice works closely with our global group of more than 400 IPT lawyers across the world. The team in France is consistently ranked as a leading practice and is one of the largest in the market that handles both contentious and non-contentious matters involving the entire breadth of IP and IT issues, including outsourcing, innovative technologies, data privacy and security and related compliance issues, patents, trademarks, designs, copyright, telecommunications, electronic communications, commercial contracts, and distribution and marketing, for clients operating in a wide spectrum of sectors, such as IT services, e-commerce, and media.

The Boston Consulting Group (BCG)

The Boston Consulting Group (BCG) is a global management consulting firm and the world's lead ing 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 81 offices in 45 countries. To find the latest BCG content and register to receive e-alerts on this topic or others, please visit *bcgperspectives.com*.


BCG
The Boston Consulting Group


DLA PIPER