RESTORING TRUST in Big Data
Bureau Veritas operates solely as an independent certification and auditing organization and offers to help businesses create a global certification system to protect personal data.

Bureau Veritas will offer three levels of certification:

"Privacy Checked/Privacy by Design" Certification
- Awards businesses a "Privacy by Design" label for using a specific product or service design, a data architecture, and de-identification or similar methods.
- Lets businesses begin the privacy certification process without redoing their entire IT architecture.
- Is more accessible for some businesses.

Governance Certification
- An international label — independent of local compliance requirements.
- Focuses on the data management system, without technical audits of resources.
- Sets up a continuous improvement process for data privacy.
- Can be tailored along the lines of the corporate social responsibility (CSR) model.
- Applies to all types of businesses.

European Union Regulation (GDPR) Certification
- Addresses Article 42 of the E.U. General Data Protection Regulation.
- Is awarded based on guidance derived from the regulation.
- Voluntary certification for businesses.

The internal audited processes relate to data governance.

Bureau Veritas certification's model will vary by region, scope of business and a company's organization.

Data is everywhere. It promises to bring us foresight, efficiency and customized services. But the misuse of data by many businesses has created a climate of distrust. People feel it is beyond their control. How can we restore trust? How can we take advantage of the potential conveniences of connected cars, smart buildings and personalized health care?

Businesses are endeavoring to provide technological solutions — by strengthening security for example. Governments are attempting to impose a legal framework. Worthy initiatives such as charters and guidelines are emerging to provide for more communication and transparency. Many businesses are adopting an approach known as "Privacy by Design" for their new products and services.

However, such strategies will not prove effective unless the public is aware of their existence and finds them credible as a means of protecting personal privacy.

In that regard, only an independent third party can legitimately verify that businesses are complying with the rules of ethics.

Bureau Veritas, a world leader in testing, inspection and certification services, is now offering help to businesses in every industry as they pledge their support for rigorous, transparent privacy protection. We are working with major players across the data value chain, to help them plan ahead for privacy-friendly solutions and refine their handling of personal data.

Bureau Veritas is offering a suite of certifications and labels to ensure transparency and the proper use of personal data.

Today we are helping to establish privacy as a major opportunity for businesses astute enough to seize it. Corporate digital responsibility is shaping up as a major challenge for the future.

PHILIPPE LANTERNIER
Executive Vice President, Chief Development Officer
Bureau Veritas
PERSONAL DATA: CONSUMERS & BUSINESSES ARE LOGICALLY INCONSISTENT

CONSUMERS SAY THAT THEY ARE CONCERNED ABOUT HOW THEIR PERSONAL DATA IS USED...

One-third of Internet users in the United States have had their personal data misused in the past year.

The most sensitive data in their minds is related to their:
- Location (82%)
- Health (81%)
- Browsing history (70%)
- Communications with friends (68%)

More than 80% (81% in France and 88% in the United States) are afraid their data will be stolen or misused.

They are afraid of being inundated with ads (87%), unable to erase their digital footprint, e.g. exercise their right to be forgotten (85%), and being a victim of bank information (77%) or identity theft (75%).

One-third of Internet users in France think that service providers can use their data (54% believe that their consent is not required).

...BUT PARADOXICALLY, MOST AGREE TO SHARE THEIR DATA

92% of Internet users in France agree that service providers can use their data so that they can access new digital services.

Consumers surveyed worldwide expect:
- 100% a financial reward
- 89% significant discounts
- 65% customer loyalty points

MANY OF THEM HAVE STARTED TO ANALYZE IT

$130 billion spent in 2016 on data and business analytics.

In 2013, 44% of businesses in North America did not yet have a data use policy.

In France, only 16,000 e-commerce, government and other organizations have appointed an official data privacy advocate, despite the fact that e-commerce alone accounts for around 200,000 active retailing sites.

ALL BUSINESSES COLLECT DATA...

MOST ONLINE BUSINESSES COLLECT DATA
- Visits
- Profiles
- Payment

...BUT FEW HAVE A REAL DATA GOVERNANCE SYSTEM

INTERNET USERS SENSE DANGER
- Credit cards: 38%
- Phone companies: 31%
- Email service providers: 29%
- Online merchants: 26%
- Search engines: 16%
- Web marketers: 7%

Bureau Veritas — Restoring Trust in Big Data
INDEPENDENT CERTIFICATION IS THE ONLY WAY TO RESTORE TRUST

BUSINESSES THEMSELVES TRY TO PUT A POSITIVE SPIN ON THINGS

Most post a “soft” privacy policy on line, which only 10% of Internet users who sign up with them read in full.

A few big companies publish ethics charters and guidelines. - Source: CML

REGULATIONS WILL SOON FORCE THEM TO GET ORGANIZED

In the United States, the draft Consumer Privacy Bill of Rights has been introduced twice already.

In the European Union, the General Data Protection Regulation (GDPR) was adopted in April 2016 and enshrines stronger obligations by 2018. Right to be forgotten, data portability, mandatory notification of personal data breach, including for data transferred outside Europe (fines of up to 4% of worldwide annual revenues).

Problem: 92% of businesses in France, Germany and the United Kingdom are concerned that they won’t be ready for 2018.

Regardless, consumers feel that complying with regulations is the bare minimum.

HOWEVER, ONLY CERTIFICATION OF GOOD DATA MANAGEMENT SEEMS LIKE THE RIGHT APPROACH

- Understandable to the public
- Made credible by the market
- Adaptable and open-ended
- Deployable internationally
- Several certification levels can be awarded: product, business, contractors

SUCH CERTIFICATION WILL HAVE TO BE AWARDED BY AN INDEPENDENT ORGANIZATION, WITH:

- Credibility
- Impartiality
- An unblemished reputation
- Transparent analytics tools
- The ability to support the certification label

PRIVACY CERTIFIED

which only 10% of Internet users who sign up with them read in full.

A few big companies publish ethics charters and guidelines. - Source: CML

In the United States, the draft Consumer Privacy Bill of Rights has been introduced twice already.

In the European Union, the General Data Protection Regulation (GDPR) was adopted in April 2016 and enshrines stronger obligations by 2018. Right to be forgotten, data portability, mandatory notification of personal data breach, including for data transferred outside Europe (fines of up to 4% of worldwide annual revenues).

Problem: 92% of businesses in France, Germany and the United Kingdom are concerned that they won’t be ready for 2018.

Regardless, consumers feel that complying with regulations is the bare minimum.

HOWEVER, ONLY CERTIFICATION OF GOOD DATA MANAGEMENT SEEMS LIKE THE RIGHT APPROACH

- Understandable to the public
- Made credible by the market
- Adaptable and open-ended
- Deployable internationally
- Several certification levels can be awarded: product, business, contractors

SUCH CERTIFICATION WILL HAVE TO BE AWARDED BY AN INDEPENDENT ORGANIZATION, WITH:

- Credibility
- Impartiality
- An unblemished reputation
- Transparent analytics tools
- The ability to support the certification label

PRIVACY CERTIFIED
Data is everywhere. It promises to bring us foresight, efficiency and customized services. Because when we talk about data, we are specifically talking about the personal data that every business today wants to collect on its own customers and the market in general. But instead of helping consumers build a closer relationship with their brands, some businesses have used personal data in a way that makes headlines, ultimately breeding a climate of mistrust. And, of course, governments themselves have sparked similar controversy, as we have seen in a number of high-profile cases.

How can we restore trust? What steps can we take to ensure that consumers and the public at large do not stand in the way of potential conveniences like networked cars, smart buildings and personalized health care? Big data is appealing yet it is also intimidating. Storage capacity, immediate processing, omnipresent information — it is a complicated business, and individuals can easily come to feel it is beyond their control.

Businesses are endeavoring to provide technological solutions — by strengthening security, for example. Governments are attempting to impose a legal framework. Worthy initiatives are emerging to provide for more communication and transparency, or to gradually educate the public on how to master available tools for protecting their personal lives more effectively. Many businesses looking to introduce new products or services are adopting an approach known as “Privacy by Design,” in which options or tools for less intrusive use of personal data are incorporated into the design process.

However, such strategies will not prove effective unless the public is aware of their existence and finds them credible as a means of protecting personal privacy. In that regard, only an independent third party can legitimately verify that businesses are complying with ethical principles.

Corporate digital responsibility is shaping up as a major challenge for the future. Bureau Veritas, a world leader in testing, inspection and certification, is now offering to help businesses in every industry as they pledge their support for stringent, transparent privacy protection, by introducing a suite of labels.

INDEPENDENT CERTIFICATION IS THE ONLY WAY TO RESTORE TRUST IN PERSONAL DATA USE

SECURITY, REGULATION, PRIVACY BY DESIGN — SUCH STRATEGIES WILL NOT PROVE EFFECTIVE UNLESS THE PUBLIC IS AWARE OF THEIR EXISTENCE AND FINDS THEM CREDIBLE.

$130 billion were spent on data and business analytics in 2016. How much was spent on reassuring consumers?
MORE DATA EQUALS LESS TRUST

WEB USERS ARE CONCERNED ABOUT HOW THEIR DATA IS USED

These days, every business seeking to retain its market share is trumpeting innovation as the solution. The bulk of today’s innovations involve digital services. Yet 80 to 90% of the public, depending on the country, say they are concerned about protecting their personal data — and the situation is growing worse by the day. Some 60% of those surveyed acknowledge that their concerns have risen in recent years.

This trend toward greater mistrust has been spurred in part by a number of recent events. The Snowden leaks in 2013 revealed how governments spy on ordinary citizens, and not just in the United States. Other news stories involving the private sector have revealed significant data breaches or ethical lapses in the relationships forged with customers.

In a world where data has come to be viewed as “the oil of the 21st century,” this is a critical issue. Big data has barely gotten off the ground, and “the personal data issue” is already starting to sow concern. Clearly, what is most at stake in the relationship among businesses, institutions, brands and the public is the matter of trust.

The risk to companies is high — and they know it. Because consumers are no longer just concerned about whether their data is protected against hacking, for example. They also want to know how businesses are using their data. On the spectrum of risks posed by the web security issues are no longer generating the most concern: identity theft and hacking of financial data are deemed possible (75% and 77% respectively), but less likely than being inundated with advertising (87%), lack of respect for privacy (85%) and being unable to erase data that has been shared (85%).

How can companies continue to develop new, more customized services if the percentage of customers who consent to the use of their location data in exchange for certain benefits has fallen by half in just two years?

80 to 90% of people in France and the United States say they are afraid their data will be stolen or misused

Governments and institutions are also grappling with the topic from a regulatory standpoint.

Naturally, their response has been to adopt policies mandating that businesses provide a high level of data protection. In April 2016, the European Union adopted its new General Data Protection Regulation (GDPR), which enshrines new consumer rights, including the right to be forgotten (also known as the right to erase) and the right to portability. It also gives individuals greater control over their personal data. In the United States, draft legislation dubbed the Consumer Privacy Bill of Rights was reintroduced in March 2015. In Canada, privacy principles have been reintroduced in March 2015. In Canada, privacy principles have been reintroduced in March 2015.

The issue of consumer trust is, ultimately, more difficult to reconcile. The most common response has been to identify personalized, value-added services that can convince customers of the tangible benefit to be gained by handing over their personal data. Other strategies including publishing charts and guidelines, educating consumers or making a verbal commitment. But this can reveal new fault lines even within a single company: between the Marketing and Legal departments, for example, or between the Business Intelligence unit and Customer Relations. Marketing departments may include some who want to preserve the brand and stay one step ahead of potential hackers, using both technology (encryption, firewalls, etc.) and organizational resources. Their efforts have not been failsafe, but, as the example of online payment shows, technology can provide credible solutions for addressing consumer concerns.

Various tools, which include 3D Secure authentication, have undoubtedly made the identification process more reliable. The boom in online retailing is clear evidence of that.

In the face of competing demands, how can businesses regain trust and also maintain their ability to capitalize on their customer knowledge in order to safeguard their market share and future growth?
DATA PRIVACY IS AN AGE-OLD CONCERN; IT IS THE BUSINESS MODEL THAT IS BOOMING

Our digital footprints are multiplying.

The major tenets of personal data protection are much the same worldwide. We tend to think that certain governments are more permissive than others, but in substance, the same principles are always at work. The most recent changes in the European Union’s GDPR regulation, such as the right to be forgotten and explicit consent, shed light on emerging concerns about data privacy protection. Because if we have always been following the same principles for protecting consumer privacy, what has changed now? Customer records have been kept since retailing began; the mail-order sales and relationship marketing of the 20th century were, after all, based on detailed customer knowledge. Protection of personal data was already standard practice among businesses. These days, it is not just the scale, but also the technology and the aims behind the collection of personal data that have changed. Each of us is conscious of having provided data voluntarily to certain business partners, whom we could readily identify. By contrast, web browsing, geolocation, online transactions and the like have opened the door to an entirely passive form of data acquisition, in which consent is initially requested in some cases and in others not at all. In the face of this explosion of data from the use of mobile phones, Internet browsers and even our cars, thermostats and televisions, the very notion of a digital footprint is open to question. These multiple digital traces, so difficult to track and erase, correspond to a whole category of private data that is especially tricky to control.

Businesses are now accumulating data on a massive scale. The diminishing cost of storage capacity and the increase in network performance and computing power have paved the way for high-volume data analysis. Any data on how a service is used or how a customer behaves, regardless of the context, can potentially generate knowledge and hence value. Analytics technology – big data – exists to identify patterns in, and lend meaning to, this mass of unstructured data. And that is exactly the concern. We tend to lose sight of why data should be collected. Our current approach to personal data is based on the idea that it generates value – but in a way that is difficult to anticipate at the moment when the company receives it from the customer. Yes, there is growing demand for more personalized services, and consumers often welcome the buying recommendations they receive at e-commerce sites. But there are significant questions about the volume of personal data that each of us provides by way of connected health devices, private messaging or the sensors now installed in our homes – this data seems to be collected for inconstant purposes.

Data is often collected without any knowledge of how it will be used.

The entire chain of service providers needs to be secured as well.

- The businesses in direct contact with customers are making the biggest commitment. They have to explain clearly why they are collecting the data, obtain consent, provide reassurance about the security measures they have implemented and coordinate measures to notify their customers. They are the ones who define a corporate data mining strategy and decide exactly how the data will be processed (anonymous versus personalized, statistics versus individualized, etc.). Naturally, they also bear responsibility for the quality of their data management, not to mention the potential harm to their image in the event of a breach.

- Data hosting providers partner with those businesses directly to store their data. Some of these providers specialize in specific sectors, such as healthcare data, they may be industry behemoths like Amazon and Microsoft or small players. They ensure that data is secure and accessible for processing purposes, and they sometimes structure data as well. Their entire business model is based on the service they provide to their clients. Trust and reliability are essential – indeed, critical to their long-term survival.

- The groups that ultimately use the analytical results – or even the raw data – are generally inside the company: the Marketing department uses the findings from big data analytics to formulate new services, the Customer Service department can send personalized messages to customers in real time, and so on. This very link in the chain is designed to create value added for the customer – after a fairly lengthy detour.

The groups that ultimately use the analytical results – or even the raw data – are generally inside the company: the Marketing department uses the findings from big data analytics to formulate new services, the Customer Service department can send personalized messages to customers in real time, and so on. This very link in the chain is designed to create value added for the customer – after a fairly lengthy detour.

- Data analysts are responsible for data intelligence. These are generally outside firms, although an internal business intelligence unit guides their work. Their primary focus is on research and performance. Their expertise is in statistics and algorithms – in other words, scientific in nature. Data analytics entails stringent ethical standards. If data anonymity can be rendered meaningless by complex algorithmic processing with today’s computing power and analytical finesse, it is possible to restrict the focus to a single individual.

With the reasons for data collection increasingly murky, it is all the more important for the public that its personal data be in the hands of businesses or institutions that it trusts. The fact is, however, that the number of links in the personal data value chain is increasing. We may say we trust a company to which we have surrendered our privacy, but in reality an entire ecosystem is at work.

When it comes to personal data, the entire data chain needs to be 100% consistent, from the service provider to the data host, the data processor and beyond. Although the questions about data privacy raised largely by an anxious public were initially targeted to B2C firms, they actually encompass a wide sphere of B2B services.
Bureau Veritas — Restoring Trust in Big Data

IN PROMOTING TRANSPARENCY

MAJOR RETAILERS AND PURE PLAYERS ARE VIEWED WITH THE SAME MISTRUST

Those who do launch new initiatives are fairly discreet about it. They are fearful of raising a splashy commitment only to be caught flat-footed later on, or they do not want to forestall the option of using personal data in the future to refine their offering and preserve operating latitude for subsequent business intelligence. However, 80% of the public say they are interested in tools to help them ‘manage their digital identity,’ and that number is growing from year to year.

Soon or later, every type of business will need to offer proof of its transparency, since each invites the same mistrust. The most powerful companies — the giants of the Internet — strike fear in consumers through their might and the enormous volume of data they wield. Paradoxically, the firms making the greatest effort to provide guarantees (as in WhatsApp’s recent decision to provide end-to-end encryption) are those most suspected of abuses. As for companies in the traditional economy, they generate fewer concerns about data, but they are running a real risk all the same, since they have not yet invested adequately in appropriate privacy management tools.

Could additional regulatory requirements offer a solution? They can certainly help. But more regulatory compliance is viewed as just a baseline, a bare minimum for which businesses no longer score points — although their reputation can be battered if they are found to be falling short. Studies have shown that the public expects institutions to do a better job of protecting consumers in the future. And that demand is undoubtedly being heard, particularly in Europe, where the E.U. is attempting to place strict guidelines on the use of data. But in the past, regulatory solutions have not been adequate to quiet concerns about practices by either digital sector giants or brick-and-mortar firms. Which are sometimes skewed for improper use of personal data.

On one hand, we have companies that would like to pledge respect for customer privacy when the personal data in their possession is so complex, including multiple layers of data managed by disparate fashion over time. In the other corner, we have digital pure players. These are companies that were designed around data management, either to provide services of various kinds (e-commerce, e-health, mobility, etc.) or because data is at the heart of their business model (e.g., Google, Facebook). Their data management is designed to be seamless: a single customer profile, a contextualized history and clearly identified categories of data. As a result, they can describe in detail how they process the data, they can set out their commitments to the public, and they can even provide interfaces that allow clients to manage certain privacy settings themselves. In theory, that could give them an advantage over businesses that have a less sophisticated knowledge of the issue. In practice, however, they also elicit significant mistrust.

REGULATIONS ALONE WILL NOT RESTORE TRUST

In the new digital age of globalized products and services, however, no company is immune from suspicion. The only solution is to ensure complete transparency, by a variety of means: explaining the company’s activities, offering every possible demonstration of proof. And highlighting the practical benefits for customers.
The right to privacy is a fundamental right. But like all fundamental rights, it needs to be applied, interpreted and circumscribed in light of real-life economic relationships, particularly in the digital sphere. It can sometimes seem as though legislators want to make data privacy an absolute right, in contrast to a more “liberal” view in which we wish to share or display.

It is here that a kind of implicit consensus has now emerged. We share large amounts of data with numerous brands, government organizations, and other entities in exchange for personalized services. In that unique relationship between an individual and a brand, mere compliance with even the most stringent regulations is no solution. It offers only minimal security, with no inherent value for the consumer; it carries no symbolic weight for the relationship. The only way to build trust is to provide the public with tools that go over and above the “legal minimum” — tools with which consumers can reassert control over their personal data and proactively redefine their relationship with each brand.

Today, data privacy is a component of every digital service offering. If you visit a website without identifying yourself, you will have access to only the most basic services. If you create a profile and then identify yourself at each visit, however, you will find content that is tailored to your presumed interests.

“Tacit consent is not always valid. The notion of a value exchange based on personal data would suggest that, in a basic economy, the public itself views personal data as equivalent in value to the benefits received from a service. Surveys show considerable ambivalence in this regard, as the public becomes more aware of the conflict between protecting your personal life and receiving customized services. Those who use a large number of services are caught between the immediate benefits available through greater customization and the potential future dangers posed by sharing sensitive data. In most cases, present needs outweigh future risks. But we may have subsequent regrets, which we then voice in opinion surveys by calling for greater data privacy protection, even in the face of our own day-to-day behavior. The ability to fine-tune our privacy settings may seem to offer one solution, in which each of us authorizes the use of our data in accordance with our own level of concern. It is hard to know what we desire. But we have clearly grasped that fact. To encourage us to share even more data, the most common strategy has been to identify personal value-added services that can convince customers of the tangible benefit to be gained by turning over their data. There are many examples of this businesses suggest products that might interest you. They anticipate your needs when you are organizing a vacation for example. They offer customized insurance policies that reflect your driving habits and personal profile, and so on. And, of course, the popularity of services offered at no charge reflects the tacit willingness of consumers to take advantage of services that make open use of their data, rather than choose a paid alternative.

Today, data privacy is a component of every digital service offering. If you visit a website without identifying yourself, you will have access to only the most basic services. If you create a profile and then identify yourself at each visit, however, you will find content that is tailored to your presumed interests.

Pinpointed and anticipated using algorithms, even unsolicited content such as product advertising or classified ads will be described as potential added value.

The prospect of tacit consent is not always valid. The notion of a value exchange based on personal data would suggest that, in a basic economy, the public itself views personal data as equivalent in value to the benefits received from a service. Surveys show considerable ambivalence on this regard, as the public becomes more aware of the conflict between protecting your personal life and receiving customized services. Those who use a large number of services are caught between the immediate benefits available through greater customization and the potential future dangers posed by sharing sensitive data. In most cases, present needs outweigh future risks. But we may have subsequent regrets, which we then voice in opinion surveys by calling for greater data privacy protection, even in the face of our own day-to-day behavior. The ability to fine-tune our privacy settings may seem to offer one solution, in which each of us authorizes the use of our data in accordance with our own level of concern.

We always regret sharing our data retropsectively. And businesses have clearly grasped that fact. To encourage us to share even more data, the most common strategy has been to identify personalized value-added services that can convince customers of the tangible benefit to be gained by turning over their data. There are many examples of this businesses suggest products that might interest you. They anticipate your needs when you are organizing a vacation for example. They offer customized insurance policies that reflect your driving habits and personal profile, and so on. And, of course, the popularity of services offered at no charge reflects the tacit willingness of consumers to take advantage of services that make open use of their data, rather than choose a paid alternative.

Today, data privacy is a component of every digital service offering. If you visit a website without identifying yourself, you will have access to only the most basic services. If you create a profile and then identify yourself at each visit, however, you will find content that is tailored to your presumed interests.

Pinpointed and anticipated using algorithms, even unsolicited content such as product advertising or classified ads will be described as potential added value.
DATA PRIVACY BY DESIGN: THE HOLY GRAIL

DATA PRIVACY NEEDS TO BE INTEGRAL TO THE DESIGN (BY DEFAULT)

The ability to calibrate precisely the level of privacy associated with each service requires a certain technical expertise that is not within every company’s grasp. Aside from structural solutions — reorganizing information within databases or operational complex procedures — companies have the option of offering privacy-enhancing technology. This technology, sometimes controlled by users themselves, or it may be installed by the company. It can be used for a variety of purposes: to anonymize data, minimize the amount of data collected or restrict the use or possession. Even when they can describe the nature of the personal data in their possession, can they describe precisely how it is structured? Have they sorted out the various “layers” of data acquired through various channels at different stages of the company’s growth, for instance after an acquisition? And have they determined what they want to do with that data? Have they determined what they are legally entitled to do? What benefits do they envisage? How will they proceed? What kind of process will they use? What types of action will they authorize, and will those actions be performed internally or externally? What precautions will they take? What resources (especially human resources) will they need? The task is much larger than simply ensuring that the company’s practices are in regulatory compliance.

IN THIS VIEW, DATA IS MANAGED LIKE AN ASSET

Beyond their technological implications, these two concepts have a significant impact on corporate management. Just as they manage their finances, their brand or their product or service portfolio, businesses must now manage their data, by treating it as an “asset” to be viewed through every possible lens. In the course of its life cycle (or use cycle), data passes through many hands, either in raw or processed form. So companies need to define some form of umbrella responsibility for that entire cycle, otherwise their privacy management will be disorganized and inconsistent and, ultimately, pose a greater risk.

This is because the first transformation needed is a cultural one. Businesses need to recognize internally that personal data generates added value, but only if it is managed according to best practices. Those best practices are not just technical (database reconciliation and consolidation, real-time incorporation of analytics, etc.), but ethical as well. Compliance with basic privacy guidelines must be the Chief Data Officer’s or the Data Protection Officer’s first order of business. This task will generally include a fundamental review of customer relationships and what they mean, corporate values, the company’s role in the community and so on.

The second transformation is organizational. It will encompass the process for developing new services, as well as the entire chain of events in the data life cycle, from collection to storage and processing. That too will affect a fairly wide range of business units within the company, but primarily those that make strategic use of data. Before the services are actually provided. New processes and procedures will need to be implemented in multiple areas, from business intelligence to product/service development, customer relations and technical project management. Each process or procedure must be defined in light of the ethical demands implicit in proper privacy management: minimize the volume of data collected, define how it will be used, notify the customer and so on.

The third transformation is very different. It involves the necessary process of monitoring the emergence of new tools for improved data management, integrating that technology into operating processes and procedures and introducing the necessary safeguards across the entire life cycle of personal data. This task is both technological and operational in scope. It has profound implications for how information systems are structured with regard to personal data. This technology watch is designed to ensure that the principle of privacy by design is upheld even after it has been incorporated into the digital service design process. While the first two transformations affect the entire company, and should provide a basis for guarantees regarding the data governance system as a whole, the third will be easier to apply project by project, department by department. It is easy to see how companies might pledge, in total confidence, to adhere to overarching organizational principles, define data management rules or establish oversight mechanisms. It is less easy to see how businesses would be able to claim, with 100% certainty, that their actual privacy protection is failsafe across all of their systems and databases, most currently including in subsidiaries. The pitfalls most commonly cited by IT executives involve their legacy information systems, plus — at multinational corporations — the need to ensure that all of their tools and methods worldwide are consistent.

WANTED: A CHIEF DATA OFFICER AND A DATA-CENTRIC ORGANIZATION

Businesses need to capitalize on these constraints by creating an internal position responsible for personal data, one that has both strategic and operational responsibilities for creating added value. In other words, the position needs to be proactive and constructive rather than defensive.

“Privacy must be the Chief Data Officer’s first order of business.”

The underlying assumption is that all of their tools and methods, whether internal or subcontractors are equally reliable in their commitment. If, for example, a service gives users the option of managing their own privacy settings, then each provider will immediately need to take account of any changes to those settings, e.g., regarding the use of personal data for marketing purposes (personalized e-mails, targeted advertising, etc.). The ecosystem of IT service providers is likely to begin offering such services across the entire data value chain. Soon it will be incumbent on data hosting providers, big data operators, publishers of analytics software and digital services firms to show that they are fully and openly adhering to best practices, so that their clients can in turn reassure the public. This will undoubtedly give rise to an entire slate of “privacy by design” services, enabling businesses that have adopted an ethical approach to privacy issues to stand out from their rivals and enhance their bottom line.

But all of this must still be put to the test. At a time when consumers are becoming more and more mistrustful, how can businesses make a credible claim to ethical handling of personal data? Here is where third parties can have a role to play, since they alone can objectively evaluate a commitment to privacy best practices.

THE ENTIRE PROCESSING CHAIN MUST FOLLOW SUIT

Businesses can certainly claim compliance with privacy principles as part of a given service, but only if all of their suppliers and subcontractors are equally reliable in their commitment. If, for example, a service gives users the option of managing their own privacy settings, then each provider will immediately need to take account of any changes to those settings, e.g., regarding the use of personal data for marketing purposes (personalized e-mails, targeted advertising, etc.). The ecosystem of IT service providers is likely to begin offering such services across the entire data value chain. Soon it will be incumbent on data hosting providers, big data operators, publishers of analytics software and digital services firms to show that they are fully and openly adhering to best practices, so that their clients can in turn reassure the public. This will undoubtedly give rise to an entire slate of “privacy by design” services, enabling businesses that have adopted an ethical approach to privacy issues to stand out from their rivals and enhance their bottom line.

But all of this must still be put to the test. At a time when consumers are becoming more and more mistrustful, how can businesses make a credible claim to ethical handling of personal data? Here is where third parties can have a role to play, since they alone can objectively evaluate a commitment to privacy best practices.
A certification and label serve as evidence that Bureau Veritas, the key is transparency. According to Edelman, the key is transparency. In concrete terms, that means announcing the results of audits and working with third parties such as governments and NGOs.

The EU’s General Data Protection Regulation encourages certification bodies, such as Bureau Veritas, to have a role to play. As an economic actor, a certification body is understood by the public. It has legitimacy conferred by the market: Certification is essentially transparent and can be deployed internationally.

Certification and labeling provide assurance of a commitment that goes beyond mere regulatory compliance, such as a pledge to “do better” over several years. These initiatives are considered voluntary by each company. In the eyes of stakeholders, their integrity is reflected in the products and services for which the businesses are seeking certification.

History suggests that private, voluntary certification is a forerunner to government standardization. And while that standardization is founded on prior consensus, private certification or labels generate consensus after the fact, based on how the label is used and recognized.

The Six Key Advantages of Certification

1. It has legitimacy conferred by the market: Certification can be established at the initiative of just a few industry firms, and acquired legitimacy by being adopted. The leading companies in their market will serve as models, with most competitors following in their wake.

2. It is immediately understandable by the public: One of the primary criticisms made of corporate data privacy protection is the complexity of corporate communication on the subject. Who can claim to have read all the endless terms and conditions of use of each company provided?

3. It is open-ended and spurs further progress: Certification can be the first step in a process of continuous improvement. It may include several levels of recognition, or become more stringent over time, or call for the adoption of new technical solutions. It defines a market standard, and in order to receive the industry’s endorsement, it needs to be appropriately discriminating without stifling innovation.

4. It can be deployed worldwide: A label is more suggestive of benefits for the user than regulatory compliance, since laws vary by country or region. As a result, it is the only strategy that can be effective on a multinational level.

5. It serves as proof of transparency and an indicator of the company’s performance. Any business that voluntarily seeks out certification is demonstrating transparency with regard to its internal processes and procedures. Certification provides customers and business partners with a guarantee of an organization’s actual level of performance.

6. It can provide insight into governance matters: Certification can serve as evidence that the company has established a structured process for handling its customers’ personal data. A continuous improvement loop—the basis for quality standards over the past 50 years—can be a powerful engine for strengthening corporate governance. That is the lesson that Bureau Veritas has drawn from the hundreds of thousands of audits it conducts each year.

PAPER TRUST

The key is transparency. According to Edelman, the key is transparency. In concrete terms, that means announcing the results of audits and working with third parties such as governments and NGOs.

The EU’s General Data Protection Regulation encourages certification bodies, such as Bureau Veritas, to have a role to play. As an economic actor, a certification body is understood by the public: It has legitimacy conferred by the market: Certification is essentially transparent and can be deployed internationally.

Certification and labeling provide assurance of a commitment that goes beyond mere regulatory compliance, such as a pledge to “do better” over several years. These initiatives are considered voluntary by each company. In the eyes of stakeholders, their integrity is reflected in the products and services for which the businesses are seeking certification.

History suggests that private, voluntary certification is a forerunner to government standardization. And while that standardization is founded on prior consensus, private certification or labels generate consensus after the fact, based on how the label is used and recognized.

The Six Key Advantages of Certification

1. It has legitimacy conferred by the market: Certification can be established at the initiative of just a few industry firms, and acquired legitimacy by being adopted. The leading companies in their market will serve as models, with most competitors following in their wake.

2. It is immediately understandable by the public: One of the primary criticisms made of corporate data privacy protection is the complexity of corporate communication on the subject. Who can claim to have read all the endless terms and conditions of use of each company provided?

3. It is open-ended and spurs further progress: Certification can be the first step in a process of continuous improvement. It may include several levels of recognition, or become more stringent over time, or call for the adoption of new technical solutions. It defines a market standard, and in order to receive the industry’s endorsement, it needs to be appropriately discriminating without stifling innovation.

4. It can be deployed worldwide: A label is more suggestive of benefits for the user than regulatory compliance, since laws vary by country or region. As a result, it is the only strategy that can be effective on a multinational level.

5. It serves as proof of transparency and an indicator of the company’s performance. Any business that voluntarily seeks out certification is demonstrating transparency with regard to its internal processes and procedures. Certification provides customers and business partners with a guarantee of an organization’s actual level of performance.

6. It can provide insight into governance matters: Certification can serve as evidence that the company has established a structured process for handling its customers’ personal data. A continuous improvement loop—the basis for quality standards over the past 50 years—can be a powerful engine for strengthening corporate governance. That is the lesson that Bureau Veritas has drawn from the hundreds of thousands of audits it conducts each year.

ONLY OUTSIDE CERTIFICATION CAN LEND CREDIBILITY TO A CORPORATE COMMITMENT

Certification represents a pledge for the future. It has legitimacy conferred by the market: Certification can be established at the initiative of just a few industry firms, and acquired legitimacy by being adopted. The leading companies in their market will serve as models, with most competitors following in their wake.

2. It is immediately understandable by the public: One of the primary criticisms made of corporate data privacy protection is the complexity of corporate communication on the subject. Who can claim to have read all the endless terms and conditions of use of each company provided?

3. It is open-ended and spurs further progress: Certification can be the first step in a process of continuous improvement. It may include several levels of recognition, or become more stringent over time, or call for the adoption of new technical solutions. It defines a market standard, and in order to receive the industry’s endorsement, it needs to be appropriately discriminating without stifling innovation.

4. It can be deployed worldwide: A label is more suggestive of benefits for the user than regulatory compliance, since laws vary by country or region. As a result, it is the only strategy that can be effective on a multinational level.

5. It serves as proof of transparency and an indicator of the company’s performance. Any business that voluntarily seeks out certification is demonstrating transparency with regard to its internal processes and procedures. Certification provides customers and business partners with a guarantee of an organization’s actual level of performance.

6. It can provide insight into governance matters: Certification can serve as evidence that the company has established a structured process for handling its customers’ personal data. A continuous improvement loop—the basis for quality standards over the past 50 years—can be a powerful engine for strengthening corporate governance. That is the lesson that Bureau Veritas has drawn from the hundreds of thousands of audits it conducts each year.

There should be multiple levels of data certification

Certification or labeling can be designed as a static system similar to compliance. Or it can be a dynamic process, driven by a commitment to do better in the future. This is an essential point for enhancing the visibility of corporate privacy practices. A label’s credibility will depend on its ability to provide total assurance regarding the guaranteed level of performance. If its aims are too broad or its criteria too stringent, it will be ineffective. Therefore, a label should include several “levels”:

- A “corporate” level, e.g., “a privacy best-in-class company”:

This refers to corporate data management and the procedures in place to educate, inform and gradually incorporate data privacy protection technology into company processes. It involves risk mitigation as it applies not to IS technology but rather to data processing by outside individuals or partners with defined roles and responsibilities within a chain of involvement. And, of course, corporate certification should indicate that the issue of privacy is addressed at the company’s top echelons and included in its existing charters, guidelines and declarations. A governance label of this kind can obviously be deployed on a broad, international scale, as is the case with other certification systems (such as CSR)

- A “product or service” label, e.g., “a privacy-by-design checked product/service”:

This label should indicate that a given product or service is truly privacy-compliant and that privacy protection was incorporated into its design from the outset. This includes the technology used for the product or service, its marketing, its application processes, and all partners and subcontractors.

- In addition, the E.U.’s GDPR defines obligations for all the parties in the processing chain, much like a traditional auditing initiative, in which the principal must pass on its own obligations to its subcontractors. In other words, we should refer to a label or certification system, rather than a single label.

We can refer to a label or certification system, rather than a single label. We can also see that one form of labeling is similar to a management audit, while another is actually a certification of a service.

Certification can only be awarded by a trusted third party

Some — indeed, many — labels already exist. More than fifty such labels are awarded in Europe alone, representing completely private or institutional initiatives. Some are based on national or international (e.g., E.U.) statutes, whereas others define their own list of criteria and best practices. Some include a legal audit, while others use a technical ‘audit’ for reporting purposes only. And some rely on an automated testing tool for identifying data security shortcomings. None fulfill the essential criterion of providing the public with clear, comprehensive information about the company’s personal data governance. The truth is that the multiplicity of labels can easily have the opposite effect: instead of restoring trust, it can lead to confusion.

Not every organization, whether public or private, has the authority or standing to establish a label. You do not become a trusted third party overnight. It requires some solid credentials:

- Legitimacy based on a genuine understanding of the industries you intend to audit or certify.

- An unblemished reputation, acquired over many years.

- Analytics tools and procedures that are completely transparent.

- Impartiality with regard to both businesses and governments.

- The backing of a strong international brand image for the label.

For any certification to be effective, its issuer — such as Bureau Veritas — must lend its own credibility to the company being certified. Trust in the certification body will be passed on to the recipient of that certification.
WELCOME TO THE AGE OF CORPORATE DIGITAL RESPONSIBILITY

The issue of data privacy poses immense challenges for businesses: consumers could lose confidence in the services they offer, their growth in certain industries could be hampered, they could lose the opportunity to provide high-added-value services, and so on. There is no doubt, for example, that e-commerce has been a critical factor in economic growth only because the banking and transaction processing ecosystems quickly addressed the issue of transaction security. Consumers now expect the same response from every company whose products or services involve the use of personal data. Data privacy has emerged as a key issue that companies in every industry, not just the digital sector, will have to confront in the future.

In that regard, the amount of thought and effort now being devoted to data privacy is comparable to what we have witnessed over the past 30 years in the area of corporate social responsibility (CSR).

Once viewed as a hindrance, CSR has come to be seen as an opportunity for businesses to improve their risk management, find potential cost savings in resource consumption (water, raw materials, energy) and waste treatment, create new avenues for promoting and communicating about the company, and stand out from potential rivals and more. CSR initially emerged as an informal undertaking that, over time, became more structured. It was accompanied by voluntary initiatives (codes of conduct, labels, etc.) that are now a familiar part of the landscape.

And ultimately it won formal recognition through dedicated standards – at the same time that laws and regulations governing the workplace, the environment, etc., were being adopted and implemented.

When it comes to meeting the challenges posed by privacy protection, regulations are necessary but not sufficient. They do not “speak” to the public. To restore trust, and simultaneously drive business expansion and economic growth, we need initiatives that allow consumers to feel they really are a central focus. By regaining control over their data and confident that the services they receive are rooted in a balanced, respectful relationship, consumers can once again, without misgivings, embrace the win-win proposition now offered by companies in every industry: managed access to their data in return for more customized services and greater value added.

The term “corporate digital responsibility” is now making its appearance. This responsibility may have several components (such as digital inclusion, for example) but it always encompasses protection of customer data privacy. Corporate digital responsibility spans multiple departments within the company. It also has strategic value and – like CSR – enhances each business’s market position.

The environmental aspects of a company’s CSR policy are not managed exclusively by its production departments, for example: indeed, in more and more companies, a CSR Director has overall responsibility for CSR affairs. Isn’t it reasonable then to assume that, in similar fashion, privacy matters could be placed in the hands of an internal overseer who wields authority across every corporate department and reports to the company’s highest executives? This is the future we envisage for corporate privacy protection, encompassed within CSR and viewed in the same light as the CSR issues that have made their way onto Executive Committee agendas in recent years. This change will happen over the medium term.

Practiced for more than 70 years and recognized around the world, voluntary certification is ideally suited to the digital economy’s needs and environment. As a globally recognized brand name in both the B2B and B2C sectors, Bureau Veritas aims to be the benchmark certification body in the field of data governance.

Bureau Veritas is introducing a certification service that can be adapted to companies in every industry, to help them ensure a smooth and secure digital transition.

With over 180 years of experience, Bureau Veritas supports companies in their commitment to transparency and continuous improvement in the eyes of their stakeholders. Our perspective on digital technology has opened our eyes to its extraordinary power to generate value and transform lives in the years to come. On the strength of our informed expertise, and mindful of our responsibilities as a trusted voice in the world of business, we are now helping to establish privacy as a major opportunity for businesses astute enough to seize it.

Bureau Veritas certification’s model will vary by region, scope of business and a company’s organization.

Bureau Veritas operates solely as an independent certification and auditing organization and offers to help businesses create a global certification system to protect personal data.

Bureau Veritas will offer three levels of certification:

**“Privacy Checked/Privacy by Design” Certification**
- Awards businesses a “Privacy by Design” label for using a specific product or service design, a data architecture, and de-identification or similar methods.
- Lets businesses begin the privacy certification process without redoing their entire IT architecture.
- Is more accessible for some businesses.

**Governance Certification**
- An international label – independent of local compliance requirements.
- Focuses on the data management system, without technical audits of resources.
- Sets up a continuous improvement process for data privacy.
- Can be tailored along the lines of the corporate social responsibility (CSR) model.
- Applies to all types of businesses.

**European Union Regulation (GDPR) Certification**
- Addresses Article 42 of the E.U. General Data Protection Regulation.
- Is awarded based on guidance derived from the regulation.
- Voluntary certification for businesses.

The internal audited processes relate to data governance.

Bureau Veritas certification’s model will vary by region, scope of business and a company’s organization.
Learn more about data privacy at:
move-forward-with-privacy.bureauveritas.com

Or contact us at:
move-forward-with-privacy@bureauveritas.com