ARE YOU GDPR READY?

TARGETING COMPLIANCE BY USING A DATA PROTECTION TECHNICAL STANDARD

BUREAU VERITAS

ARE YOU GDPR READY?

Targeting compliance by using a Data Protection Technical Standard

Contents

In 2018, data protection rules in Europe complete their biggest overhaul in two decades.

The General Data Protection Regulation* (GDPR) is designed to meet the needs of the 21st century. The amount of digital information we create, capture and store has grown exponentially as consumers and businesses take advantage of the opportunities offered by the digital economy. But the misuse of data by businesses and government has started to create public distrust (see page 3-5).

Against this backdrop, GDPR provides the requirements for the protection of personal data. It seeks to harmonize data privacy laws across Europe, and give greater protection and rights to individuals. It changes how businesses and public organizations process and store data, and imposes financial penalties of up to 4% of revenues on organizations that fail to comply.

With the May 2018 deadline fast approaching, this paper explains how adoption of a voluntary Data Protection Certification can help you reach compliance.

** Published as Regulation (EU) 2016/679*

ARE YOU GDPR READY?

About the Technical Standard

The Technical Standard for compliance with the (EU) 2016/679 regulation on Personal Data Protection was published in September 2017. Developed by Bureau Veritas Certification, a global leader in risk management and management system certification, it provides a practical and comprehensive method for implementing the processes required to achieve compliance with GDPR.

DOWNLOAD the Technical Standard PDF
http://bit.ly/2zq1mh1

WHO IS COVERED BY GDPR?

GDPR covers all organizations, albeit making a distinction between data controllers and data processors. A controller is the person or business that decides the purpose and manner for which personal data is, or will be used. A data processor is anyone who processes personal data on behalf of the data controller – for example providing data analytics services or storing data on a server. While the regulation applies to both, data controllers are subject to far more obligations.

GETTING TO GRIPS WITH GDPR

GDPR is a wide-ranging regulation covering the data protection rights of individuals on the one hand, and the obligations of businesses on the other. These include a clear responsibility for companies to obtain the consent of people they collect data about. "Data" includes both personal data – broadly defined as a piece of information that can be used to identify an individual such as a name or IP address – and sensitive personal data such as religious and political views or sexual orientation.

A key concept is accountability. Organizations assume full liability for the data they process and must allocate the necessary resources and skills to ensure optimal personal data protection. Obligations increase for larger organizations, as well as companies that carry out "regular and systematic monitoring" of individuals, or process volumes of sensitive data.

The regulation also seeks to increase transparency following a spate of high-profile data breaches, involving the account details of millions of internet users. Organizations who fall victim to hackers, or lose sensitive customer data must report the incident to their country's data protection regulator within 72 hours.

Much of GDPR is about handing power back to consumers. For example, individuals can make requests for personal information free of charge, and businesses must provide the reply within one month. GDPR also gives consumers the right to have their personal data erased.

IN SUMMARY *GDPR puts the onus on businesses to demonstrate compliance in the way they process and store data, and respond to requests for information. To achieve this, businesses need to define coherent processes and ensure they are adopted consistently across the organization. The Technical Standard is designed to help them achieve this.*

CONSUMERS

do not act consistently

Consumers are concerned **how their personal data is used**

Paradoxically **most agree to share** their data

CONSUMERS

More than 80% of consumers are afraid their data will be stolen or misused

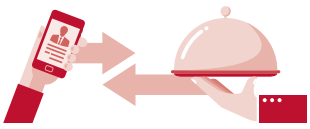
Source: GfK

1/3 of internet users in the United States have had their personal data misused in the past year

Source: GfK

92% of internet users in France think that service providers can use their data

Source: IPSOS for Elia



62% of consumers agree to share more personal information so that they can access new digital services

Source: Microsoft Research

Consumers are afraid of...

87% being inundated with ads

85% being unable to erase their digital footprint

77% being a victim of bank information or identity theft

Source: IPSOS for Elia

In their mind, the most sensitive data is...

82% location

70% browsing history

81% health

68% communications with friends

Source: Pew Research Center

BUSINESSES

struggle to manage the data they collect

All organizations **collect data** (visits, profiles, payments)

But few have a real **data governance system**

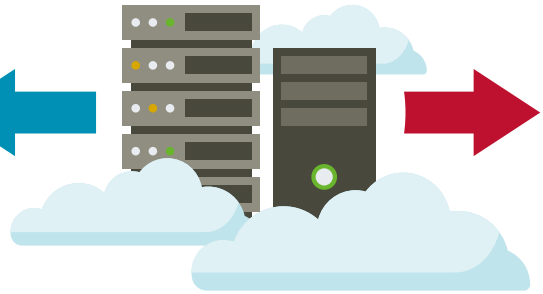
BUSINESSES

They spent

$130 bn.

in 2016 on data and business analytics

Source: IDC

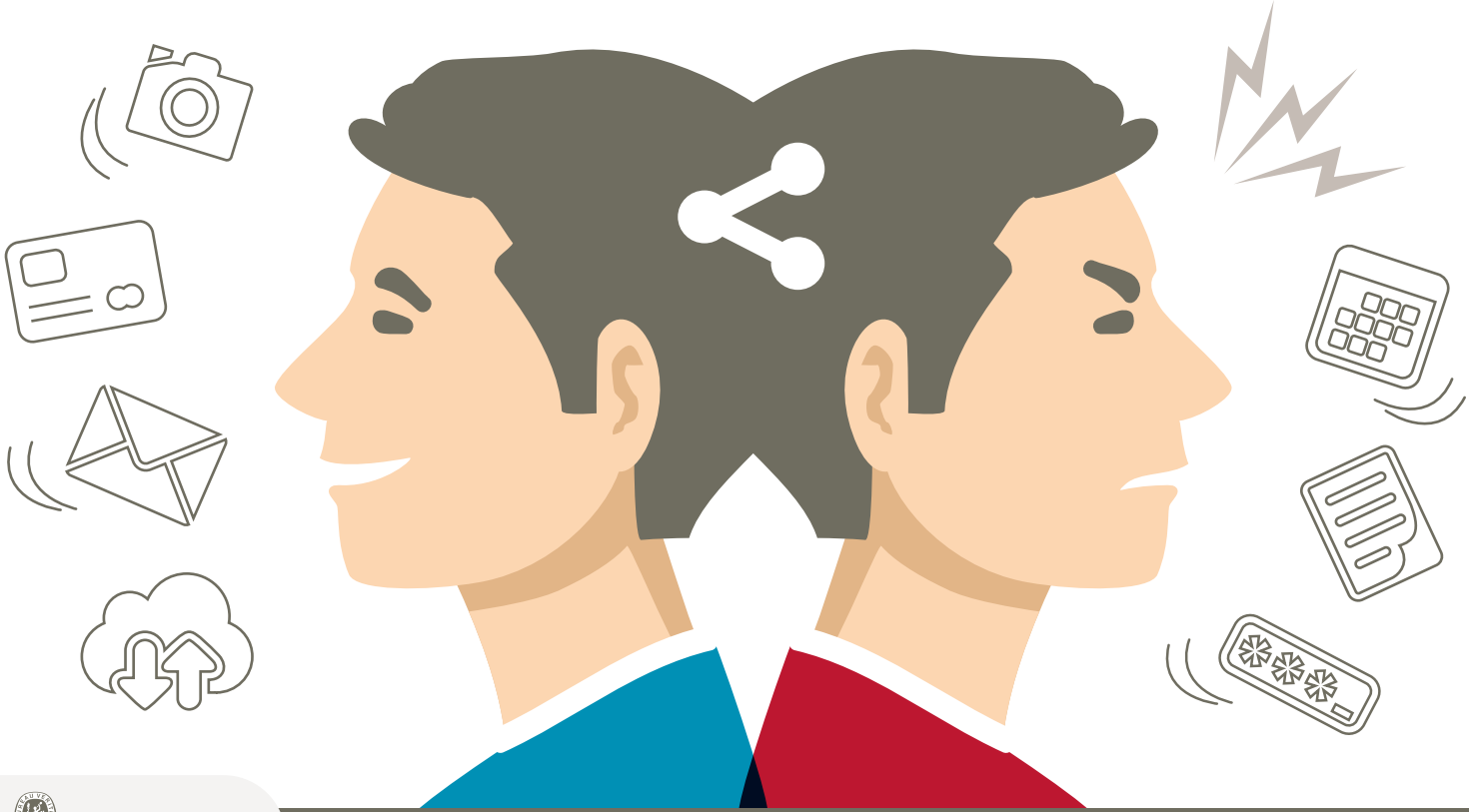


Only

16,000

e-commerce, government and other organizations have appointed an official data protection advocate in France

Source : AFDCP, Fevad



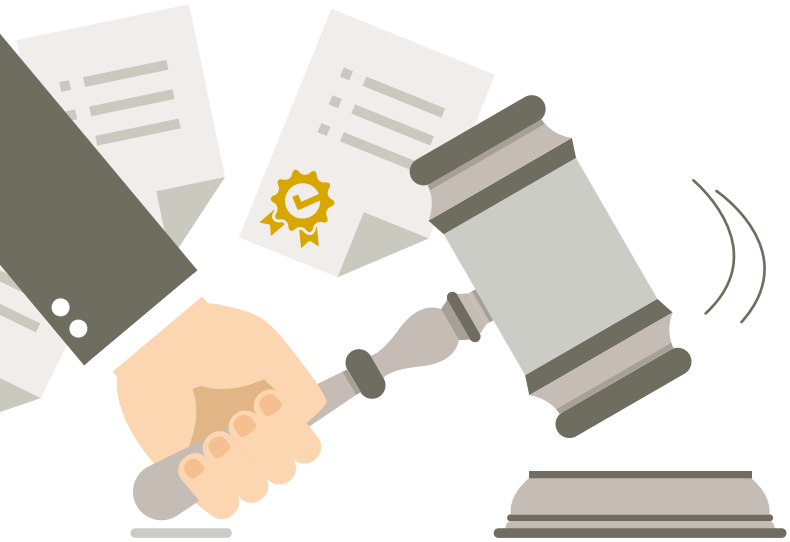
Tough regulations are

A DRIVER FOR CHANGE

BUSINESSES themselves try to put a positive spin on things

+

REGULATIONS are forcing them to get organized



Most organizations post a "soft" privacy policy online, which only 10% of Internet users who sign up with them read in full

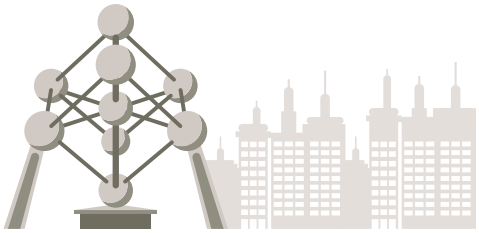
(Source CNIL)

A few big companies publish ethics charters and guidelines

In the United States

The draft Consumer Privacy Bill of Rights has been introduced twice already

1 1 0 1 1 0 1 1 0 1
1 0 1 0 0 0 1 0 1 0
1 1 0 1 1 0 1 1 0 1



In the European Union

The GDPR* was adopted in 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)

**General Data Protection Regulation*

INDEPENDENT CERTIFICATION

is the only way to maintain and increase trust in your brand.

Certification of good management shows you take data protection seriously

- Understandable to the public
- Made credible by the market
- Adaptable and open-ended

- **Data controllers**
  Reassure end users their personal data is secure
- **Data processors**
  Demonstrate credibility to data controllers

Certification is best obtained from an independent body with:

- Credibility
- Impartiality
- Transparent analytics tools
- The ability to support the certification mark

Move Forward with Confidence

BUREAU VERITAS

Technical Standard
OVERVIEW

The Standard covers six main themes, which closely track the regulation. It also includes helpful tables that enable compliance, risk managers and data protection officers to cross-reference the Standard with both GDPR and ISO 9001 to facilitate integration of processes into company management systems on the one hand, and verify compliance with the regulation on the other.

Organization and Structure

Emphasizes the need for leadership and commitment by top management and a documented organizational structure, with roles and responsibilities for personal data management identified, assigned and thoroughly understood across the organization. This includes the appointment of a Data Protection Officer and drafting of a Personal Data Policy.

Personal Data Risk Management

Maps risks and compliance obligations faced by the organization. It includes the Data Protection Impact Assessment – a key requirement of GDPR to determine all activities, products and services that can impact the confidentiality and integrity or personal data, and the potential for data breaches. Processes for managing data breaches are also covered.

Management System

Advocates a systematic approach to managing data protection risks, integrated with organizational processes. This includes documenting information related to data processing and personal data protection, and communicating with employees and external parties. The focus of the Standard is on continuous improvement, achieved through regular monitoring, internal audits and management reviews.

Product and/or Service Control

Details the need to review, define and document personal data compliance obligations and customer requirements for products and services from design and development stage. This includes integrating continuous compliance throughout the life cycle.

Operational Control

Explains the need to develop and implement documented procedures and work instructions to enable employees and external providers to target compliance.

Resources

Outlines the resources needed to implement the Standard, including infrastructure, personnel skills, awareness and knowledge.

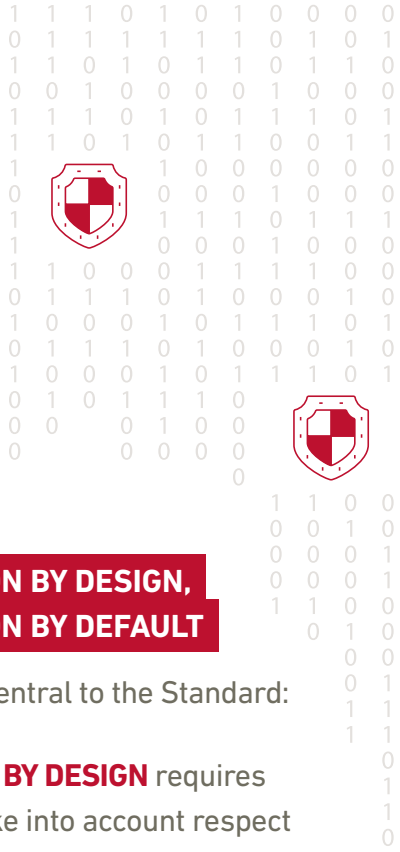
What does the Data Protection Technical Standard **AIM TO ACHIEVE?**

For organizations, striking the right balance between identifying customer insights from big data analysis and using that information to create additional value without compromising individual rights is one of the major challenges of the years to come.

The Data Protection Technical Standard enables organizations to integrate GDPR data protection requirements as a default right from the start and also to build in important specifics - obtaining consent, proportionality, the right to portability - without fundamentally changing the organization's processes.

The Standard supports companies in devising and implementing the policies and procedures required to comply with GDPR

It employs the process approach, which incorporates the Plan-Do-Check-Act cycle and risk-based thinking. Addressing the key principle of accountability – the data controller's liability for any processing of personal data carried out by itself or on its behalf by another organization – it requires adoption of internal rules and a proactive approach to demonstrating compliance.



DATA PROTECTION BY DESIGN, DATA PROTECTION BY DEFAULT

Two concepts are central to the Standard:

DATA PROTECTION BY DESIGN requires organizations to take into account respect for data protection in the design of products and services using personal data.

DATA PROTECTION BY DEFAULT requires organizations to have an information system that guarantees a high level of data protection at all stages. The result is a high level of reassurance for customers that their data is secure, as well as compliance with GDPR requirements.

KEY BENEFITS
of implementing the Data Protection Technical Standard

A systematic approach to personal data protection management can provide top management with information to build success over the long term. It enables you to:

1 Demonstrate compliance with regulatory requirements

The Data Protection Technical Standard closely tracks the requirements of GDPR, providing a framework for implementing policies and processes to reach compliance.

2 Safeguard your reputation

The Standard helps prevent or mitigate personal data breaches. It builds understanding of how personal data breaches occur, and what can be done to prevent them. It also helps you prepare for any data breaches, so that staff are trained and procedures are in place to limit damage, and provide information to data subjects, authorities, customers and employees.

3 Provide products and services that meet customer demand

For companies to win and keep their customers', employees' and other stakeholders' trust they need to demonstrate digital responsibility. The Standard adopts a life cycle perspective, emphasizing control of the way products and services are designed, developed and processed relating to personal data.

4 Address digital risks and opportunities

GDPR grew out of a lack of trust by consumers and regulators about how companies use the increasingly large volumes of data to which they have access. Adoption of the Technical Standard promotes confidence in your organization's use of big data, enabling you to grasp the opportunities of digital transformation.

NEXT STEPS

Bureau Veritas offers a range of services to get you on the road to compliance with GDPR.

GET CERTIFIED

Certification against this Technical Standard by Bureau Veritas provides independent assurance that a company has implemented the Standard across its organization, that it is understood and consistently applied by employees and that any non-conformities are addressed. In doing so, it helps the organization achieve regulatory compliance*.

TRAIN YOUR EMPLOYEES TO ENSURE CONSISTENT IMPLEMENTATION

Employee awareness and understanding of data protection issues, and the processes you put in place to address them, are crucial. Bureau Veritas can support you with training for employees and contractors.

IMPLEMENT THE TECHNICAL STANDARD

Download a copy of the Technical Standard to get started. You can follow this standard to develop the processes, policies and documentation you need to implement to reach GDPR compliance.

DOWNLOAD the Technical Standard PDF
http://bit.ly/2zq1mh1

For more info on CERTIFICATION

For more info on TRAINING

**Adoption of this Technical Standard does not reduce the accountability of the data controller or processor to comply.*

ABOUT BUREAU VERITAS

Bureau Veritas is a world leader in testing, inspection and certification. We help clients across all industries address challenges in quality, health & safety, environmental protection, enterprise risk and social responsibility. We support them in increasing performance throughout the life of their assets and products and via continuous improvement in their processes and management systems. Our teams worldwide are driven by a strong purpose: to preserve people, assets and the environment by identifying, preventing, managing and reducing risks.

For more information, contact Bureau Veritas:

Le Triangle de l'Arche
8 cours du Triangle
CS 90096
92937 Paris La Défense Cedex
FRANCE

certification.contact@bureauveritas.com

Download the Technical Standard

Visit our Data Protection pages

BUREAU VERITAS

Editorial, design and production: IMPACT-communications.fr / BOLDcie.com
Photo credits: iStock / Thinkstock -