Is your company data privacy compliant?
Assessing your compliance through a health-check

Questions for the C-suite
► Is privacy a board-level priority within your organization?
► What steps do you take to anonymize the data to ensure customer privacy?
► Is privacy a consideration when acquiring and implementing new technology?
► Do you have privacy governance and operating models?
► Do you monitor and measure your privacy performance on an ongoing basis?

Data privacy is about the appropriate use of personal information of an individual, which will depend on the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal issues surrounding them. Each individual has the right to control the collection, use, and disclosure of personal information.

Challenges
Organizations have to strike a balancing act when it comes to data protection and data privacy. Information assets must be used effectively and efficiently for the organization to be successful. However, there is a complex range of standards to meet, both in terms of regulatory requirements and arising from customer and employee expectations.

Regulatory
Complex regulatory environment at the local, national and global level; privacy and data protection laws, customs and practices vary from country to country.

Globalisation
Business today are compelled to interact beyond traditional market borders.

Outsourcing
Companies are outsourcing more activities than ever to third-party providers, which introduces an entirely new level of complexity to data risk and data privacy issues.

Technology
Every advance in data-handling technology, including the consolidation trend in ERP systems, brings new privacy and cross border data flow implications.

A new legal framework for data privacy and data protection
The Belgian Data Privacy Act has undergone multiple modifications since its origination in 1992 up to 2006. On January 25th 2012, the European Commission proposed a draft of the General Data Protection Regulation (GDPR), a comprehensive reform of the EU's 1995 data protection rules to strengthen the protection of individuals with regard to the processing of personal data and the free movement of such data. The European Council is in the process of integrating EU member states’ comments on the draft GDPR. The adoption of the regulation is aimed for in 2014 and the regulation is planned to take effect in 2016 after a transition period of 2 years.

Following key principles are applicable:

Data minimization
Only those personal data may be processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, it must be ensured that by default personal data are not made accessible to an indefinite number of individuals.

Accountability
Personal data must be processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation compliance with the Regulation.

Transparency
Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
The legal framework is only 1 part of the puzzle
To understand what data privacy compliance means and what needs to be done to effectively manage and protect personal data it is important to take a bottom up approach and consider what can go wrong.

Non-compliance with data privacy regulations or operating insufficient security around the protection of data can:
- Result in reputational damage, litigation and major fines
- Lead to the loss of customer confidence, market share and the erosion of shareholder value
- Impact the ability of the business to deliver customer services

Business drivers and challenges demonstrate the need for a sound data protection framework
The diagram below presents a holistic view of a data protection framework with a focus on aligning controls to the data that matters most to the business. EY uses this model in performing program assessments, developing strategy, implementing processes and technology and designing management reporting. Maturity models and work programs supporting this model have been developed, rolled out globally and used repeatedly.

Data governance
Policies and standards | Identification | Risk assessment | Classification | Architecture | Quality
---|---|---|---|---|---

Data protection controls
Focus areas
Data in motion | Data in use | Data at rest
Perimeter security | Privileged user monitoring | Encryption
Network traffic monitoring/blocking | Workstation restrictions | Obliteration/tokenization
Web content filtering | Application controls | Mobile device protection
Data collection and exchange | Data labelling/tagging | Network/server repository control
Messaging (Email, IM) | Removable/external media control | Physical media control
Remote access | Export/clipboard/print control | Archive, disposal, destruction

Supporting information security processes

A data privacy health-check as starting point for your data privacy program
A “data privacy health-check” is a short-term exercise resulting in a data privacy remediation roadmap. In order to come to this high-level roadmap, following main activities will be executed:
- A definition of a target compliancy model
- An assessment of the current data privacy compliancy state
- A gap analysis and benchmark to EY’s Privacy Maturity Model