WHITEPAPER

The New EU General Data Protection Regulation and its Consequences for IT Operations and Governance

sqs.com

Author: Anita Vocht
Senior consultant

SQS Nederland

Published: September 2016

Transforming the World Through Quality

ANITA VOCHT
Senior consultant
anita.vocht@sqs.com

Anita Vocht is a senior consultant at SQS and has worked in a wide range of functions in the software industry. With over 20 years of experience in IT delivery, she specialises in the areas of test management, process improvement (Lean) and quality management. As a certified Privacy Professional (CIPP/E, CIPM), she is particularly interested in the implications of the new EU data protection regulation for IT governance and operations.

Contents

Management summary

The new EU data protection regulation will come into force in two years' time. It has far-reaching consequences for any organisation dealing with personal data of EU citizens and is impacting IT operations in particular.

IT leaders should proactively engage in privacy programs and live up to the challenge of transforming their business and taking data protection to the next level.

Keywords

EU GENERAL DATA PROTECTION REGULATION (GDPR)

PRIVACY COMPLIANCE PRIVACY PROGRAM

DATA MANAGEMENT DATA GOVERNANCE

Introduction

In recent years IT innovation, coupled with a renewed focus on customer experience, has initiated the rapid proliferation of cloud computing, big data, mobile interconnectivity and the Internet of Things. It is the most important driver of the disruptive changes that are currently taking place, with pro-found effects on businesses, public authorities and people's private lives. These changes can be considered as both positive and negative developments. On the upside, IT innovation enables the growth of completely new business models. In general, it delivers ways and means to make our lives easier and more comfortable. On the downside, it makes businesses and jobs obsolete and poses a serious threat to people's freedom and privacy.

Legislation usually follows new developments at a much slower pace and the current EU data protection reform is no exception. It couples data protection, as a fundamental right of EU citizens, with current practices of data proliferation that include the risks of fraud, identity theft and loss of individual freedom.

This has resulted in the new General Data Protection Regulation (GDPR), a more rigorous and coherent data protection framework, which provides a uniform piece of legislation with standardised requirements throughout the EU. It will ensure that personal data* of EU citizens is subjected to higher levels of protection, without hindering the growth of trade. Balancing privacy protection with the benefits of digital developments will be essential for the growth of the digital economy.

The new legislation came into force in May 2016, requiring companies to be compliant by May 2018. Its impact is by no means limited to European countries. Any organisation that processes EU citizens' personal data can – and most likely will – be held accountable for non-compliance issues regarding this data.

Governments and businesses need to start preparing for the changes the GDPR brings. In this paper, the requirements for data privacy compliance are related to practical guidelines for implementation, with particular focus on IT governance and operations.

Market trends and challenges

Most organisations operating within EU jurisdiction are now aware that stricter privacy regulations are due in two years' time. However, in a recent survey [1], less than one third of the respondents agree that their corporate privacy and security policies have kept up with recent technology and regulatory changes. Few organisations are actually aware of the full impact the new legislation will have on their operations.

So far, EU national privacy authorities (with the possible exception of Germany) have been fairly lenient in enforcing privacy regulations. However, that is likely to change due to the new legislation at hand and the growing awareness and concern among the general public. Currently, only 37% of customers** believe that governments and businesses are adequately protecting their personal information [1].

The trends toward technical innovations, growing customer concerns and stricter regulation will have a huge impact on how organisations and businesses deal with personal data, especially in relation to IT.

Three major trends and corresponding challenges can be identified; these are represented in Figure 1.

* In this paper the terms 'privacy', 'data privacy' and 'data protection' are used interchangeably. They all refer to the definition of personal data that is used in the EU: any and all data that is related to an identified or identifiable individual [2].

** 'Customer' is used in this paper as a synonym of the legal term 'data subject'. It refers to the individual whose personal data is being processed by businesses, authorities or other organisations.

The challenges can be summarised as:

1. Prevent unlawful access to personal data
2. Align data processing practices with consumers' expectations
3. Ensure compliance with privacy laws and regulations.

These are important drivers of change in the years to come, for any organisation dealing with personal data of EU citizens.

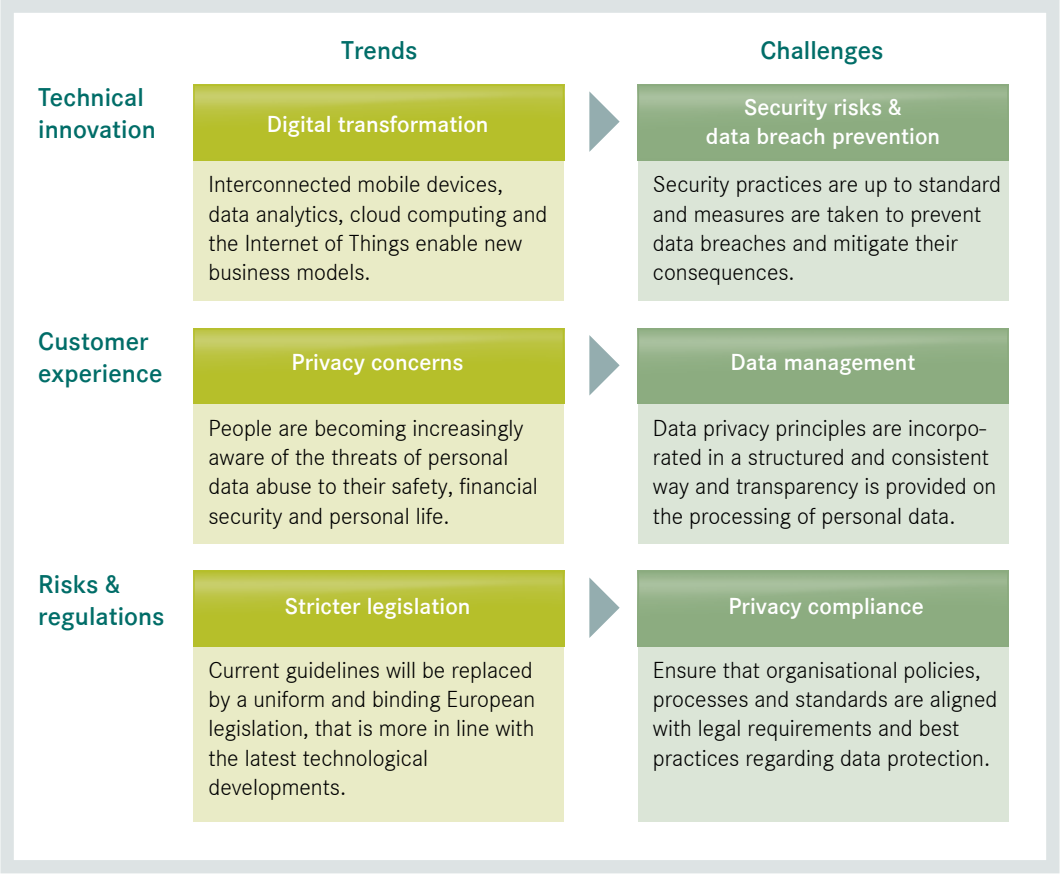

Figure 1: Trends and challenges in relation to processing personal data

What is the new GDPR legislation about?

Nowadays, data is one of an organisation's most important assets. It helps to reduce costs, reduce risks, improve processes and decisions and optimise customer experiences. Protecting this corporate data is therefore a key-responsibility.

The GDPR essentially applies to personal data of EU citizens in all forms, be it digitised or in paper archives. In this paper the focus will be on digital data. Personal data is data relating to natural persons. It is a sub-category of data that requires more stringent organisational and technical safeguards.

Providing customers transparency with regard to their personal data, while at the same time applying adequate data management and data governance practices, will become decisive features in this new reality (Figure 2).

- **Data transparency**

  The most essential aspect of the new legislation is that customers will be more in control of how their personal data is gathered, stored and processed (in legal terms: "rights of the data subject"). This requires organisations to ensure that customers have transparency on the personal data in their care and to provide them with the possibilities of choice and consent.

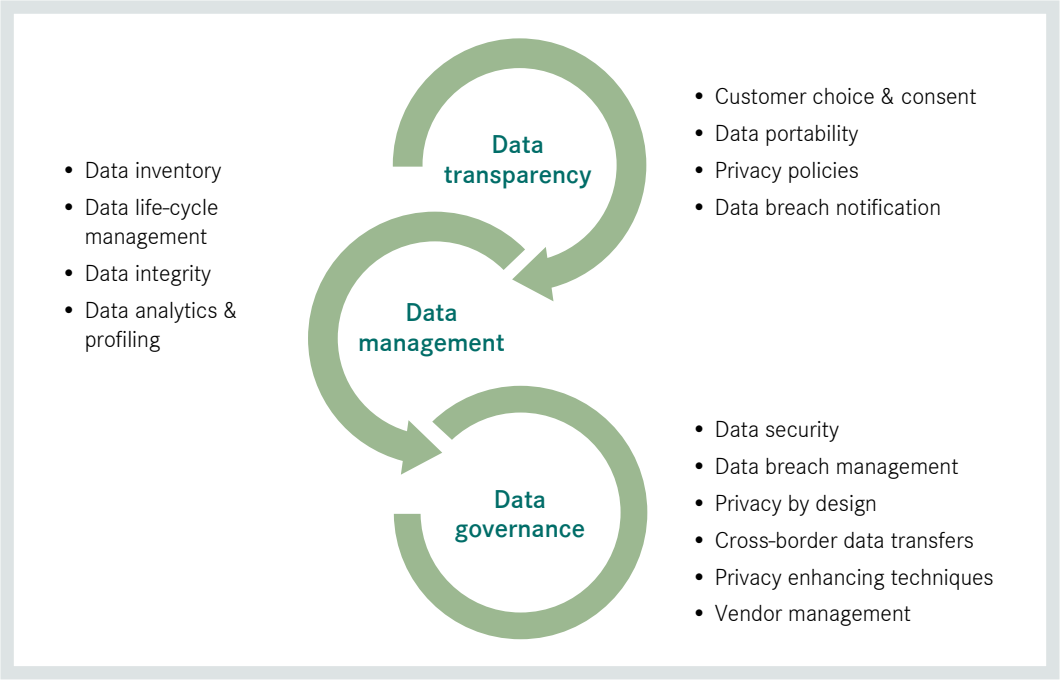

Figure 2: Key areas of the EU General Data Protection Regulation (GDPR)

- **Data management**

  Data management relates to all data processing activities performed in an organisation or by external processors. Personal data needs to be managed throughout its life cycle, taking into account *fair information practices:*

  - Limited data collection (proportionality)
  - Clear defined purpose
  - Data integrity
  - Limited retention
  - Limited disclosure to third parties

- **Data governance**

  Data governance is defined as "exercising authority, control and shared decision-making over the management of data assets" (DMBOK). Strong data governance practices help to ensure compliance, while reducing costs and providing the necessary auditability and control.

GDPR implications for IT processes

Protecting personal data in compliance with the new regulation will affect both business and IT. Since most data that an organisation holds is in digital form, the impact on IT processes is profound.

Changes can be anticipated in:

- System development and application management
- IT operations (incident response, monitoring, business continuity, customer services)
- Data security
- Data analytics
- Third party data processing (hosting, outsourcing)
- Vendor management

This chapter illuminates some of the possible repercussions of the new legislation on IT processes, in light of the GDPR key-areas. It should be kept in mind that the GDPR is by no means unambiguous; some legislative provisions leave ample room for debate and interpretation. It remains to be seen how strictly some legal provisions will be interpreted and enforced by the national Data Protection Authorities.

Also, the impact per organisation will vary, since legal provisions and risk drivers differ according to geography, industry, sector and data category [3]. Data hosting by external providers and cross-border data transfers pose additional challenges.

Data transparency

Customers (data subjects) have enhanced rights to notice, access, rectification and to object to processing [4].

For all customer requests (Table 1) involving the processing of personal data, the following must be in place:

- The details of the processing of personal data must be provided to the customer
- Notice must be given of the customers' rights
- A process for handling and documenting customers' requests must be in place (incl. user interface)
- The customers' identity must be authenticated before a request is granted
- Applications must be available to process (and log) data changes based on a customer's request
- Applications must be available to exempt the data from further processing
- Helpdesk support must be provided
- Additional requirements for *explicit* consent (as opposed to unambiguous consent):
  - Explicit consent must be actively obtained and it must be documented
  - As soon as explicit consent is withdrawn, the data processing must stop

Key-area	Legal provisions	IT implications
Customers' choice	The right to access the personal data an organisation holds	Ability to provide the customer with insight into their personal data
	The right to have incorrect information corrected	Ability to rectify the personal data as requested
	The right to object to data processing for direct marketing purposes	Ability to exempt personal data from future processing
	The right to be forgotten	Ability to delete personal data
Customers' consent (explicit)	Data processing of special categories of personal data (e.g. ethnicity, health, religious beliefs) is not allowed unless explicit consent is provided.	In the case that consent is withdrawn, the processing must stop. Sensitive data must be erased on request.
	Cross-border transfers of personal data to non-EU countries with no additional safeguards is not allowed unless explicit consent is provided.	In the case that consent is withdrawn, the processing must stop.
	Automated processing resulting in profiling and automated decision-making with possible adverse effects for the customer is not allowed, unless explicit consent is provided.	In the case that consent is withdrawn, the processing must stop and the automated decision must be reversed.
	Data portability aims to increase customers' choice of online processing. The right to obtain a copy of personal data or have it transferred to a competitor.	Ability to deliver the requested data to the customer in a commonly-used format or to transfer it to another party
Data privacy policies	Disclosures about data processing and customers' rights must be intelligible and easily accessible.	There is a substantial increase in the number of disclosures due to enhanced customer rights.
Data breach notification	Notice is required if a data breach is likely to result in high risk to a person's rights and freedom.	Notify the customer(s) affected by a data breach without delay.

Table 1: IT implications in relation to customer control and data transparency

Data management

Personal data needs to be managed throughout its life cycle, taking into account fair information practices for data processing (Table 2).

Key-area	Legal provisions	IT implications
Data catalogue [5]	Organisations must be able to identify, control and manage all stored personal data, including data that is processed and stored by third parties. The first step is to catalogue these data assets.	Personal data is processed by multiple applications, stored in various databases on different storage devices and in different locations. Setting up a comprehensive inventory of data assets is a complex task, requiring IT knowledge, tooling, funding and support.
Data lineage [5]	Organisations not only need to know what personal data is processed, but also how, when and by whom (flow of data artefacts).	The end-to-end data flow of personal data must be traced and documented, to assess risks and deploy appropriate security safeguards.
Data life cycle management & data integrity	Personal data must be subject to proper data life cycle management in line with fair information practices regarding collection, purpose, use, integrity, retention and disposal of data, as well as disclosure to third parties.	• Limited data collection (purpose-related only) • Limited data retention • Data should be accurate, complete, relevant and up to date • Data archiving sometimes requires anonymisation • Logical versus physical data deletion
Data analytics (business intelligence)	Current data analytics practices are for the most part clashing with legal restrictions and fair information practices, such as limited data collection, processing restricted to purpose and limited disclosure to third parties.	Data analytics involves maximising data input without explicit purpose. Limited disclosure is difficult to achieve, since anonymising large data volumes is complicated and testing big data applications is often done in production, by fencing off part of the production system. It is as yet unclear how the regulation will affect these practices (with the exception of profiling).
Profiling	A privacy impact assessment (PIA) is required for profiling and automated decision-making involving natural persons.	Assessing privacy risks should be an ongoing element of data analytics practices.

Table 2: IT implications in relation to data management

Data governance

Data governance is an essential part of business and IT governance. Implementing data protection requirements involves IT processes for:

- Developing new IT products and services
- Purchasing IT products and services
- Operations and maintenance of IT products

In Table 3, the GDPR implications for the system development life cycle are depicted.

Key-area	Legal provisions	IT implications
Projects and portfolio	Data privacy compliance is a legal obligation. The impact of every business change or IT change should be evaluated accordingly. For major changes, a Privacy Impact Assessment (PIA) may be in order.	• Define generic data protection requirements for corporate IT (system, architecture, software related) • Perform a privacy risk analysis for every new service (or major change)
Privacy by Design (PbD)	Embed privacy values and preferences into the design and operation of information technologies, systems and infrastructures.	• Incorporate Privacy by Design in the system development process • Enhance privacy awareness through ongoing education • Privacy by Design training • Verification & validation of Privacy by Design software features and defaults • Anonymising (production) test data with the help of a software product [6].
Privacy Enhancing Technologies (PET)	There are no legal stipulations on implementing technical safeguards, but these may contribute to improving data protection practices.	There are powerful solutions to cope with privacy compliance challenges, e.g. data mapping tools, continuous monitoring tools, the use of synthetic data for test purposes [6] or data pseudonymisation and anonymisation techniques. The GDPR creates incentives for data controllers to pseudonymise data [4].

Table 3: IT implications (system development life cycle)

There are also significant implications for the IT processes governing the purchase of products and services and operations and maintenance. These are listed in Table 4.

Key-area	Legal provisions	IT implications
Data security & business continuity	Technical and organisational safeguards to protect (personal) data should be adequate and up to standard.	• Access to non-anonymised personal data must be restricted for non-authorised users (OTAP environments) • Technical and organisational safeguards to ensure backup and recovery of personal data
Data breach management	Reasonable measures must be taken to prevent and mitigate data breaches. Serious data breaches must be reported to the supervisory authority within 72 hours.	• An incident-response plan for data breaches • IT operations involvement in data breach prevention and mitigation • Operational security safeguards (security controls and monitoring)
Cross-border data transfers	Transferring personal data of EU citizens to a non-EU country is not permitted unless that country is deemed "adequate" or in the case that model contract clauses/ Binding Corporate Rules apply.	This ruling will cause practical issues since organisations may currently store EU personal data on (company) servers outside of the EU. Also, cloud providers typically store EU personal data on servers all over the world.
Vendor management	GDPR compliance also applies to external processors under contract (e.g. outsourcing partners, cloud providers).	• (Re)assess vendor agreements with external vendors and suppliers to achieve compliance [4] • Perform audits to monitor vendor compliance on an ongoing basis
Monitoring & enforcement	There must be a formal process in place to monitor and enforce privacy requirements.	• Set up policies for data protection and validate alignment with current IT standards and practices • Consider technical capabilities to automate monitoring tasks, e.g. security analytics to track & analyse cyber-attacks and data breaches • Define a set of practical indicators, metrics and monitoring requirements to implement into daily operations • Assign the authority to enforce compliance and work with stakeholders

Table 4: IT implications (IT operations and governance)

The way forward

The new EU privacy legislation will become effective in 2018, leaving organisations sufficient time to adapt, provided they start doing so now.

The benefits of doing so will likely outweigh the costs. Non-compliance evokes the prospect of reputational damage and hefty fines adding up to 4 % of companies' annual worldwide turnover. Employing the appropriate organisational and technical safeguards will not only be a mitigating factor, but also demonstrates good business ethics and corporate sustainability. Taking data protection seriously can become a major selling point in the digital economy.

The question is how to turn this into a practical endeavour whilst achieving a healthy balance between the costs and benefits of legal compliance.

Maturity through agility

Becoming compliant is not a straightforward path from A to Z. Neither is it a stairway to (maturity) heaven. Using models or privacy frameworks can certainly be helpful in supplying criteria or best practices, but should not be applied rigidly. Becoming compliant should rather resemble a journey: the path and the destination may change over time and progress is achieved as we go along.

Important elements in such an approach should be:

1. **An attitude adjustment**

   It is important to look beyond the letter of the law to achieve compliance. In the EU, adequate protection of information and people's privacy is considered a human right.

2. **A comprehensive perspective**

   a. Implementing data privacy principles requires a multifaceted approach.

   b. Data privacy awareness should be incorporated at all organisational levels.

3. **A risk-based strategy**

   The key guiding principle for any control implementation is to decide on the appropriate level of compliance. It is important to determine what level of risk and exposure is acceptable for an organisation.

4. **An iterative approach**

   Achieving data privacy compliance is not a one-off project but an ongoing process. It would therefore be advisable to embed a privacy management program in a continuous improvement cycle (as is shown in Figure 3). The essence is to start small, aspire to achievable targets, evaluate results and gradually increase scope and impact.

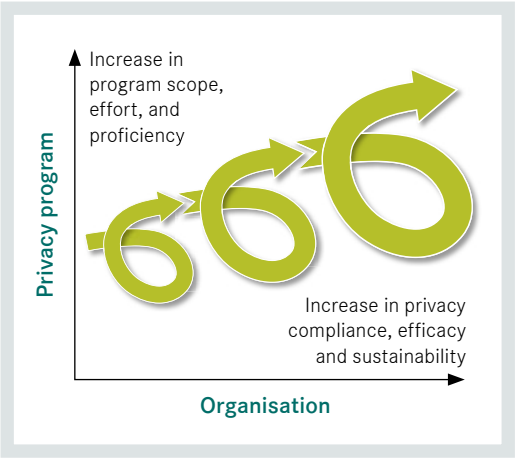

Figure 3: Achieving data privacy compliance in continuous improvement cycles

Privacy program

For many organisations, setting up a privacy program will be the first practical step in recognising the need to act [3]. It enables a structural approach to reaching privacy compliance goals, in line with business needs and priorities.

Data privacy compliance is a boardroom topic and information technology is an important enabler. IT stakeholders should therefore be involved in a privacy program from the very start.

IT needs to take a proactive role in translating legal obligations into a privacy strategy in line with the organisational strategy and IT objectives.

This also involves alignment with accepted IT industry standards and best practices, e.g. ISO/IEC 27001.

Conclusion and outlook

The GDPR implications for most organisations processing data of EU citizens are far-reaching and IT practices will be heavily impacted. The extent of the implications may differ, but becoming data privacy compliant will be a major operational reform. In doing so, organisations will look to those that not only understand the regulatory changes, but can offer IT advice and solutions to ensure that companies, and the personal data they hold, are well-protected.

References

[1] ISACA survey (2015). Keeping a Lock on Privacy: How Enterprises Are Managing Their Privacy Function. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/keeping-a-lock-on-privacy.aspx

[2] The EU Data Protection Directive 95/46/EC https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm

[3] Russell R. Densmore (2013). Privacy program management, tools for managing privacy within your organization. ISBN 978-0-9885525-1-7

[4] IAPP (2016). The top 10 operational impacts of the EU's General Data Protection Regulation. https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr

[5] David Loshin (2015). Seven Data Strategies for Regulatory Compliance. http://governyourdata.com/page/white-papers

[6] Samuel Mischler (2014). Synthetic data and its consequences, how to eliminate legal and regulatory obstacles in testing. SQS Whitepaper Book 2014

SQS Software Quality Systems AG
Phone: +49 2203 9154-0
Fax: +49 2203 9154-55
info@sqs.com | www.sqs.com