PRIVACY BY DESIGN IN GDPR : FROM A QUALITY PROCESS TO A LEGAL REQUIREMENT

Regulation (EU) 2016/679, 27 avril 2016

ISO 9001 :2015, 5th edition 2015-09-15

Cathy VRANCKX

Friday , 29 june 2018

TABLE OF CONTENTS

1. INTRODUCTION

The Information and Communication Technologies bring about a lot of changes in our life: we find or share information around the world wide. Information concerns not only people but also companies, governmental organisations or any legal entities, that is the purpose of the Digital Single Market[1]. From a person with rights and freedoms to data subjects, we become natural person with personal data[2]. From a real body subject to virtual objects, we become products in a virtual marketplace. Therefore, we are a market items just like being data. That means, we need to rule any use of information about anybody by anyone.

*"Nowadays, privacy by design, or its variation **data protection by design**, is regarded as a multifaceted concept, involving various technological and organisational components, which implement privacy and data protection principles in systems and services."*[3]

A common principle of Law states "*the Society precedes the Rule*". The privacy by design is not the odd one out. Indeed, the business people hasn't wait for such rules to design some methods.

In 90's, the concept of privacy by design has been developed by Dr Ann Cavoukian[4] to prevent "*the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems."* [5] In October 2010, the Information and Privacy Commissioner of Ontario presented at the International Conference of Data Protection Authorities and Privacy Commissioners:

- it is an internal component of privacy protection
- It is strictly related to privacy measures and privacy enhancing technologies (=PETs).
- it is integrated into the design of information and technology system

The **Privacy – Enhancing Technologies** should be integrated as toolkit for any organisation to ensure a data protection. By definition, they refer mainly to technology uses to support compliance with data protection like encryption, Users' Rights Management (e.g. Access Control List, Metadata), IT infrastructure (e.g. Cloud, Information security),IT governance (e.g. risk assessment, security check, quality control and insurance or testing), Graphical User Interface (e.g. Identification procedure, user account management).[6]

The **General Data Protection Regulation[7],** which came into force on 24/05/2016, will apply from 25/05/2018 in all European members' states to decree a data protection scheme framework shared inside the European union and abroad. Some generic principles, which are also applied in PETs or used in quality standard (*e.g. ISO 9001: 2015*), are taken over mandatory items for data protection:

- Privacy by design
- Privacy by default

1 See http://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html

2 See art.4:"[…] an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

3 See https://www.enisa.europa.eu/topics/data-protection/privacy-by-design

4 See https://www.ryerson.ca/pbdce/about/ann-cavoukian/

5 See https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/

6 See https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies/

7 The Regulation (EU) 2016/679 replaces the Data Protection Directive 95/46/EC

2. DEFINITIONS

2.1. Concerned persons

This section aims to define roles and duties of the main actors involved within GDPR:

Data subject: natural person related to personal data

e.g. the citizens of this member state who has claim for a new passport

Controller: legal or natural person who define purposes and or means for processing

e.g. member state law(new format of passport with biometrics), companies (Industry or service Company...), Organisations (Non-Profit Organisation, Hospitals, governmental agencies, municipalities...)

Processor: legal or natural person who executes the processing operation

e.g. public or private operator involved with a controller

2.2. Privacy By design

Within GDPR, the art 25 1. states:"*the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."*

At this stage, we observe that **Pseudonymisation** and **Data minimisation** are retained as the two Privacy-enhancing Technologies, which GDPR encourages.

The art. 4 (5) defines Pseudonymisation:"*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*"

Within ISO 9001: 2015, the art. 8.3 in "*design and development*" section states:" *implement and maintain an appropriate design and development process that ensures the subsequent provision of required products and services.*"

The art. 8.3.1 describing the compulsory items for the planning may consider other concerned parties including users in the design and development process and the control over this design, that they shall have. Thus the privacy by design becomes a method to include all parts involved according their requirements.

More over, **documented information** should be retained for each steps. These documents or provisions proves the PDCA[8] cycle has been properly executed:

- **P**lan: the task is collected as an item of the process.
- **D**o: the task has been done.
- **C**heck: the task has been done as it has to be done following instructions (conformity) or not (no conformity).
- **A**ct: An action plan must be launched to find why it didn't work properly and the solution to prevent such an event in the future.

This ISO standard doesn't recommend any technology. It helps to drive activity or project with methodology and appropriate documentation in order to prove that what has to be

8 See https://www.manager-go.com/management-de-la-qualite/dossiers-methodes/pdca-deming-en-pratique

implemented as to be done in compliance with company's standards and in accordance to the ISO Standard.

2.3. Privacy by default

Within GDPR, the art 25 2. states:"*The controller shall implement appropriate technical and organisational measures for ensuring that, **by default, only personal data which are necessary for each specific purpose of the processing are processed**. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."*

That means, the dataset must be defined for each part of process in which they are involved. Only the data required have to be processed.

3. CONSTITUTIVE ITEMS

3.1. ISO 9001: 2015

The ISO standard provides a general framework within quality management to support organisations and companies. But the most remarkable interest is that "t*his International Standard employs the process approach, which incorporates the Plan-Do-Check-Act (PDCA) cycle and* ***risk-based thinking****.* [9]" That means, each organisation must identify and evaluate the risks for their own activities at each steps and, among other, at the starting point, when the idea becomes to be designed.

So early in design phase and before the development phase, the standard suggest to identify risks and evaluate them. Consequently, preventive measures shall be define according the list of risks. Those types of measures includes actually technical and or organisational security measures.

Please note:

According the ISO 9001 8.5[10], there are two types of actions

-preventive action: action to eliminate **the cause of** a potential non conformity.

-corrective action: action to eliminate **the cause of** a detected non conformity.

Those type of actions shall be includes in organisational and technical measures

3.1.1. Risk-based thinking

"R*isk-based thinking enables an organization to determine the factors that could cause its processes and its quality management system to deviate from the planned results, to put in place preventive controls to minimize negative effects and to make maximum use of opportunities as they arise*[11]". The company or organisation should make a risk assessment of their activities:

- List the risks that can occur
- Identify the risks from this list that can be related to an activity
- Analyse the risks: can the risk happen? How often? What are the consequences (= gravity level)if it happens?
- Define the risks related: table of risk by activity or department with figures (names of the risk, frequency, gravity)
- Define an action plan to prevent: e.g. within IT department, electricity breakdown in server room, fire in server room, server crash …
- Define a communication plan: Who to contact? How to inform the concerned people ?

3.1.2. Documented Informations

At each phases of activities related to quality, the standard recommends to provide informations based on documents or provisions.

Example: 8.3.1 The organization shall establish, implement and maintain a design and development process that is appropriate to ensure the subsequent provision of products and services.

1. **Planning:** determine time line, resources and tasks

9 See https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:en

10 See http://the9000store.com/iso-9000-tips-iso-9001-requirements/iso-9000-tips-corrective-and-preventive-action/

11 See https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:en

Documented Information: scope of the design (*e.g. Customers 'needs and requirements, time-scales, CV's – resources assignments – specifications, design plan*) and stages of design process (*e.g. WoS[12], Gantt[13], design review, codes of conducts or best practices , reports,..*)

2. **inputs**: determine information and resources required to start design

   Documented information: legislation (*e.g. Regulations, directives)*, policies, specifications, risks assessments, performances issues, communication issues *(e.g action plan, check-list),…*

3. **controls**: apply appropriate controls to check that the achieved activity results are the expected ones (or very closed in case of) and reviews, validation issues (including testing issues) and actions are running properly[14].

   Documented information: methods (e.g. process definition, data mapping, calculation spreadsheet)***, tools*** (*e.g.* software) ***and testing*** *(e.g. test cases, protocols definitions ….)*

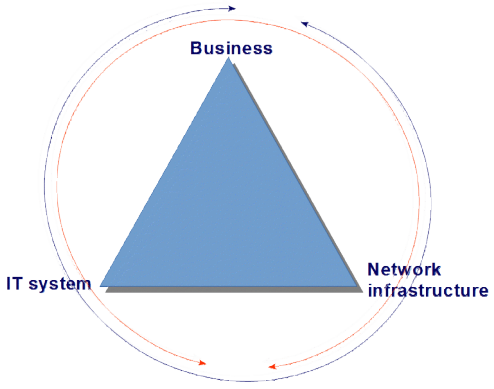
4. **outputs**: define the results of design

   Documented information: standard (e.g. process definition, specifications, ….), provisions, traceability, quality insurance...

5. **changes:** define any updates, releases or changes within the design process

   Documented information: specification(e.g. process definition, process reviews, design plan, design reviews), change management issues (*e.g. testing reports, design reviews, action plan, incident reports,..)*

3.2. Within Information technology business analyse



The privacy by design covers a triangle relationship between "*IT systems, accountable business practices and networked infrastructure.*[15]"

This view shows the interaction between the three main fundamental bases for designing a project:

- The Business defines its needs and requirements including the data and business processes
- The IT system provides the environment of Information and which are technologies in use
- The network infrastructure determines how to communicate and how to organise processing

12 *WoS stands for **W**ork **o**f **S**tatement, for more details about document template please go to* *http://www.wordtemplatesonline.net/statement-of-work-template/*

13 *Gantt is a tool management chart to get an overview of task and resources, see* *https://templates.office.com/en-us/Gantt-project-planner-TM02887601*

14 See *http://www.relevantbusinesssolutions.co.uk/782-2/*

15 See https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/

Privacy by Design may be applied to any types of personal data including specific categories of data such a medical information and financial data. The purpose is still to provide the right high level of protection.

How to proceed?

1. The risks must be defined.
2. Measures must be taken according to listed risks.
3. Appropriate security plan must be implement regarding those measures

→ How high sensitive are the data how high should be the appropriate organisational and or technical measures. The strength of the implemented privacy measures is strictly related to the sensitivity of the data.

The IT business analyse should taken into account the 7 fundamental principles:

1. Proactive not reactive: preventative not remedial
2. Privacy as the default setting: the data protection should be the 1st component
3. Privacy embedded into design: data protection should be fully integrated
4. Full functionality: positive-sum, not zero-sum
5. End-to-end security: full lifecycle protection
6. Visibility and transparency: keep it open
7. Respect for user privacy: keep it user-centric

3.3. Within GDPR

The GDPR set up two specific privacy-enhancing technologies:

- Pseudonymisation: privacy by design/default
- Data minimisation: privacy by design/default
- Encryption: privacy by design and security plan (e.g. banking apps)

The art 32.1 (a) mentions Pseudonymisation and encryption as security measures too.

The data protection scheme is defined and integrated at an early stage, while the project or idea or activity is designed. However some measures can be implemented later when suitable safeguards are defined.

Please note:

In case of impact assessment (see art. 35. 7(d), "*the measures envisaged to address the risks, including **safeguards, security measures and mechanisms** to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*"

Regarding art.89, safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes have to be appropriate and ensure, that technical and organisational measures are activated.

3.3.1. Pseudonymisation

According to art 4 (5), "*Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"*

What are the mandatory items?

- manner of processing
- no longer identification to a specific data subject without additional information
- additional information in another place AND measures to blur or mask the link to an identified or identifiable natural person

According to art 25 1., the **Pseudonymisation** defines the technical and organisational measures "which are *designed to implement data-protection principles"*[16]*.*These measures are integrated in the design it self by several types of descriptive documentation:

Where are the items of Pseudonymisation?

- **Scope document**: describe the activity/application, its context and the data required for processing
- **Functional analysis:** describe the functionalities of an activity /application, the worklow
- **Processes** (to-be/ as-is)
- **Data mapping**: describe the links (=method) between data models (= definition), their role (= process).
- **Technical scope** or specification: includes the description and purpose of algorithms' choice.
- **Testing**: test case, Unit test to control the set implementation

Why are they implemented?

They are defined at the early stage of design to guarantee the most efficient protection of personal data for the data subject and ensure the operator (controller and/or processor) "*to be able to demonstrate that processing is performed in accordance with this Regulation" (see art 24 1.).* The privacy by design is one of the general obligation for the controller.

3.3.2. Data minimisation

According to art.5.1(c), data minimisation is a distinctive feature of personal data:"*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*"

What are the mandatory items?

- adequate
- relevant
- limited for use and processing

According to art 25.1, Data minimisation aims:"*in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."*

16 See Art 25 1., GDPR

The main purpose of Data minimisation is to reduce to bare necessities:

1. to reduce the amount of collected data processed to the strictly requirement
2. to reduce the processing operations

3.3.3. Security of Personal Data

Within **security of personal data** (art 32), the controller implements appropriate technical and organizational measures including *inter alia* :

- Pseudonymisation and encryption (e.g. online banking, online payment, e-commerce)
- Ensure confidentiality, integrity; availability and resilience of processing system *(e.g. prevent hacking*).
- Restore availability and access in time in case of incident (*e.g. server down*).
- Regular security test (e.g. IT quality management)
- Risk assessment
- Code of conducts (art40- 41): when enterprises decide to implement a code of conducts, the monitoring compliance and the approval must be undertake by the supervising authority or a body (regarding its independence and expertise in relation to the subject-matter)
- Certification (art 42):

3.3.4. Privacy by default

The art 25.2 states that only the personal data required have to be processed and what are the conditions of their processing:

- **personal data which are necessary for each specific purpose of the processing**: the controller or processor must define within a scope list of personal data and their use
- **personal data definitions**:
  1. *the amount of personal data collected*
  2. *the extent of their processing*

Please note

The Right to restriction of processing is defined within **art. 18**:"*The data subject shall have the right to obtain from the controller restriction of processing*".The data subject can now lodge a complain to fix the limitation of processing or object of processing (see art. 21) following conditions:

1-The data subject contest the accuracy of personal data
2-The processing is unlawful (see art. 6)
3-No need longer of such data
4-The data subject launched objection to processing

3. *the period of their storage*
4. *their accessibility: by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*

Please note

The right to access is defined within **art. 15:** "*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being*

processed, and, where that is the case, access to the personal data and the following information". The art 15 provides more precision and confirms these 2 conditions too:

1) period for which the personal data will be stored, or, the criteria used to determine that period
2) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations

This accessibility has to be mentioned within either the consent agreement from the data subject (see art. 7) or the information and access to personal Data (See art.13 and 14).In this latter case, the art. 14 confirms these both conditions:

- the period for which the personal data will be stored

- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability

- **Obligation for the controller and processor:** this duty is reported through the obligations stated in art 13 and 14. The controller and or processor must inform the Data subject about the processing of personal Data

4. REMEDIES, LIABILITIES AND PENALTIES

4.1. Sanctions

From art. 77 to art. 84, the GDPR states a pane of sanctions:

1. Right to lodge a complaint with a supervisory authority
2. Right to an effective judicial remedy against a supervisory authority
3. Right to an effective judicial remedy against a controller or processor
4. Suspension of proceedings
5. Right to compensation and liability
6. Administrative fines

To make it short, every Data subject can file a plea without prejudice to any other administrative or judicial remedy or non-judicial remedy against supervising authority or against controller and or processor .

4.1.1. Trial case against a controller or processor

According to art.82, "*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered*".

Then any data subject that suffers a non-materiel damage (personal data are not material) can start a trial in some cases:

- personal data linked to an identified natural person (Pseudonymisation)
- personal data linked to an identifiable natural person (Pseudonymisation)
- no respect of restriction (Data minimisation)
- no minimisation (Data minimisation)
- data breach: the additional information is not kept separately
- no consent
- no information or communication

4.1.2. Administrative fines

The infringements for a controller or processor in case of lack in privacy by design or by default are related to information duty, consent and main obligation of a controller and or processor:

- specific child's consent (art 8)
- duties of controller and processor (art **25** to 39)

Maximum: up to 10 000 000 EUR or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

5. LINK REPOSITORY

5.1. European sources

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

http://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html

https://www.enisa.europa.eu/topics/data-protection/privacy-by-design

5.2. International Sources

https://www.ryerson.ca/pbdce/about/ann-cavoukian/

https://www.ipc.on.ca/english/privacy/introduction-to-pbd/

https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies/

https://www.manager-go.com/management-de-la-qualite/dossiers-methodes/pdca-deming-en-pratique

https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:en

http://the9000store.com/iso-9000-tips-iso-9001-requirements/iso-9000-tips-corrective-and-preventive-action/

5.3. Miscellaneous

http://www.wordtemplatesonline.net/statement-of-work-template/

http://www.relevantbusinesssolutions.co.uk/782-2/

https://templates.office.com/en-us/Gantt-project-planner-TM02887601