Ladies and gentlemen,

On reading these guidelines, I had the impression that I was re-reading Article 25 and recital 78 without any real input for practitioners in the implementation of the approach.

We could summarize these guidelines as : Carrying out a processing form (Art 30) and an impact assessment (Art 35) before any new processing operation allows data protection to be taken into account right from the design stage. (Art 25)
Since when is compliance with one article based on compliance with other articles?

I also find it surprising that these guidelines do not mention privacy-enhancing technologies.

I therefore suggest that you read the last article I wrote on the subject to better understand the spirit of this approach, which is, however, perfectly summarised in Article 25 and recital 78.

I am at your disposal to discuss my comments.

Yours sincerely.

Alessandro FIORENTINO
Vice-President of the Privacy Tech Privacy by Design Ambassador for France
Phone : +33685789504
Email: alessandro@privacytech.fr

Data protection by design

Some refer to it as an approach, a promising concept, a set of principles or an article of the general data protection regulation. She's much more than that.

The concept of Privacy by Design is a set of principles and practices that govern the relationship between people and information.

It is a paradigm, a way of looking at things, a coherent vision of the system based on a defined basis, a disciplinary matrix, a theoretical model.

It is a form of design rail whose laws are intended for designers to express how an ab initio information system should be designed and thought out in its broad outline to ensure IT compliance and freedoms.

A paradigm shift

The General Data Protection Regulation adopted on 27 April 2016 is now at the heart of business concerns. We're talking about a paradigm shift. For many, the application of the principle of "accountability" introduced by paragraph 2 of article 5 entails a shift from a declarative logic to an accountability logic.

This analysis is correct, but it is important to stress that the Regulation is also based on a multitude of principles that reflect a proactive obligation.

Data protection by design introduced by Article 25 is the key to this proactivity. It is a form of temporal indicator, it situates the place of personal data protection in time.

Article 25: Data protection by design

If we were to retain the essentials, data protection by design implies implementing technical and organisational measures that we must determine upstream in order to frame data protection and provide data subjects with an optimum level of protection without any intervention on their part.

In order to understand all that Article 25 implies, we must go back to the origins of the concept.

The origins of the concept

This concept was created in Canada in the 1990s by Dr. Ann CAVOUKIAN in her capacity as Information and Privacy Commissioner of Ontario.

At that time, the protection of personal data was not yet a concept synonymous with economic issues. Driven by the defense of the fundamental freedoms of the individual, Ann CAVOUKIAN presents the concept of Privacy by Design as a step towards ensuring the protection of privacy.

At the origin of the concept of Privacy by Design are the "Privacy Enhancing Technologies" (PETs). Privacy by Design is an evolution of PETs.

The term PET first appeared in 1995 in the report "Privacy Enhancing Technologies: The Road to Anonymity".

The report was the result of a joint project between the Dutch data protection authorities and the Office of the Information and Privacy Commissioner of Ontario. Ann CAVOUKIAN on the Canadian

side and John BORKING on the Dutch side played a key role at this time. They presented a new approach to privacy protection.

PETs are at the origin of the principle of "data minimization", it is on the basis of this principle that the concept of Privacy by Design was developed.

An ethical approach

Based on the principle that the protection of personal data could not be ensured simply by complying with the legal framework, which is sometimes out of step with current technologies, this approach requires that any technology that uses personal data should incorporate technical privacy protection features from its conception and comply with them throughout the data life cycle.

This approach makes it possible to carry out IT projects in compliance with the various legal frameworks in order to protect the personal data of the people concerned by these projects.

It is a question of anticipating all potential abuses and the risks of abusive exploitation of data. This concept of Privacy by Design is a solution that will allow us to deal with it.

The concept is translated into French as protection intégrée de la vie privée (PIVP), or Privacy by Design by the Office of the Information and Privacy Commissioner of Ontario.

The approach is based on seven fundamental principles, and represents a solution allowing technologies to evolve without infringing on the privacy of individuals, a healthy and sustainable coexistence of digital and individuals.

These seven basic principles can be applied to all categories of personal data, to all organisational measures, as well as to all technical devices necessary for their implementation. These must be appropriate to the sensitivity of the data processed.

The aim is to give the data subject back control over his or her data. By respecting the seven fundamental principles developed by Ann CAVOUKIAN, all companies that process personal data will then be able to adopt a responsible and sustainable approach while benefiting from a competitive advantage. This could even be seen as the birth of a form of digital corporate social responsibility.

The seven fundamental principles

Here are the seven fundamental principles published in August 2009, these principles are followed by Alessandro FIORENTINO's personal reading on each of them:

1. Take proactive and non-reactive, preventive and non-corrective measures. (Corresponds to Article 25.1)

Integrated privacy protection (IPPP) is characterized by proactive rather than reactive measures. It involves anticipating and preventing privacy incidents before they occur. Indeed, the PIVP does not wait for privacy risks to materialize, nor does it propose any solutions to resolve privacy breaches that have already occurred. Rather, it is intended to prevent them. In short, integrated privacy protection comes before and not after such incidents.

This principle emphasizes that the concept of Privacy by Design does not offer any corrective solution in the event of a breach of privacy, its implementation must be part of the life cycle of a digital project from its conception.

It is a matter of anticipating privacy incidents before they occur, and this first principle puts the importance of acting upstream at the forefront.

This principle is a form of temporal indicator, it situates the place of personal data protection in time.

2. Ensuring implicit protection of privacy (corresponds to Article 25.2)

One thing we can be sure of is that built-in privacy protection is implicit. It aims to provide maximum privacy by ensuring that personal information is systematically protected within computer systems or as part of internal practices. So an individual's privacy is protected even if he or she does nothing, because privacy protection is built into the system, implicitly.

The first step is to ensure the minimization of the collection of personal data and to offer the maximum privacy to the user, privacy protection is not optional, indeed a user must benefit from maximum protection without any intervention on his part.

The concept of "implicit protection" defines the protection of personal data as a convenience that aims to protect the individual interest of each person, a form of digital literacy or decency.

This second principle is today known as Privacy by Default and is set out in paragraph 2 of article 25 of the General Data Protection Regulations of 27 April 2016.

3. Integrate privacy protection into the design of systems and practices (Corresponds to section 25.1)

Integrated privacy protection, as the name suggests, is built into the design and architecture of an organization's computer systems and practices; it is not grafted onto them after the fact. Privacy protection therefore becomes an essential part of the core functionality. It is an integral part of the system, without prejudice to its functions.

This principle defines privacy protection as an element to be integrated into the design and architecture of computer systems, as well as in the practices of organizations.

The protection of personal data must be an integral part of the system and of the organisational strategy of the organisation without affecting its core functions.

4. Ensure full functionality in a positive-sum paradigm, not zero-sum paradigm (Corresponds to Article 25.1)

Integrated privacy protection seeks to address all legitimate interests and objectives involved in a positive-sum paradigm, not an outdated zero-sum approach that requires unnecessary trade-offs.

Built-in privacy avoids these false dichotomies, such as the dichotomy between privacy and security, by demonstrating that it is truly possible to achieve both objectives at the same time.

The purpose of this principle is to impose an implementation of the concept of Privacy by Design without harming the business, taking into account all the legitimate interests and objectives of the organization. Data protection shall not take precedence over the smooth running of business.

The concept of Privacy by Design is not an adversary of business, they are both partners and complementary in a positive-sum paradigm.

Data protection from the design stage must be considered by all the organization's staff, and more particularly by the sales function, as an invaluable added value. It enables the parameter of user or customer confidence, a major element in customer relations, to be maintained.

5. Ensure end-to-end security for the entire retention period of the information (Corresponds to section 25.1 and section 32)

Integrated privacy protection, when built into the system before the information it contains is collected, persists securely throughout the entire retention period of the information, so that security measures critical to privacy are implemented from start to finish. This ensures that the data is securely stored and then securely destroyed at the end of its retention period. As such, Integrated Privacy Protection ensures comprehensive, secure, end-to-end management of information throughout its retention period.

This principle calls for the security of information throughout its lifecycle, which is referred to as comprehensive management to ensure that the data is kept securely and destroyed at the end of the retention period.

6. Ensuring visibility and transparency (Corresponds to Article 5.2)

With integrated privacy protection, all stakeholders will be assured that regardless of the practices or technologies employed, the system is operating in accordance with the promises and objectives set out, subject to independent audit. The components and operation of the system remain visible and transparent to both users and providers. Verification builds trust.

Privacy by design ensures the controller that the system operates in accordance with the promises and objectives set.

Each of the elements integrated into the systems inherent to the protection of personal data must remain visible and transparent in the event of independent verification, this principle aims to maintain a high level of confidence.

7. Respecting the privacy of users (corresponds to the emphasis on the importance of control of the data subject in recital 78)

Above all, integrated privacy protection requires designers and users to put the interests of individuals first by providing, among other things, strong and implicit privacy safeguards, appropriate notice requirements, and enabling and user-friendly, user-centred functions.

This principle imposes on the designers who develop the project and on the users who will use the project once developed, to always give priority to the interests of the individual, i.e. the people concerned by the data managed via the project or having access to it via webservice. The principle places the protection of the user's personal data at the centre of all considerations.

This principle is not independent, it is intertwined with the other six principles, it requires designers to provide the systems or products they develop with a certain "adequacy", in line with user expectations and legal requirements.

As in the second principle, it can be seen as a form of savoir vivre or numerical propriety that must be present within the system.

Towards legal recognition of the paradigm

A recommendation of the European Parliament to the Council of Ministers on strengthening security and fundamental freedoms on the Internet published on 26 March 2009 marks for the first time Europe's commitment and support in promoting the concept of Privacy by Design. "Data protection and privacy should be introduced as early as possible in the life cycle of new technological developments, ensuring a user-friendly environment for citizens".

In 2010, the European Data Protection Supervisor Peter HUSTINX points out that the current legal framework already imposes the obligation to implement PETs via Recital 46 and Article 17 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In October 2010, the concept of Privacy by Design was recognized as an international privacy standard following the unanimous adoption of a landmark resolution at the International Conference of Data Protection and Privacy Commissioners in Jerusalem.

The adoption of the general data protection regulation on 27 April 2016 gives legal recognition to this approach.

Article 25 of the Regulation integrates the consideration of data protection by design and data protection by default, these two notions take over the original concept.

Privacy enhancing technologies

PETs (Privacy Enhancing Tehcnologies) are these key tools, they are applications and mechanisms integrated into services, online platforms and information systems that make it possible to protect personal data and control the use made of it. These mechanisms allow users to control, minimize or anonymize the data they share.

In some cases, they may also negotiate the terms and conditions for the processing of their data by online applications or services. PETs are intended to cover one or more of the fundamental principles on which the concept of Privacy by Design is based or to meet data protection requirements through technical devices within the information system itself.

Compliance with retention periods is one of the most relevant examples, a TEP to meet this requirement would consist of mapping the categories of data present in the information system and the retention periods inherent in each of them, in order to automate the purging of data when the time comes to ensure the life cycle of the data until it is destroyed.

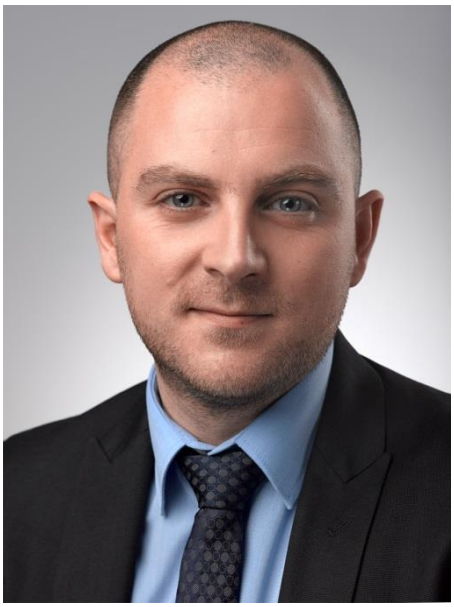
We could also consider a PET that would define the maximum number of records that could be extracted to limit potential data leaks.

Data encryption is also one of the key technical devices in the implementation of a Privacy by Design approach.

The implementation of these privacy-enhancing technologies will represent a real added value to ensure the legal security of the organisation and will ensure the confidence factor of users or customers. In accordance with Article 25, these measures must nevertheless remain appropriate in relation to the processing operations concerned.

Who am I?

Alessandro FIORENTINO



Privacy by Design Ambassador

Responsible for the personal data protection offer of Infhotep and Vice-President of the Privacy Tech association.

Alessandro FIORENTINO began his career as an analyst programmer, he then assumed the role of information systems architect in a large group of wealth management brokers.

Holder of a Master's degree in Management and Protection of Personal Data from the Institut Supérieur d'Electronique de Paris (ISEP), he defended a professional thesis on the implementation of Privacy by Design.

Named "Privacy by Design Ambassador" on May 22, 2013 by the Office of the Information and Privacy Commissioner of Ontario, Canada, PbD promoter Alessandro Fiorentino is part of an exclusive group of individuals and organizations that apply the principles of "Privacy by Design" in their work.

He works on several innovation and prospective projects related to the concept, and is currently in charge of the Privacy by Design teaching unit within the Master's Degree in Management and Protection of Personal Data at the Institut Supérieur d'Electronique de Paris (ISEP) and the DPO Methodologies teaching unit within the Master's Degree in Management and Protection of Personal Data at the Institut Mines-Telecom Business School.