WAVESTONE

# PRIVACY BY DESIGN

## ANTICIPATE TO PROTECT BETTER

**The European Personal Data Protection regulation introduces several major concepts, one of the most important being the obligation to ensure data protection at conception, summed up by the term "Privacy by Design".**

**Adopting a Privacy by Design approach means integrating the right to privacy, right from project conception, i.e., ensuring the relevance of data collected, understanding the risks to the persons concerned, anticipating information and the rights to it, etc.**

The French  Data Protection law named "Information and Liberties" (like many other laws about personal data protection from European countries that follow the European directive about personal data protection), via its article 34, already required the person responsible for data processing to "take all the necessary precautions, with regard to the nature of the data and the risks presented by its processing, to preserve the data's security" but did not explicitly impose the implementation of a Privacy by Design approach. Given this, few organisations have already taken such an approach.

Privacy by Design however allows **minimizing the effort made to comply with the law by avoiding a compliance effort later on**, usually needing projects to adapt the existing setup, which are difficult organizationally, technologically complex and expensive.

Given regulatory deadlines, in order to best handle compliance requirements, the first Privacy by Design initiatives are beginning to multiply. Our experience shows that there are several key success factors to take into account: be super-pragmatic in the definition of a Privacy Impact Assessment, avoid creating a process that does not correlate with the existing one, focus energy on the most sensitive projects and provide tools to project managers.

## AUTHORS

RAPHAËL BRUN
raphael.brun@wavestone.com

THIBAULT LAPEDAGNE

## CREATE A PRAGMATIC PRIVACY IMPACT ASSESSMENT METHODOLOGY

Rather than start from scratch, peers' studies can provide inspiration. In particular, the CNIL (French Data Protection Agency) decided to support persons in charge of automated data processing wishing to take on Privacy by Design by publishing a revised version of its privacy risk management guide in July 2015. It is adapted to the position of European regulation and experience by proposing a method for carrying out Privacy Impact Assessments (PIA).

> Besides the French Data Protection Agency's EIVP method, it is worth considering the following texts:
> - Guidelines of the Article 29 Data Protection Working Party (2015)
> - Norm project ISO/IEC FDIS 29134 (2017)
> - English (2014) and Belgium (2017) national authorities' recommendations

The guide sets out the way to use the EBIOS method, already well known for information security, for the subject of Personal Data Protection. The first two steps aim respectively at identifying the specific context for data processing, and identifying the necessary measures to respect fundamental legal principles: respect for the purpose, relevance of collected data, personal information, exercise of rights, data security and accomplishing the formalities. Next comes the risk analysis step, during which relevant threats are identified and associated with events of three main categories: unauthorized access, modification or loss of personal data. The risks linked to Data Protection compliance are assessed in terms of seriousness and probability and a decision must be made to accept them or not. The EBIOS risk analysis method aims to be exhaustive. This generally requires organizations that use it for information security risk analysis to involve security integration teams in projects in order to dedicate enough time to supporting project managers and to be competent with the method, often perceived as complex.

Teams in charge of compliance are generally neither organised nor large enough to support all an organisation's projects based on such a time-consuming method.

Systematically carrying out EBIOS risk analyses for Personal Data Protection risks thus often seems too ambitious given the resources to commit and also risks over-burdening the project manager and hindering efficient project methodology.

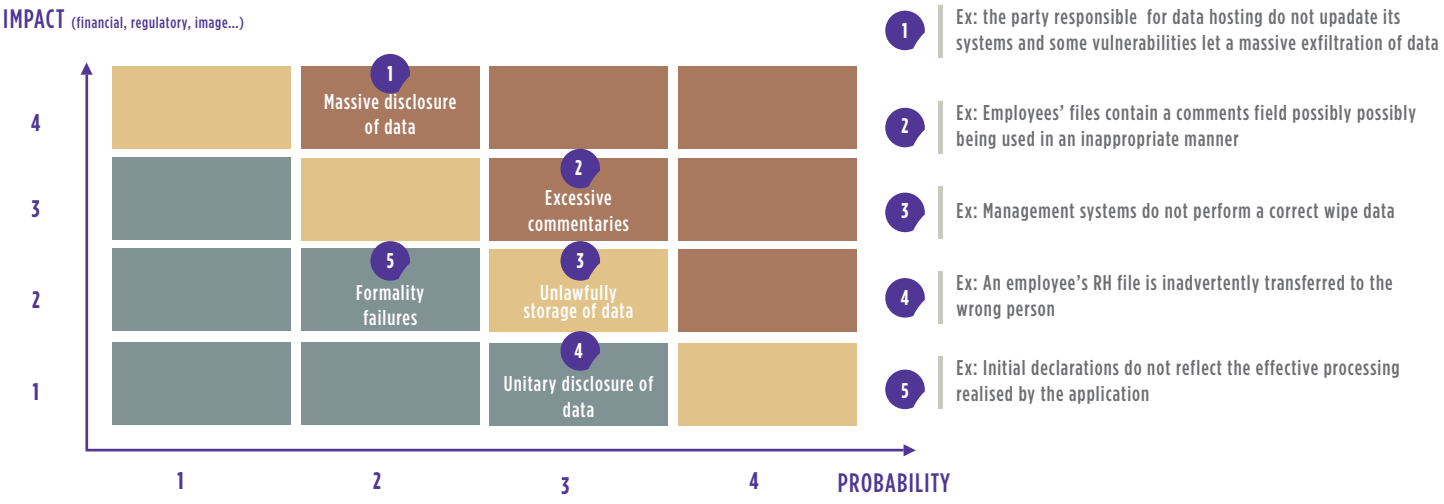
It is therefore up to the DPO[1] to adapt and simplify the risk analysis method that they wish to use to the teams' ability to provide support. Several means are possible: completing a simple risk pre-qualification questionnaire to prioritize efforts between projects; limiting the number of risk scenarios to analyse; reducing the lists of applicable threats to the context; pre-identifying typical risks, etc.

## INTEGRATE IT INTO EXISTING PROJECT METHODOLOGY

One pitfall often met for new methods is the desire to base them on a new process, specific to the subject being dealt with i.e. compliance with the GDPR, that can then be implemented within the organisation. This approach tends to be doomed to failure with time-wasting, lack of understanding of project managers' methods and redundancy of requests.

The Data Protection Officer should rather aim to integrate key steps, committees, deliverables, etc., into the project management

Example of a risk matrix for a staff file management application project



process. Teams such as Operations or Quality for example, are generally responsible for project methodology and can support the officer in their understanding and challenge their proposed amendments.

For several years many organizations have already amended their project management processes to integrate information security requirements. The success of this exercise often depends on the right distribution of work within the projects main phases. These can be broken down into:

- **Preliminary study:** evaluation in order to identify the most sensitive projects and prioritize the support effort. A detailed information security risk analysis will only be carried out for the most sensitive projects.
- **Conception:** identification of the security requirements to take into account by each stakeholder.
- **Implementation:** following up the correct implementation of chosen measures to respond to requirements.
- **Testing:** carrying out security testing to confirm that security requirements have been taken into account and that the measures are efficient. This is often complemented by a security audit or intrusion test.

Since the issues are similar, the same method is fully adaptable to a Privacy by Design context. The errors to avoid are also the same: understaffed support teams for the project managers, complexity of the method, absence or lateness of testing to validate compliance and the end of the process, lack of implication from stakeholders responsible for compliance in key committees.

Ideally, Privacy by Design aims to evolve current methods for integrating security in projects, as this approach is already proven and well known by project stakeholders.

## IDENTIFY SENSITIVE PROJECTS TO PRIORITISE SUPPORT EFFORTS

In the majority of organizations, the volume of projects is too high for compliance teams to be able to support each one, and in particular carry out even a simplified risk analysis. It is therefore necessary to adapt PIA's systematic approach by identifying the projects that present an acute sensitivity as early as possible in order to prioritize support efforts.

Project managers, not often familiar with the GDPR, can find themselves in difficulty when required to express their project's sensitivity in terms of the regulation. It is therefore necessary to support them during this stage by providing a list of questions understandable to a layman.

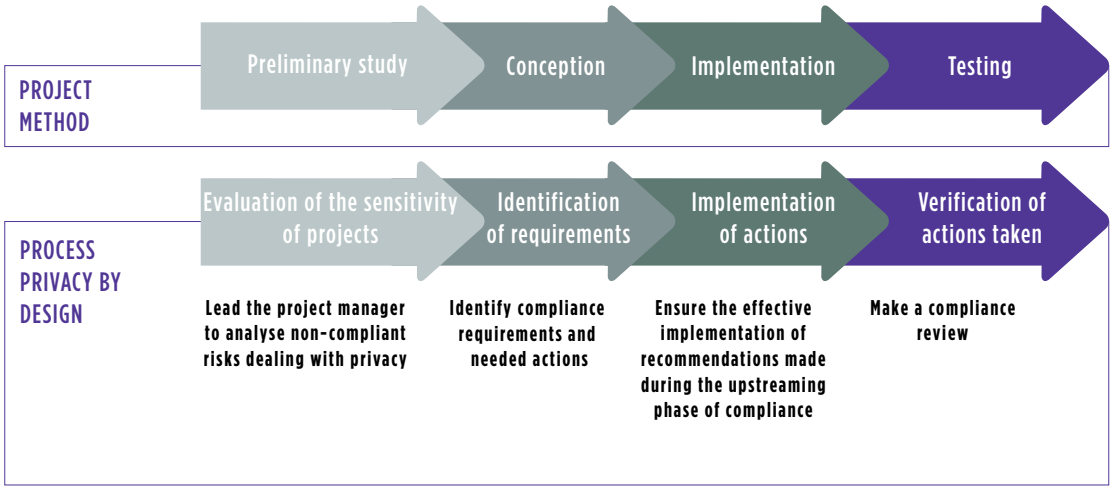
> The Personal Data Protection officer should rather aim to integrate key steps, committees, deliverables, etc.

In reality, several factors can make a project sensitive, for example, handling sensitive data in the context of transfers outside the European Union. Other more indirect factors to the regulation may also be identified: use of new technologies such as Big Data, or the existence of sensitive data in the organisation's context, such as the identity of staff working close to carcinogenic substances.

It is necessary to identify the list of criteria making a project sensitive in terms of the organisation's specific context and the risks attached to it.

Providing autonomy to the project manager leading this stage gives assurance that all projects will undergo an assessment of their sensitivity in relation

Privacy by Design integrated into project methodology




to the GDPR. Finally, by associating compliance teams with project teams during the Preliminary Study phase, the project managers' analysis can be challenged prior to validation.

It is a good idea to adapt the compliance team's investment to the sensitivity of projects. From a remote follow-up of the least sensitive projects (providing compliance guides, answering expertise requests, etc.) to a close follow-up for the most sensitive projects (specific Privacy work groups, detailed risk analysis, checking deliverables, expressing compliance requirements, steering compliance testing, etc.)

In each case, the team should maintain a list of projects, sensitivity assessments and ensure their presence at the right management forums to have access to the current status of the project (creation, on hold, etc.) and to have a direct access to the project portfolio that more advanced organizations maintain.

## PROVIDE TOOLS TO PROJECT MANAGERS

Since not all projects can be supported closely by the compliance team, project managers who need to handle the compliance requirements autonomously need to have the tools to assist them, generally a guide to compliance with the GDPR. This guide does not have to resemble a legal document but rather a clear, explicit and understandable transposition of the regulation for a layman and should support the project manager to select the best measures to comply, whether organizational or technical.

One of the topics requiring special attention is for example the transfer of data to third parties or outside the European Union. Data transfer – which can include a simple data flow via network equipment, mail hosting in the Cloud or consulting data on a website – needs to be set out clearly in order for the project manager to identify on his/her own which data transfers occur in the context of the project. Clause templates could be included in the guide, for integration in contracts with third parties or using a list of subsidiaries that signed Binding Corporate Rules to ensure that international transfer has been authorized.

This compliance guide can be associated with a template test booklet, to check that all the fundamental legal principles have been respected. A list of a dozen of questions will help the project manager to check the main points and validate overall compliance with the GDPR: have the disclaimers been added? Are there specific clauses in contracts? Has the data retention period been defined and the methods of deletion studied?

In the medium term, the tools can go further by offering project managers technical solutions to facilitate compliance. Shared encryption or data anonymization platforms, or compliant data collection processes could be created. Existing information security investments have a strong potential for exploitation.

## PROCESSES TO CREATE, TEAMS TO DEPLOY THEM

The DPO and its team need to be pragmatic to adapt existing processes by including their essential requirements while identifying the most sensitive projects that need extra vigilance.

Beyond the process itself, as early as possible the DPO needs to ask the question of resource requirements to support these projects: how many staff need to be mobilised to comfortably support the project managers? What skills are expected from these teams (legal expertise, business knowledge, ability to interact with IT or security teams, project management skills, etc.)? What collaboration and sharing is possible with existing business areas (information security, compliance, continuity, etc.)?

These are the many questions that need to be answered to successfully deploy a Privacy by Design process, the critical element for ensuring that this obligation becomes an opportunity!

1. DPO : Data provacy officer

WAVESTONE

www.wavestone.com

Wavestone is a consulting irm, created out of the merger of solucom and Kurt salmon's european activities (excluding retail & Consumer goods Consulting) and one of the leading independent consultancy groups in europe.

Wavestone draws on its operational, sector-speciic and technological expertise to enlighten and partner business leaders in their most critical decisions