WAVESTONE

PRIVACY BY DESIGN

ANTICIPER POUR MIEUX PROTÉGER

Le règlement européen sur la protection des données à caractère personnel (RGPD) introduit plusieurs concepts majeurs dont un particulièrement structurant qui donne obligation d'assurer la « protection des données dès la conception » qui se résume par un terme consacré, le « Privacy By Design ».

Adopter une démarche de Privacy By Design c'est intégrer le respect de la vie privée dès la conception des projets, c'est-à-dire s'assurer de la pertinence des données collectées, comprendre les risques pour les personnes concernées, anticiper l'information et le droit d'accès, etc.

La Loi Informatique et Liberté, via l'article 34, demandait déjà au responsable de traitement de « prendre toutes les précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données » mais n'imposait pas explicitement la mise en œuvre d'une démarche de *Privacy By Design*. De ce fait, peu d'organisations ont déjà mis en place une telle démarche.

Le *Privacy By Design* permet pourtant de **minimiser les efforts fournis pour se conformer à la Loi en évitant la mise en conformité *a posteriori*** qui demande souvent le déploiement de projets d'adaptation de l'existant difficiles organisationnellement, technologiquement complexes et financièrement coûteux.

Au regard des échéances réglementaires, et afin de mieux traiter les contraintes de conformité, les premières initiatives de *Privacy By Design* débutent et se multiplient. Nos retours d'expérience montrent que plusieurs facteurs clés de succès sont à prendre en compte : **s'armer de pragmatisme** dans la définition de *Privacy Impact Assessment*, ne pas concevoir un processus décorrélé de l'existant, concentrer l'énergie mise en œuvre sur les projets les plus sensibles et outiller les chefs de projets.

AUTEURS

RAPHAËL BRUN
raphael.brun@wavestone.com
THIBAULT LAPEDAGNE

CONCEVOIR UNE MÉTHODOLOGIE DE PRIVACY IMPACT ASSESSMENT PRAGMATIQUE

Plutôt que de repartir de zéro, il convient comme souvent de **s'inspirer des travaux de réflexion menés par ses pairs.** En particulier, la CNIL a décidé d'accompagner les responsables de traitements désireux de s'engager dans le *Privacy By Design* en publiant en juillet 2015 **une version révisée** de son guide de gestion des risques sur la vie privée. Elle l'adapte ainsi au positionnement du règlement européen et aux retours d'expérience en proposant une méthodologie pour mener des *Privacy Impact Assessment* (PIA).

> En sus de la méthode EIVP (2015) de la CNIL, il convient notamment de s'inspirer de :
> - Lignes directrices du G29 pour les AIPD (2017)
> - Projet de norme FDIS ISO/IEC 29134 (2017)
> - Recommandations des autorités nationales anglaises (2014) et belges (2017)

Le guide décrit la façon d'employer la méthode EBIOS, déjà très connue et reconnue pour la sécurité de l'information, sur le sujet *Privacy*. Les deux premières étapes visent respectivement à identifier le contexte particulier aux traitements mis en œuvre par le projet et à identifier les mesures nécessaires au respect des principes juridiques fondamentaux : respect de la finalité, pertinence des données collectées, information des personnes, exercice des droits, sécurité des données, accomplissement des formalités. Puis vient l'étape dite d'analyse des risques durant laquelle les menaces pertinentes sont identifiées et associées aux évènements redoutés suivant trois grands types : accès illégitime, modification ou disparition des données personnelles. Les risques liés à la conformité *Pivacy* sont alors évalués en termes de gravité et de vraisemblance et font l'objet d'une décision quant à leur acceptation.

La méthodologie d'analyse de risques EBIOS vise l'exhaustivité dans l'analyse des risques encourus. Cette exhaustivité impose généralement aux organisations qui l'utilisent pour leurs analyses de risques SSI de s'appuyer sur des équipes d'intégration de la sécurité dans les projets à même de **consacrer suffisamment de temps à l'accompagnement des chefs de projets** et en mesure de maîtriser la méthodologie, souvent perçue comme complexe au premier abord.

Les équipes en charge de la conformité ne sont **généralement ni organisées ni dimensionnées** pour réaliser un accompagnement de tous les projets d'une organisation sur la base d'une méthodologie aussi chronophage.

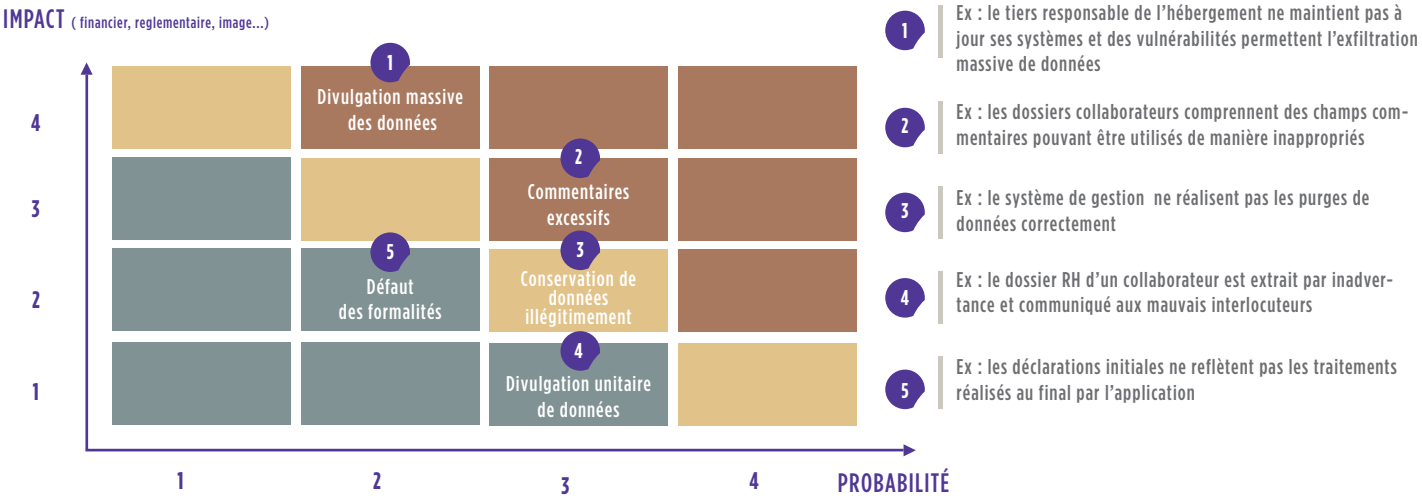
La conduite systématique d'analyses de risques EBIOS pour encadrer les risques *Privavy* apparaît alors souvent comme trop ambitieuse au regard des ressources à engager et risque ainsi d'alourdir de façon démesurée la charge du chef de projet et donc d'entraver le bon déroulement de la méthodologie projet.

Il reviendra donc au CIL[1] ou futur DPO[2] d'adapter et de simplifier la méthodologie d'analyse de risques qu'il souhaite déployer aux capacités d'accompagnement de ses équipes. Plusieurs pistes sont envisageables : réalisation d'un questionnaire simple de pré-qualification du risque pour prioriser les efforts entre les projets, limitation du nombre de scénarios de risques étudiés, réduction des listes de menaces applicables dans le contexte, pré-identification des risques types, etc.

S'INTÉGRER DANS LA MÉTHODOLOGIE PROJET EXISTANTE

Un écueil souvent rencontré pour de nouvelles méthodologies : vouloir s'appuyer sur un nouveau processus, propre au sujet

Exemple de matrice de risques dans le cadre d'un projet d'application de gestion



traité (ici la mise en conformité RGPD), qu'il faudra alors déployer dans l'organisation. Évangélisation chronophage, non connaissance des méthodes de travail des chefs de projets, redondance dans les demandes : autant de raisons justifiant l'échec probable de cette orientation.

Le DPO devrait plutôt chercher à s'intégrer dans le processus de gestion de projet existant : étapes clés, comités, livrables, etc. Des équipes (responsable méthode ou qualité par exemple) ont en général la responsabilité des méthodologies projet et peuvent accompagner le DPO dans sa compréhension et challenger ses propositions d'amendements.

Depuis plusieurs années de nombreuses organisations ont d'ailleurs déjà amendé leur processus de gestion de projet pour y intégrer les exigences de sécurité SI. Un exercice dont la réussite dépend souvent d'une bonne répartition des travaux au sein des grandes phases d'un projet. Il se décompose en plusieurs phases :

- **Étude préalable :** appréciation de la criticité du projet afin d'identifier les projets les plus sensibles et prioriser les efforts d'accompagnement. Une analyse de risques SSI détaillée sera seulement conduite pour les projets les plus sensibles.
- **Conception :** identification des exigences de sécurité à prendre en compte par chacun des acteurs.
- **Mise en œuvre :** suivi de la bonne mise en œuvre des mesures choisies pour répondre aux exigences.
- **Recette :** conduite d'une recette sécurité qui valide la prise en compte des exigences sécurité et l'efficacité des mesures mises en place. Elle est souvent accompagnée d'un audit de sécurité ou de tests d'intrusion.

Les enjeux étant similaires, la même méthodologie est tout à fait adaptable dans un contexte de *Privacy By Design*. Les erreurs à éviter seront alors les mêmes : sous dimensionnement des équipes en charge d'accompagner les chefs de projets, complexité de la méthode, absence ou réalisation trop tardive de la recette visant à valider la conformité en fin de processus, non implication des acteurs en charge de la conformité dans les comités clés.

Idéalement, le *Privacy By Design* cherchera à faire évoluer la méthodologie existante d'intégration de la sécurité dans les projets, celle-ci étant déjà rodée et bien connue des acteurs du projet.

IDENTIFIER LES PROJETS SENSIBLES POUR PRIORISER LES EFFORTS D'ACCOMPAGNEMENT

Dans la majorité des organisations, le volume de projets est trop important pour que les équipes en charge de la conformité aient la capacité d'accompagner chacun

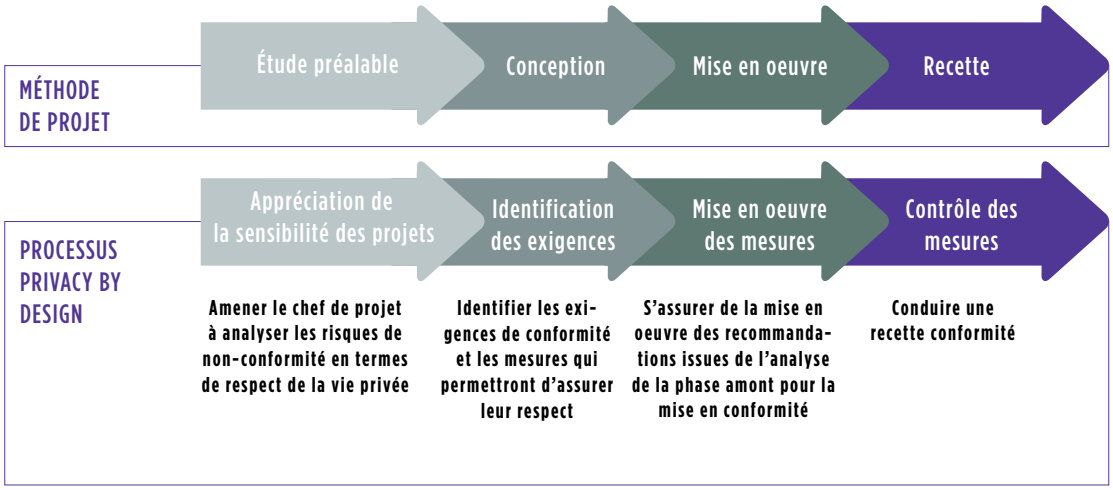
> « Le DPO devrait plutôt chercher à s'intégrer dans le processus de gestion de projet existant: étapes clés, comités, livrables ..»

d'eux et en particulier de réaliser une analyse de risques même simplifiée. Il est donc nécessaire d'adapter l'approche systématique de PIA en identifiant le plus en amont possible les projets qui présentent une sensibilité accrue afin de prioriser les efforts d'accompagnement.

Les chefs de projets, souvent peu familiers avec le RGPD, peuvent se retrouver en difficultés lorsqu'il s'agit d'exprimer la sensibilité de leur projet au sens du règlement. Il est donc nécessaire de les accompagner dans cette étape en leur fournissant une liste de questions simples et compréhensibles par les non-initiés.

Dans la pratique, plusieurs facteurs peuvent rendre un projet sensible. Par exemple, la manipulation de données sensibles au sens du règlement ou la mise en œuvre de transferts hors UE. D'autres facteurs, moins directement liés au règlement peuvent également être identifiés : utilisation de

Le Privacy by Design intégré à la méthode projet



nouvelles technologies (*Big data* par exemple) ou existence de données sensibles dans le contexte de l'organisation (ex : identité des collaborateurs intervenant à proximité de produits cancérigènes).

Il conviendra donc d'identifier la liste des critères rendant un projet sensible en fonction du contexte spécifique de l'organisation et des risques qui pèsent sur elle.

Rendre autonome le chef de projet dans la conduite de cette étape permet de s'assurer que tous les projets feront l'objet d'une appréciation de leur sensibilité vis-à-vis du RGPD. Enfin, en associant les équipes conformités aux comités chargés du suivi des projets en phase d'étude préalable, l'analyse des chefs de projets peut être challengée avant validation.

Il conviendra alors d'adapter l'investissement de l'équipe conformité à la sensibilité des projets. D'un suivi distant pour les projets les moins sensibles (alimentation en guides de mise en conformité, réponses à des demandes d'expertise) à un suivi rapproché pour les projets les plus sensibles (groupes de travail spécifiques sur le sujet du Privacy, analyse de risques détaillée, vérification des livrables exprimant les exigences de conformité, pilotage de la recette conformité, etc.). Dans tous les cas, l'équipe devra maintenir une liste des projets, des évaluations de criticité et s'assurer d'être présente dans les bonnes instances pour avoir accès à l'actualité des projets (création, arrêt…), voire disposer d'un accès direct au portfolio projet qui existe dans les organisations les plus avancées.

OUTILLER LES CHEFS DE PROJETS

Tous les projets ne pouvant être accompagnés de façon rapprochée par l'équipe conformité, les chefs de projets devant traiter la mise en conformité en autonomie devront disposer d'outils pour les aider, généralement un guide de mise en conformité au RGPD. Ce guide ne doit pas ressembler à un document juridique mais bien plus à une traduction concrète, explicite et intelligible du règlement pour un non initié et doit permettre d'accompagner le chef de projet dans le choix des meilleures mesures pour s'y conformer, qu'elles soient organisationnelles ou techniques.

L'un des sujets qui nécessite une attention particulière est par exemple le transfert de données à des tiers ou hors de l'UE. Le transfert de données - qui peut désigner aussi bien le simple transit d'un flux par un équipement réseau, l'hébergement dans le *Cloud* de la messagerie ou la consultation de données sur un site web - sera explicité afin que chef de projet puisse identifier par lui-même les transferts de données réalisés dans le cadre de son projet. Il pourra alors par exemple s'appuyer sur les modèles de clauses proposées dans le guide pour les intégrer dans ses contrats avec des tiers ou utiliser une liste des filiales ayant signées les *Binding Corporate Rules* pour s'assurer que son transfert à l'international est autorisé.

Ce guide de mise en conformité pourra être associé à un cahier de recette type, permettant de contrôler le bon respect des principes juridiques fondamentaux. Une liste de questions restreintes (autour d'une dizaine généralement) aidera le chef de projet à contrôler les points majeurs et ainsi valider la conformité globale du projet au RGPD : les mentions d'information sont-elles bien ajoutées ? Les cases de champs libres disposent-elles d'un *disclaimer* sur leur bonne utilisation ? Les contrats contiennent-ils des clauses spécifiques ? La durée de conservation des données a-t-elle été définie et leurs modalités de suppression étudiées ?

À moyen terme, l'outillage pourra aller un cran au-delà en proposant aux chefs de projet des solutions techniques pour faciliter la mise en conformité. Des plateformes mutualisées de chiffrement ou d'anonymisation de données ou encore des processus de collecte de données conformes pourront être construits. Les investissements déjà réalisés dans la filière sécurité de l'information pourront être largement exploités.

UN PROCESSUS À CONCEVOIR ET DES ÉQUIPES POUR LE DÉPLOYER :

Le DPO et ses équipes devront s'armer d'une bonne dose de pragmatisme pour adapter les processus existants en les alimentant de leurs exigences essentielles tout en identifiant les projets les plus sensibles.

Mais au-delà du processus en lui-même, le DPO devra se poser au plus tôt la question de ses besoins en ressources pour suivre ces projets : combien de personnes sont à mobiliser pour accompagner sereinement les chefs de projets ? Quelles sont les compétences attendues de ces équipes (expertise juridique, connaissances métiers, capacité à interagir avec les équipes IT et SSI, compétences de chef de projets, …) ? Quelle mutualisation possible avec les filières existantes (RSSI, Conformité, RPCA, etc.) ?

Autant de questions auxquelles il conviendra de répondre afin d'assurer au Privacy By Design un déploiement réussi, élément clé pour que cette contrainte devienne une opportunité de confiance dans la transformation digitale !

1. CIL : correspondant informatique et libertés
2. DPO : Data provacy officer

WAVESTONE

www.wavestone.com

Dans un monde où savoir se transformer est la clé du succès, l'ambition de Wavestone est d'apporter à ses clients des réponses uniques sur le marché, en les éclairant et en les guidant dans leurs décisions les plus stratégiques.

Wavestone rassemble plus de 2700 collaborateurs présents sur 4 continents. Il figure parmi les leaders indépendants du conseil en Europe, et constitue le 1er cabinet de conseil indépendant en France.

Wavestone est coté sur Euronext et est éligible au PEA-PME. Wavestone a été labellisé Great Place To Work en 2017.