De manière générale, le document et la méthodologie sont fortement orientés sur les dimensions juridiques. Celles-ci sont globalement bien traitées et accompagnent assez bien le questionnement. En revanche, les points relatifs à la sécurité (Data Protection by Design & Default, sécurité, analyse et gestion des risques) me semblent particulièrement faibles…

Malheureusement, je le constate lors des formations que je dispense, ce sont précisément ces points qui posent le plus de difficultés aux DPO et aux organisations. En effet, l'extrême subjectivité de la gestion des risques et la difficulté, pour les non-experts en analyse et gestion des risques, à réaliser une analyse **pertinente** et dont les résultats sont **justifiables**, **sans se perdre** (ceux qui ne se contentent pas d'une analyse bâclée se perdent dans l'infinité des scénarios).

À mon sens, c'est **le grand apport du Standard Data Protection Model (SDM) allemand**. Avec une vision opérationnelle concrète de la protection et de la sécurité by design, le SDM apporte l'éclairage souvent manquant dans les diverses recommandations et méthodes d'analyse d'impact, dont celle proposée ici par l'EDPB. Malheureusement, le SDM ne fournit pas de méthode pour réaliser une analyse d'impact. C'est la raison pour laquelle j'ai développé ma propre méthodologie, qui mixe globalement le contenu de votre template et le SDM. Il s'agit d'une méthode « libre » (licence CC-BY-SA) que je peux présenter si cela vous intéresse.

Concernant la forme et le format du fichier de template, pour un rapport final, le format « Word » en tableaux est indéniablement pratique (le format docx semi-propriétaire, n'est pas idéal) . Il s'avère cependant être un médiocre outil de collecte d'informations ou de support à l'animation d'une analyse. (En ce sens, un outil informatisé tel que celui de la CNIL n'est pas supérieur.) En effet, la majorité des utilisateurs se contentent, au mieux, d'afficher le template sur un écran lors de sessions de travail, ou, au pire, transmettent le template à divers acteurs en leur demandant de remplir « leurs » cases.

Je suis convaincu que le support influence les pratiques, et ce type de support, d'expérience, engendre une collecte d'informations médiocre, donc une qualité d'analyse faible. Une bonne analyse repose en effet sur la collecte des bonnes informations. Lorsqu'on propose à des personnes de remplir des cases, elles s'enferment dans ces cases. Or, mener une analyse d'impact, c'est explorer les possibles, tout le contraire d'une perspective étroite. Personnellement, pour éviter cela, j'utilise le mindmapping qui permet d'ouvrir et faire des liens entre les éléments abordés. Je pense qu'il est important que **le guide explicatif ne se limite pas à expliquer le template. Il devrait guider la manière de conduire les ateliers, de favoriser la collecte des bonnes informations.** Par exemple, lorsqu'on parle de risques, les bonnes informations ne sont obtenues que si le contexte de l'analyse garantit une certaine sérénité propice à la transparence : les personnes interrogées doivent pouvoir s'exprimer librement. Le guide pourrait également aider à sélectionner les personnes à interroger.

En dehors de cette remarque générale, voici quelques suggestions et commentaires sur des points précis :

- Point 1.1.d (template) / 1.1.4 (documentation) : la case « contexte » me semble trop générale. Elle ne permet pas de guider suffisamment le questionnement sur les éléments de contexte. La diviser en sections thématiques aiderait les analystes.
- Point 1.2 : vous précisez qu'idéalement, la description fonctionnelle devrait être accompagnée d'un diagramme. Je pense que cette recommandation est essentielle et mériterait d'être davantage mise en avant. Je recommande personnellement l'utilisation du langage de modélisation Archimate, qui permet de représenter sur une seule carte : les acteurs, leurs responsabilités, les liens entre eux (sous-traitants, responsables conjoints), les finalités, les données, les applications, les flux et les processus. Ce langage, conçu pour les architectes d'entreprise, est idéal pour cartographier les traitements de données. La réalisation d'une carte Archimate fait partie de la méthode que j'ai créée.
- Point 2.2.b : la description de ce qui est attendu dans la section « Data Quality » est insuffisante. Ne pourrait-il pas y avoir des explications sur l'exactitude, la fraîcheur, la précision, la consistance… ?
- Points 2.3.4/d et 2.3.5/e : la séparation des points suit la logique de scission dans les articles du RGPD, mais dans les faits la sécurité doit faire partie intégrante du « by design ». Séparer les deux engendre de la confusion : certains pensent que la protection by design ne consiste qu'à mettre en place de l'anonymisation, de la pseudonymisation ou du chiffrement. De nouveau, le SDM allemand est probablement une bonne source d'inspiration sur ce point.