Capitaliser sur ses processus pour se conformer au RGPD

Le RGPD, de quoi s'agit-il ?

Le RGPD[i] sert à protéger, à l'échelle européenne, la vie privée de l'individu contre une utilisation abusive de ses données personnelles, alors que les injonctions paradoxales ne manquent pas :
- pour l'entreprise, la donnée est devenue un actif stratégique avec des besoins de corrélation et d'analyse des données massives,
- ladite entreprise s'appuie sur des organisations et des systèmes d'information largement ouverts aux clients et partenaires, avec des services désormais proposés dans le Cloud.
Ce contexte a amené le régulateur, l'Union Européenne, à exiger des entreprises une **capacité à s'autoréguler** et à **prouver la conformité** de leurs **traitements**, en remplacement des exigences de déclarations préalables antérieures.

La **définition d'un traitement** est large : «toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction».

La notion de données est donc une composante essentielle de la RGPD, mais sous un angle synthétique particulier, seules les données personnelles et sensibles nécessitant une protection encadrée par la loi. Les durées de conservation sont également une préoccupation renforcée, pour ne pas dire nouvelle.

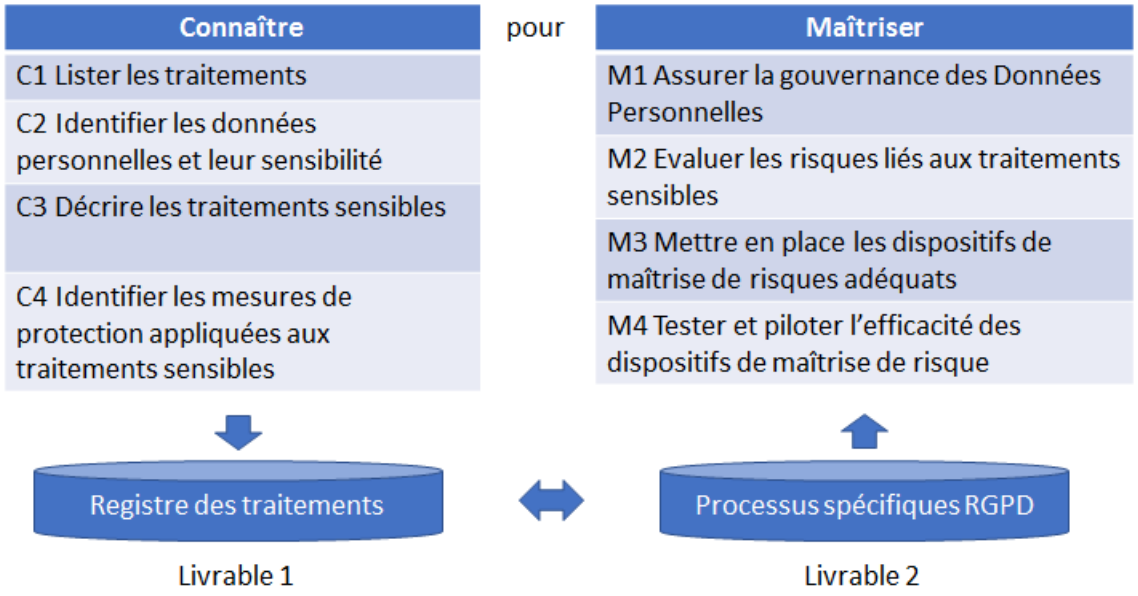
L'enjeu de l'exigence de la **capacité à s'autoréguler** est d'importance, car les sanctions encourues se veulent représentatives des dommages causés aux individus : **là où l'entreprise pouvait jusqu'à présent limiter son évaluation du risque à un impact interne** (par exemple pour un vol de données : une perte d'actif et le cas échéant un risque de réputation) **elle devra désormais considérer la probabilité d'une forte sanction financière**.

Les étapes incontournables

La CNIL propose une démarche en 6 étapes dans un excellent document de synthèse :

1- Désigner un délégué à la protection des données, le DPO, qui va orchestrer les travaux en lien avec les responsables de traitements et les sous-traitants et gérer la relation avec l'autorité de contrôle
2- **Cartographier les traitements** et pour chacun les **catégories de données personnelles exploitées** et compléter cet inventaire selon 5 axes : Qui sont les responsables du traitement ? Pourquoi les données sont-elles traitées ? Où sont-elles hébergées ou transférées ? Combien de temps sont-elles conservées ? Comment sont-elles protégées ?
3- Prioriser les actions suite à une **revue orientée risques et conformité légale des traitements** décrits à l'étape 2. Deux livrables sont attendus : les **premières mesures d'urgence** et l'identification des **traitements à risque**.
4- Ces traitements à risques doivent faire l'objet de mesures de protection adaptées au risque encouru. Elles sont recensées dans le cadre **d'études d'impact sur la protection des données (PIA)**.
5- Les processus internes doivent ensuite porter la préoccupation de protection des données à tous les niveaux, de la conception des applications [Security by Design], aux rapports avec les individus concernés, jusqu'au lien avec les autorités de contrôle.
6- La dernière étape de documentation de la conformité vise à garantir **la pérennité de l'implication de l'entreprise** au-delà du mode projet initial.

A compter de la seconde étape, la présentation suivante pourrait également être proposée :



La contribution de l'approche processus (Connaître)

[C1] Le référentiel processus constitue un excellent support pour identifier la maille pertinente des traitements à analyser, par processus ou regroupement de processus, et donc construire l'inventaire des traitements.

[C2] Une approche « moderne » de la modélisation des processus, permettant un dialogue étroit entre métier et SI, vous aura amené à **formaliser les jalons clés d'un processus** : ces étapes, qui ont vocation à être

- pilotables par le métier,
- et donc matérialisées dans le SI.

En créant un lien entre processus et données à piloter, ces jalons constituent une source précieuse pour nourrir l'inventaire des données métier associées à chaque traitement.

Difficulté supplémentaire qui n'est pas propre au RGPD mais caractérise tout chantier SI ciblé données, il s'agira d'assurer **au sein du référentiel** la cohérence entre **2 visions de la donnée** :

- la vision métier, qui reprendra le vocable familier des parties prenantes
- et la vision SI, qui permettra de faire le lien avec les référentiels de données.

Cette dernière, plus rigoureuse mais aussi plus complexe et fragmentée, peut difficilement servir de base à des échanges avec le métier : il est en effet fréquent qu'une « donnée métier » se traduise au plan informatique par une demi-douzaine de « données SI ». Ainsi, derrière la notion de « client entreprise », se cachent le tiers personne morale, le tiers personne physique, le rôle client, la localisation géographique,…
Seul un sous-ensemble de ce périmètre étant susceptible de porter des données pouvant être qualifiées de personnelles.

[C3] La description des traitements sensibles peut ensuite faire l'objet d'une modélisation spécifique RGPD. La norme BPMN permet de décrire des enchaînements d'opérations manuelles ou automatisées, en qualifiant chacune des opérations, et permet d'indiquer les données utilisées. Le traitement RGPD peut donc être considéré comme un « sous-processus » réutilisable si besoin, dans différents contextes.

[C4] Les mesures de protection appliquées aux traitements sensibles à identifier à cette étape ne concernent à mon sens que les mesures très spécifiques et directes au traitement concerné. De nombreux dispositifs essentiels de maîtrise des risques sur les systèmes d'information ont une portée générale (sur l'accès au système d'information ou les moyens d'extraction de données par exemple) et leur place est dans une approche globale de management du risque (voir ci-dessous les points [M2] et suivants).

[LIV1] Pour produire le registre des traitements il faut établir les liens entre les traitements (et leurs finalités), les acteurs (et leurs habilitations), les données (et leur qualification éventuelle Données Personnelles ou DP sensibles), les applications et les dispositifs de maîtrise de risques (DMR) en vigueur. Par rapport à la norme BPMN, seuls les derniers éléments devront être complétés : les applications et les risques, eux-mêmes reliés aux dispositifs de maîtrise de risques. Si quelques compléments s'imposent, comme l'identification de rôles précis tels que le DPO, le responsable de traitement ou les sous-traitants RGPD, la plupart des informations requises sont probablement déjà disponibles, sous une forme ou sous une autre, dans votre référentiel processus.

[LIV2] Enfin, le référentiel devra **porter les processus requis par le RGPD** :
- concevoir une application ou un traitement. Il s'agira de prendre en compte la protection des données personnelles dès la conception : minimisation de la collecte de données au regard de la finalité, cookies, durées de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données, rôle et responsabilité des acteurs impliqués ;
- traiter les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits : droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement ;
- mais aussi l'ensemble des activités visant à documenter la conformité au RGPD.

Des processus à la gouvernance des données (Maîtriser le besoin de données)

Rappelons que la réalisation de l'inventaire des traitements et des données a amené à se poser les questions suivantes :
- Qui sont les responsables du traitement ?
- Pourquoi les données sont-elles traitées ?
- Où sont-elles hébergées ou transférées ?
- Combien de temps sont-elles conservées ?
- Comment sont-elles protégées ?

La mise en pratique est potentiellement délicate, quand, avec la généralisation de traitements dans le Cloud, il devient parfois impossible de localiser le stockage de la donnée. Les réponses, au-delà d'un inventaire ponctuel, permettent de formaliser et d'**impulser une véritable approche de gouvernance des données** à partir des étapes manuelles et automatisées identifiées et du cycle de vie de la donnée défini par des jalons.

Il restera alors à **construire un dispositif pérenne de gouvernance** :
- en instituant un lien régulier entre DPO, services opérationnels et services IT qui amènera nécessairement à une meilleure maîtrise des données et traitements,
- en appliquant aux données les mêmes règles SI ou métier,
- et enfin pilotant les données (nombre, qualité, ancienneté…).

Management du risque (Maîtriser les risques liés aux données strictement nécessaires)

[M2] [M3] L'identification et l'évaluation des risques liés aux données ne sont pas nouvelles par nature. Néanmoins dans le cadre imposé par le RGPD, les sanctions encourues prennent en compte les dommages causés aux individus là où l'entreprise pouvait jusqu'à présent limiter son évaluation du risque à un impact interne (par exemple pour un vol de données : une perte d'actif et le cas échéant un risque de réputation). De plus :
- des diligences d'évaluation et de traitement des risques sont précisées,
- la notion de responsabilité est étendue, et notamment dans le cadre des traitements sous-traités,
- le cadre fixé est celui des « traitements » là où vos travaux antérieurs se sont sans doute appuyés sur les applications.
L'ensemble de ces éléments devrait amener à restructurer un large périmètre de l'approche « classique » de **cartographie des risques** liés aux systèmes d'information. Les principes restent toutefois les mêmes : identification du risque, évaluation brute, mise en place et de dispositifs de maîtrise du risque et évaluation nette.

[M4] La capacité à documenter la conformité RGPD de l'entreprise sera toutefois fortement consolidée par l'usage d'un outil de Gouvernance des risques et de la conformité (GRC) pour démontrer l'exhaustivité de travaux réalisés et l'efficacité des dispositifs de maîtrise de risques. Ce type d'outil permet d'impulser les travaux récurrents, permettant ainsi de passer d'un mode « projet » de mise en conformité RGPD à un mode permanent d'évaluation des risques et de documentation de la conformité.

En conclusion

La boîte à outil Processus s'avère parfaitement adaptée pour aborder la problématique RGPD et permettra à l'entreprise de maîtriser sa démarche vis à vis des exigences définies par le législateur : maîtrise des bases juridiques de sa collecte d'information, de leur caractère proportionné (nature, durée de détention), de l'exploitation transparente et loyale de l'information…

Elle devra toutefois être complétée par des outils de Gestion des Risques et de la Conformité pour couvrir la dimension dynamique de la Gouvernance du dispositif.

Ce travail contraint par le RGPD offre également l'opportunité de revisiter les processus sous l'angle de l'interaction avec les individus (expérience client, usager, salarié…). La sélection par l'entreprise des seules informations à caractère personnel qui lui sont **strictement** nécessaires peut incidemment conduire, au-delà du respect de la norme imposée, à une meilleure expérience client.

Laurent Hassid

Directeur associé chez BPMS

[i] Règlement Général sur la Protection des Données