RGPD[1], une opportunité pour la Gouvernance de vos données !

La partition Praxeme, un cadre méthodologique pour la direction d'orchestre du DPO[2]

En résumé

Ce *Position Paper* décrit l'intention portée par CONIX et le *Praxeme Institute*[3] dans l'apport d'un cadre méthodologique pour la gouvernance des données au travers du cas du RGPD.

Nos convictions sont les suivantes :

- La gouvernance des données est un des sujets les plus complexes du moment, du fait de sa transversalité, de sa portée à l'échelle de l'entreprise, de sa nouveauté à cette échelle, des innovations data (solutions de capture, stockage, exploitation, traitement, diffusion…), de l'autonomisation des données (sources externes, approche de type *data lake* et *datalab*), du rôle des données de plus en plus important dans les relations clients et de la multiplication des réglementations sur les données.

- L'application du RGPD est l'opportunité de mettre en place cette gouvernance et d'éviter une suite d'initiatives locales sans concertation, sans alignement et vision d'ensemble, pour dépasser les silos.

- Le premier point que doit traiter la gouvernance des données est la capacité d'assurer cette concertation et cet alignement. À l'image d'un DPO face à la diversité des métiers de l'entreprise et qui est attendu sur la bonne application du RGPD. Le dialogue IT / Métier, la concertation entre Métiers sont, comme bien souvent, un élément clé.

- Pour assurer cette concertation et le bon niveau de dialogue, il y a besoin de proposer une grille de lecture orientée données (dont les données personnelles), une partition, un repère commun d'entreprise pour l'ensemble des acteurs, qui leur permettra de « jouer juste » l'application du RGPD au travers de leurs contributions.

- La meilleure façon pour travailler à cette échelle est de s'appuyer sur les pratiques dites d'architecture d'entreprise dont Praxeme fait partie. La vocation de ces pratiques est justement d'être en appui des transformations à l'échelle de l'entreprise comme on l'attend pour le déploiement du RGPD et de la gouvernance associée.

- Au travers de Praxeme et du « Repère Praxeme », nous pensons offrir cette partition, guide pour les différents acteurs dans leur analyse et décision de conception pour l'application cohérente et efficace du RGPD,

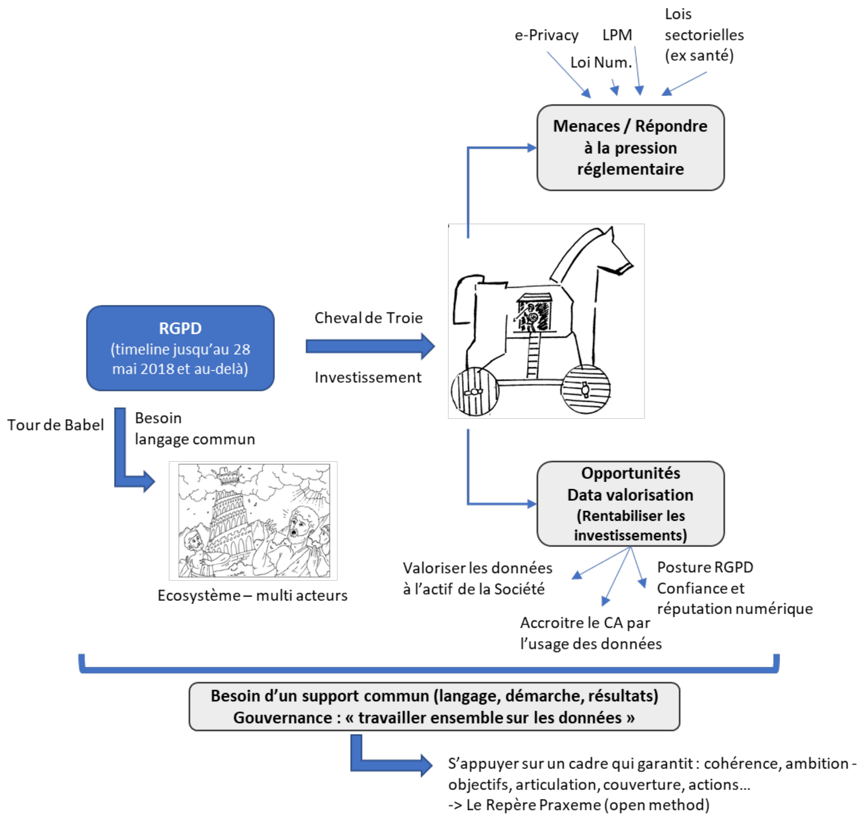
---

[1] Règlement Général pour la Protection des Données - ***Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016*** : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

[2] *Data Protection Officer* ou Délégué à la Protection des Données (DPD).

[3] Praxeme est la méthodologie de transformation d'entreprise, issue de l'initiative pour une méthode publique. Le *Praxeme Institute*, association sans but lucratif, a pour objet le développement et la diffusion de cette méthode. Voir : www.praxeme.org.
CONIX : cabinet de conseil spécialisé dans le domaine de la Data et du réglementaire. CONIX, membre fondateur du *Praxeme Institute*, accompagne la méthode publique Praxeme depuis son origine, et a pris en charge des contributions sur le volet Data : http://www.conix.fr/

- Au-delà, la gouvernance qui sera mise en place dans le cadre du RGPD est un excellent cheval de Troie pour toute entreprise qui vise à maîtriser les données personnelles pour établir une relation de confiance numérique avec ses clients et parties prenantes et plus largement à valoriser ses données comme levier de croissance et de compétitivité accrue.



Le RGPD est un Cheval de Troie pour une gouvernance des données élargie et valorisée.

Ce *position paper* introduit l'idée de « partition », guide pratique pour la mise en place de la gouvernance des données par le déploiement du RGPD.
Il fixe un cadre de contributions à la méthode Praxeme.

La méthode publique Praxeme appréhende l'entreprise comme un système complexe, qu'elle analyse à travers sept aspects soigneusement articulés. Elle favorise une approche interdisciplinaire de la transformation.

L'initiative pour une méthode publique vise à élaborer et diffuser une méthode ouverte et libre de droits (« *open method* »). Les contributions à la méthode sont protégées par une licence « *creative commons* » qui autorise l'usage et la réutilisation de tout ou partie d'un document du fonds Praxeme, sous seule condition que l'origine en soit citée[4].

Parmi les contributions, on trouve des procédés, autrement dit des guides pratiques (modes opératoires) pour appuyer, par exemple, les actions de déploiement du RGPD et de la gouvernance associée.

Une part de ces procédés existe déjà (voir les références *Figure 8* en annexe), d'autres viendront compléter la méthode au fil des contributions autour de la gouvernance des données tel qu'envisagé dans ce *position paper*.

[4] À noter : les documents existent en anglais et en français. Ils sont à disposition sur le site web du *Praxeme Institute* : http://www.praxeme.org/telechargements/catalogue/.

Une opportunité dans un contexte anxiogène

Dans un peu moins de 6 mois[5], le RGPD devra être mis en œuvre. Une abondante littérature sur le sujet a déjà été produite, pour décortiquer et expliciter le règlement.

Nous allons plutôt vous exposer ici notre vision, opportuniste et opérationnelle, enrichie par les retours d'expérience de CONIX et appuyée sur le cadre que propose la méthode d'entreprise Praxeme. Loin de trembler devant le couperet de l'application du RGPD, nous y voyons un levier pour l'un des chantiers les plus complexes de ces dernières années : la mise en place de la Gouvernance des Données.

En effet, toutes les composantes de la Gouvernance des Données se retrouvent dans les attendus et livrables du RGPD. Nous voyons donc le texte réglementaire comme un aiguillon pour adopter les bonnes pratiques, celles qui aideront les entreprises à préparer leur futur.

Or, face à l'énormité du chantier RGPD dans des délais aussi courts, le risque serait de bâtir des livrables focalisés, peu évolutifs, voire jetables, alors même que les premières briques de la Gouvernance des Données pourraient être posées et organisées pour l'Entreprise, dans une perspective de long terme.

Au-delà du RGPD, la donnée devient un actif, une source évidente de revenu.

C'est tout un nouveau pan de gouvernance que les entreprises doivent prendre en main. Rater l'opportunité de mettre en place cette gouvernance au travers du RGPD, c'est rater sa bascule dans le monde des données.

De la problématique au plan d'action

La Gouvernance des Données a, de tous temps, été très difficile à mettre en place, car elle concerne l'ensemble des données de l'Entreprise. Dans ce contexte, il est complexe, quel qu'en soit le sponsor, de prioriser ou de définir un axe stratégique de mise sous contrôle, puis de déploiement, car les données sont éminemment transverses à plusieurs processus, métiers, domaines, ou même classe de risques.
L'organisation de la chaîne de responsabilité dans la Gouvernance vient entrechoquer les silos fonctionnels et/ou organisationnels. Les responsables pressentis peuvent légitimement faire valoir ambigüité ou impossibilité à exercer leur autorité sur l'ensemble de la chaîne de circulation de la donnée, de l'acquisition à l'exploitation.
De plus, dans un contexte budgétaire contraint, la Gouvernance des Données ex nihilo est perçue comme un centre de coûts sans réel ROI direct. Ceci ajoute un élément de complexité, cette fois-ci au niveau des moyens humains et ressources IT pouvant être mobilisés.

[5] Pour le 24 mai 2018

Au fil des tentatives, les entreprises ont bien souvent arbitré la démarche globale après un POC[6] au profit de nouveaux silos partiels, la plupart du temps techniques, autour du MDM[7] ou du DQM[8], sans réellement nommer les *Data Owner* nécessaires, ni les CDO[9].

Dans ce quasi *no man's land* « data », tonne soudain le RGPD, avec son lot de données prioritaires clairement identifiables, de livrables précis (*data lineage*, dictionnaire…), des risques associés très parlant en termes de sanctions mais surtout d'image et de réputation, avec au cœur du règlement, la nomination impérative d'un acteur central : le DPO.

Sans une approche méthodologique rassurante et pragmatique, quelle différence y a-t-il entre les difficultés de mise en œuvre d'une démarche de Gouvernance des Données et l'application du RGPD ? Aucune ! Et c'est pour cela que la mise en application du RGPD prend du retard, car, vue sous le seul angle de la contrainte réglementaire, la tâche est énorme.

Pourtant, l'entreprise a mûri, les dictionnaires même incomplets existent, les processus sont décrits, et les *data lineages* sont à portée de constitution, pour peu que la méthode pour les réaliser soit robuste et pragmatique, les initiatives autour des données se multiplient (*datalab*, *data factory*, DMP[10]…) et les outils ont fait un bon énorme pour manipuler de gros volumes de données et en suivre la qualité ou les variations (big data, data viz, data science…).

Nouveau besoin de gouvernance, existant difficile à maîtriser, multiplication des initiatives, réglementation sur les données… Les acteurs de la donnée – et plus particulièrement les DPO – se retrouvent à devoir harmoniser, faire converger les règles, les actions et l'organisation de toute l'entreprise. Sans un cadre, sans une partition pour la gestion des données de l'entreprise, aussi bon chef d'orchestre que soit le DPO, la mission sera impossible.

Une méthode et une partition pour orchestrer la gouvernance des données et interpréter le RGPD

Multiplicité des préoccupations : La protection des données s'impose aux entreprises, comme une préoccupation incontournable. Cependant, d'autres préoccupations ou exigences liées aux données pèsent sur la conception et le fonctionnement des entreprises. Certaines d'entre elles peuvent même se révéler contradictoires. C'est le cas de la valorisation des données et des opportunités liées à leur exploitation dans l'économie numérique (communication et personnalisation client, par exemple).

On ne peut donc pas élaborer une réponse isolée, focalisée sur la seule protection des données et sans confrontation aux autres déterminations qui s'exercent sur l'entreprise. Cette tendance est, hélas, très naturelle : à chaque préoccupation sa fonction, son responsable, son comité, son processus… Cette tendance organique alourdit l'organisation, et aboutit à empiler les dispositifs, sans résoudre de potentiels conflits. Elle met en difficulté ceux qui ont un rôle transverse, d'orchestration… comme le DPO.

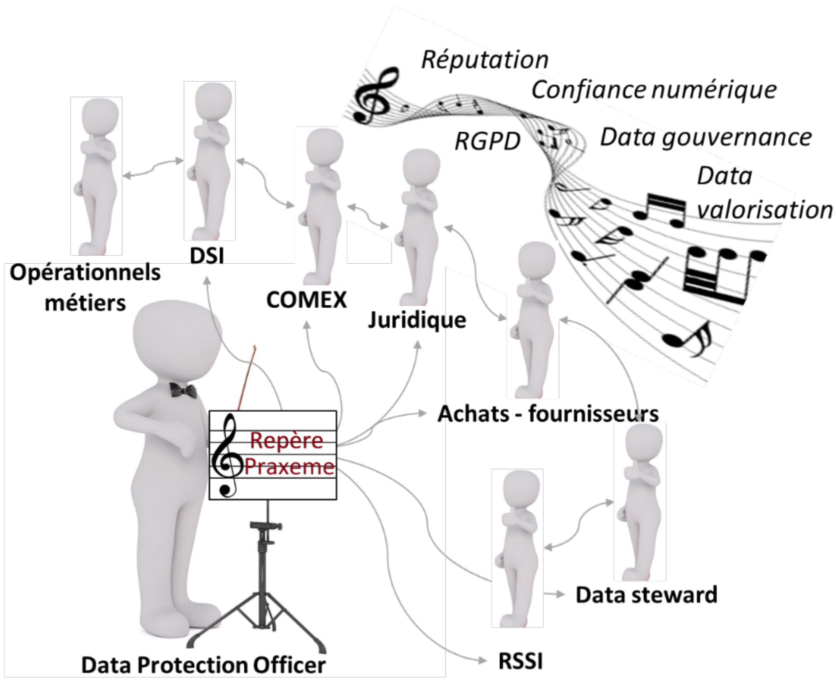
[6] *Proof Of Concept*.
[7] *Master Data Management*.
[8] *Data Quality Management*.
[9] *Chief Data Officer*.
[10] *Data Management Platform*.

Je suis DPO, autour de la table, je réunis :

- les juristes qui couvrent le volet juridique du RPGD,
- le RSSI[11] et son spécialiste de la cybersécurité,
- l'exploitation informatique en charge de superviser les flux de données et de gérer les archives et backup de données,
- le responsable métier de la relation client,
- le chargé des études et projets de la DSI[12],
- le service achat et de gestion des fournisseurs,
- le responsable de la cellule d'administration des données client…

Vais-je arriver à ce que tout le monde se comprenne et converge ?

Besoin d'une vision d'ensemble, d'une partition pour toute l'entreprise : À rebours de cette tendance, il convient d'intégrer la protection des données dans une réflexion plus large, plus ambitieuse, qui prend en charge toutes les dimensions de l'entreprise. Plutôt que de concevoir une réponse dédiée à la protection des données, il faut partir de la réalité de l'entreprise, analysée dans tous ses aspects, pour l'envisager dans toutes les perspectives pertinentes. La protection, mais aussi la valorisation des données, rejoignent ces perspectives, comme la qualité, l'agilité, la performance opérationnelle, l'éthique, etc.



Gouvernance des données : quelle partition pour les acteurs de l'entreprise ?

[11] Responsable de la Sécurité des Systèmes d'Information.
[12] Direction des Systèmes d'Information

Élaborer la partition via une méthodologie fédératrice : Afin de faciliter cette approche, nous nous appuyons sur la méthode publique Praxeme. L'intérêt est double :

- D'une part, en tant que publique, ouverte, donc largement partagée, elle apporte la caution d'une méthodologie qui s'adresse à tous les profils impliqués dans la transformation de l'entreprise.
- D'autre part, elle embrasse tous les aspects de l'entreprise – de ses valeurs à l'infrastructure –, et offre ainsi la partition attendue pour articuler les responsabilités et orchestrer les interventions.

Une des caractéristiques de Praxeme consiste à appréhender la *totalité de l'entreprise* et non seulement un de ses aspects (les processus, l'informatique, le juridique, etc.).

Exemple : Comment aligner les juristes en charge de l'application de la réglementation sur l'ensemble des données personnelles et l'exploitation informatique en charge de gérer les archives des données clients ?

En cela, Praxeme répond à la première demande des dirigeants d'entreprises : articuler les expertises, mettre en ordre de marche les différentes compétences nécessaires pour penser et améliorer l'entreprise et ses systèmes (organisation, processus, personnel, informatique, etc.).

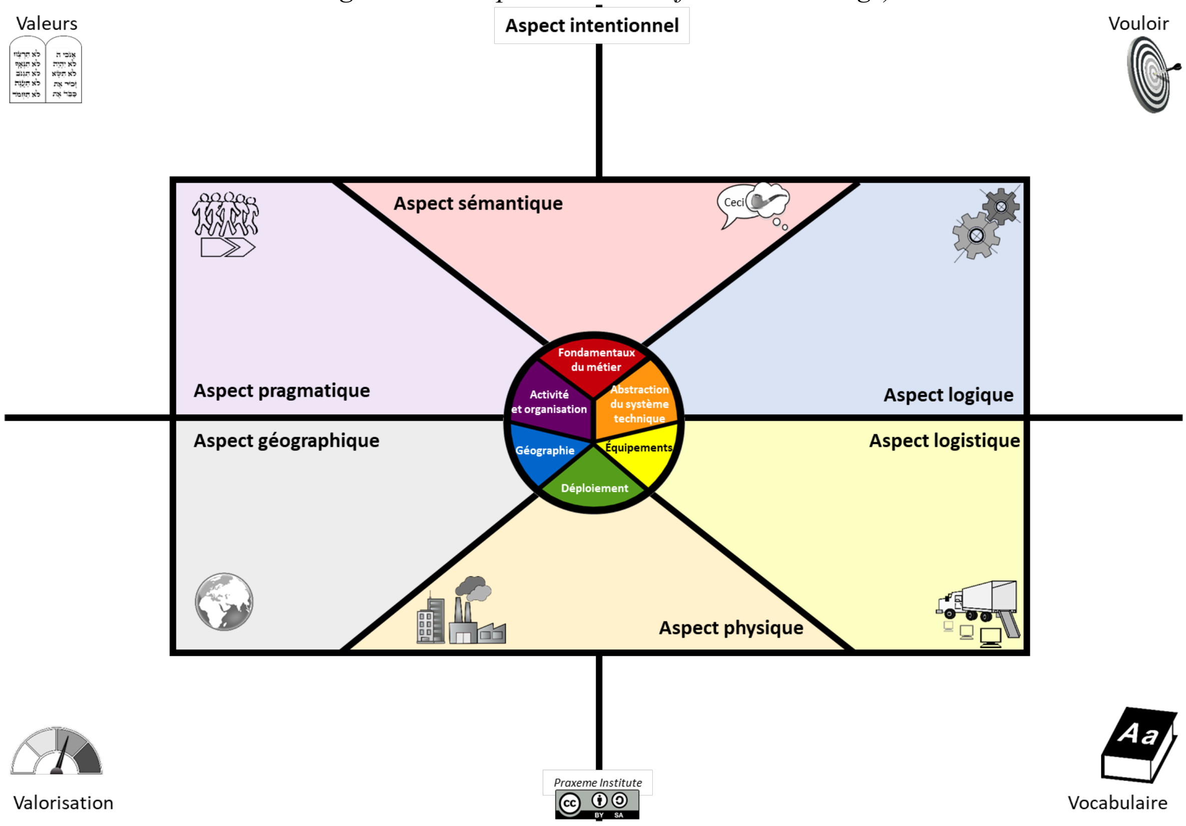
Cette méthode se différencie des référentiels de pratiques qui se spécialisent sur une discipline : l'élaboration de la stratégie, l'organisation, la conception des processus, l'expression des exigences, l'architecture informatique… Elle offre un cadre qui peut être partagé par tous les acteurs de l'entreprise. Cette approche holistique est exactement ce dont les entreprises ont besoin pour traiter le sujet de la gouvernance des données et, par là-même, le sujet de la protection des données et au-delà du RGPD.

La partition pour la gouvernance des données : le Repère Praxeme

Le Repère Praxeme est un outil d'analyse et de conception qui fournit un cadre de représentation de l'entreprise en tant que système. Il en ordonne la perception et facilite l'alignement des décisions entre acteurs. Grâce à cette mise en ordre et à la grille de lecture qui embrasse tous les aspects de l'entreprise, le recours à ce repère stimule la réflexion stratégique et la conception architecturale d'ensemble[13].
Il sert de guide de questionnement, pour établir un bilan, pour exprimer des exigences, pour étudier les implications de différents scénarios de conception et pour s'assurer de l'ajustement de chaque préoccupation (celle des juristes, celle de l'exploitation informatique, celle des responsables de processus, celle des projets « digitaux », celle du *datalab*…). Il permet de donner une vue synthétique et cohérente d'un objectif de transformation et de ses conséquences, tant sur le versant métier que sur le versant technique. Nous l'appliquons ici, avec un objectif de transformation particulier : conformer l'entreprise au RGPD.

[13] Cf. PxPRD-01f (formulaire) et PxPRD-01i (instructions), disponible sur la page des téléchargements : http://www.praxeme.org/telechargements/catalogue/.

Figure 1. Le Repère Praxeme (formulaire vierge)



Le Repère Praxeme fournit le papier à musique !
La portée se compose des sept aspects du Système Entreprise.

L'aspect d'un Système Entreprise est une portion de sa réalité, isolée pour en faciliter l'étude. L'aspect est délimité en tenant compte de sa logique interne, à l'exclusion de toute considération d'organisation. Un aspect rassemble des éléments de même nature, par exemple :

- des intentions (objectifs, exigences, valeurs…), pour l'aspect intentionnel,
- des connaissances portant sur les fondamentaux du métier, pour l'aspect sémantique,
- des processus, règles d'organisation, rôles… pour l'aspect pragmatique…

Les aspects sont des univers bien distincts, mais ils ne flottent pas dans le vide. Ils entretiennent des relations précises qui tissent la réalité du système. La Topologie du Système Entreprise fixe ces relations, dans un double souci de cohérence et d'efficacité :

- cohérence : le modélisateur ne peut relier des éléments que si leur nature le permet ;
- efficacité : les relations préparent la dynamique de la transformation, avec des règles de passage d'un aspect à l'autre.

Toute démarche interdisciplinaire s'attaquant à un objet aussi complexe que l'entreprise requiert un cadre de représentation.

Le cadre de représentation est une grille de lecture appliquée à l'entreprise pour en ordonner la perception. Il guide les actions de transformation.
Nous le recommandons pour la mise en application du RGPD.

Le cadre de représentation proposé par la méthode Praxeme se nomme la Topologie du Système Entreprise. Il identifie et articule sept aspects de l'entreprise. Tout ce qui se dit et se pense du RGPD s'ordonne à travers ces sept aspects. Ce cadre aide à administrer, à articuler la masse d'informations et de décisions qui concernent le déploiement du RGPD, de la stratégie à l'infrastructure. La rigueur structurelle et les capacités de description offertes par ce cadre constituent l'atout pour réussir son investissement et son projet de transformation RGPD.

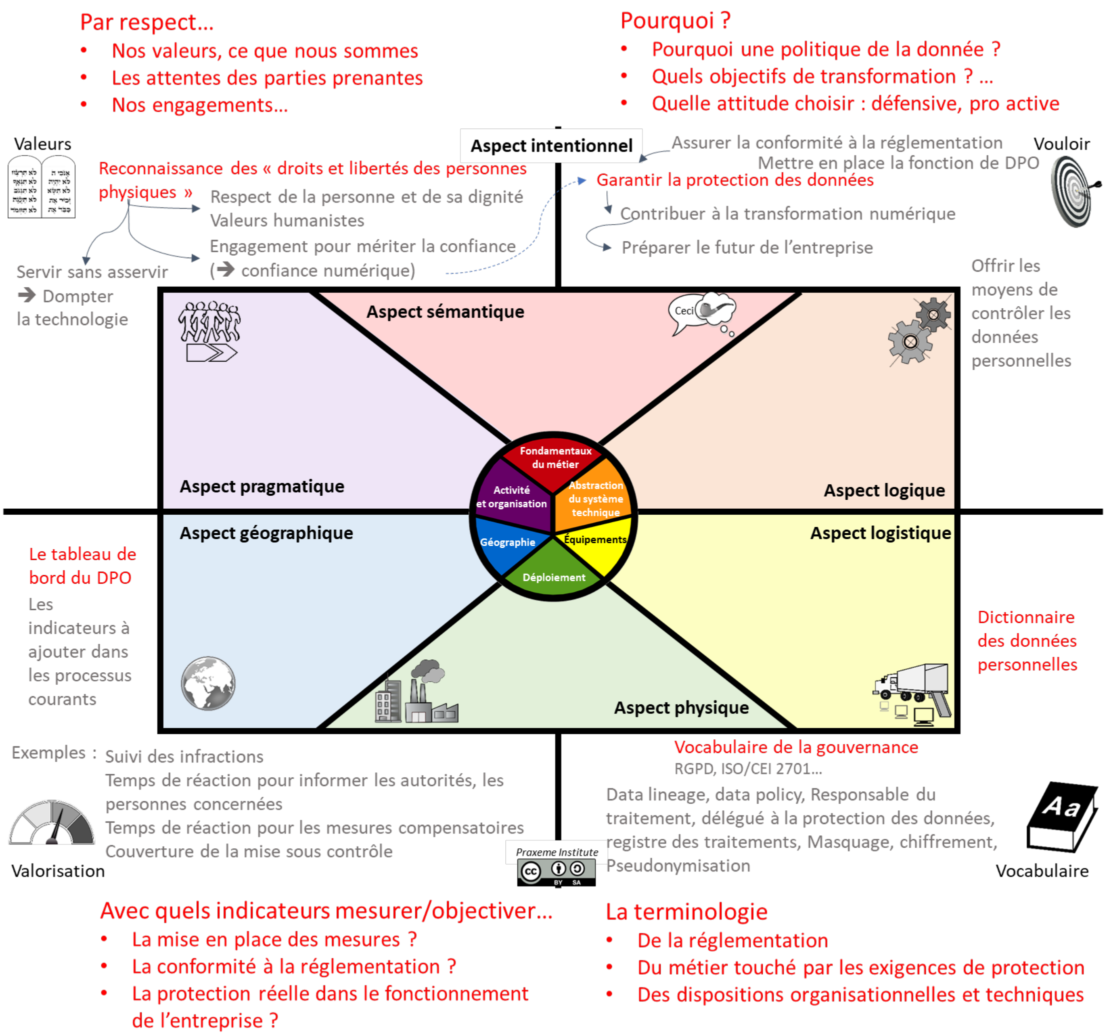
Figure 2. La définition des aspects

Aspect	Définition	Contenu (pour une application à l'entreprise)
Intentionnel	Aspect qui rassemble les éléments d'intention fixant les finalités et les contraintes d'un système	La morale de l'entreprise et ses finalités (valeurs, stratégie, culture…), les objectifs, exigences, indicateurs, la terminologie de l'entreprise
Sémantique	Aspect d'un système qui isole la connaissance des objets manipulés et des concepts nécessaires à son fonctionnement	La connaissance, les fondamentaux du métier (l'environnement, l'offre de l'entreprise, les objets métier, etc.)
Pragmatique	Aspect d'un système portant sur les activités et la façon de les mener	Les activités de l'entreprise et son organisation (rôles, processus, styles de management et de contrôle, gouvernance…)
Géographique	Aspect d'un système à travers lequel se précise sa distribution spatiale	La localisation des activités de l'entreprise (géographie de l'entreprise, virtualisation, télétravail, équipement nomade…)
Logique	Aspect d'un système qui fournit une abstraction de ses moyens logistiques et techniques	Un aspect intermédiaire entre métier et technologie, introduit dans la chaîne de transformation pour faciliter la conception des systèmes techniques (équipements)
Logistique	Aspect d'un système composé de ses moyens logistiques	L'ensemble des ressources techniques au service de l'activité, notamment l'informatique, les données, les équipements de transport et de production
Physique	Aspect sous lequel un système apparaît comme déployé, dans sa réalité physique	Le Système Entreprise complètement déployé (avec toutes ses ressources localisées)

Ce que pourrait être l'application du repère au déploiement du RGPD à l'échelle de l'entreprise et sa contribution à la gouvernance des données

Analyse intentionnelle : Dans un premier temps, le thème de la protection des données est intégré à l'analyse intentionnelle de l'entreprise : il s'agit d'élaborer un modèle cohérent des « intentions », prenant en compte les préoccupations, la réglementation, les valeurs et les objectifs stratégiques. Entre ces éléments d'intention, il peut exister des relations de contribution ou de contradiction. Il importe de les dégager. Au lieu de traiter chaque préoccupation séparément, l'analyse intentionnelle prend en charge l'ensemble des déterminations internes et externes, de façon à résoudre les éventuels conflits d'intention. Ainsi, nous sommes en situation de découvrir que la protection des données peut entrer en résonnance avec certaines valeurs de l'entreprise, ce qui pourrait insuffler un nouvel esprit à la réponse apportée.

Figure 3. Illustration de l'analyse dans la perspective de protection des données



Analyse des différents aspects du système entreprise : À partir de ce modèle unifié des intentions, nous pourrons ensuite examiner chaque aspect de l'entreprise. Par exemple, à travers l'aspect pragmatique, nous évaluerons les processus de l'entreprise, non pas dans l'optique exclusive du RGPD, mais en vérifiant qu'ils répondent bien à l'ensemble des enjeux.
Deux natures de mesures peuvent être envisagées :

1. mise en place de processus ou procédures dédiées au RGPD (notifier les autorités en cas de perte de données, tenir le registre des traitements…) ;
2. renforcement des processus « métier » courants, dans la perspective de la protection (geler les opérations en cas d'attaque…).

Cette dernière nature prépare, par exemple, le récapitulatif des usages des données, des finalités et donc le futur registre des traitements.

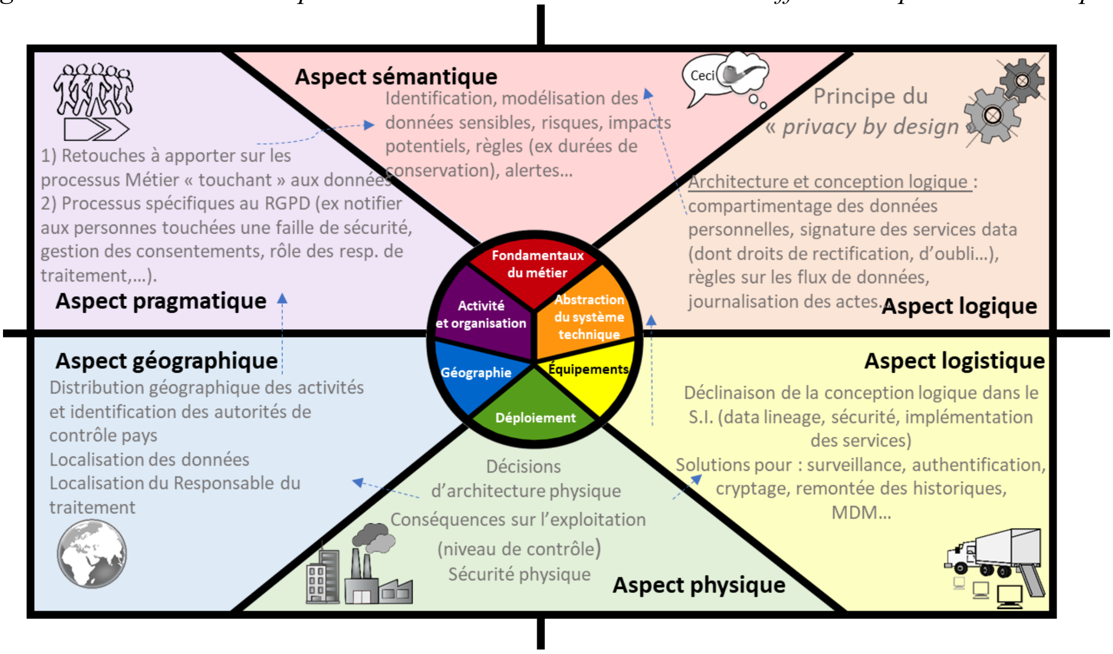
De la même façon l'application du RGPD amène à repérer les données personnelles et les informations qui leur sont rattachées. Ce travail se réalise à un niveau que la méthode identifie comme l'aspect sémantique de l'entreprise. Il s'agit du capital intellectuel de l'entreprise, la connaissance fondamentale du métier. Ajuster l'entreprise au RGPD fournit l'opportunité de poser les premières briques de l'aspect sémantique.

Ensuite, à partir des choix sémantique et pragmatique, un travail de conception logique est à mener. Ici s'impose le principe du « *privacy by design* ». Ce travail se mène à deux niveaux :
1. choix d'architecture (décisions structurelles) et dispositifs généraux (journalisation des actes, historisation des états) ;
2. choix de conception logique (détails sur la signature des services, sur les structures d'échange, sur le modèle des données)[14].

Une fois les décisions de conception prises, il s'agit de s'assurer de leur transposition dans l'aspect logistique, puis dans l'aspect physique (choix d'hébergement). Cette projection dans le monde technique tient compte des besoins d'évolution du système et des contraintes de distribution géographique. Par exemple, la réglementation peut limiter les transferts de données entre les pays (exemple du transfert de données hors UE), ou imposer l'hébergement des données sur le territoire national.

[14] Les procédés relatifs à l'architecture et à la conception logiques, particulièrement dans une approche orientée services, font l'objet de la version 2 de Praxeme pour l'aspect logique. Pour en savoir plus : info@praxeme.org.

Figure 4. Illustration de dispositions RGPD à considérer dans les différents aspects de l'entreprise

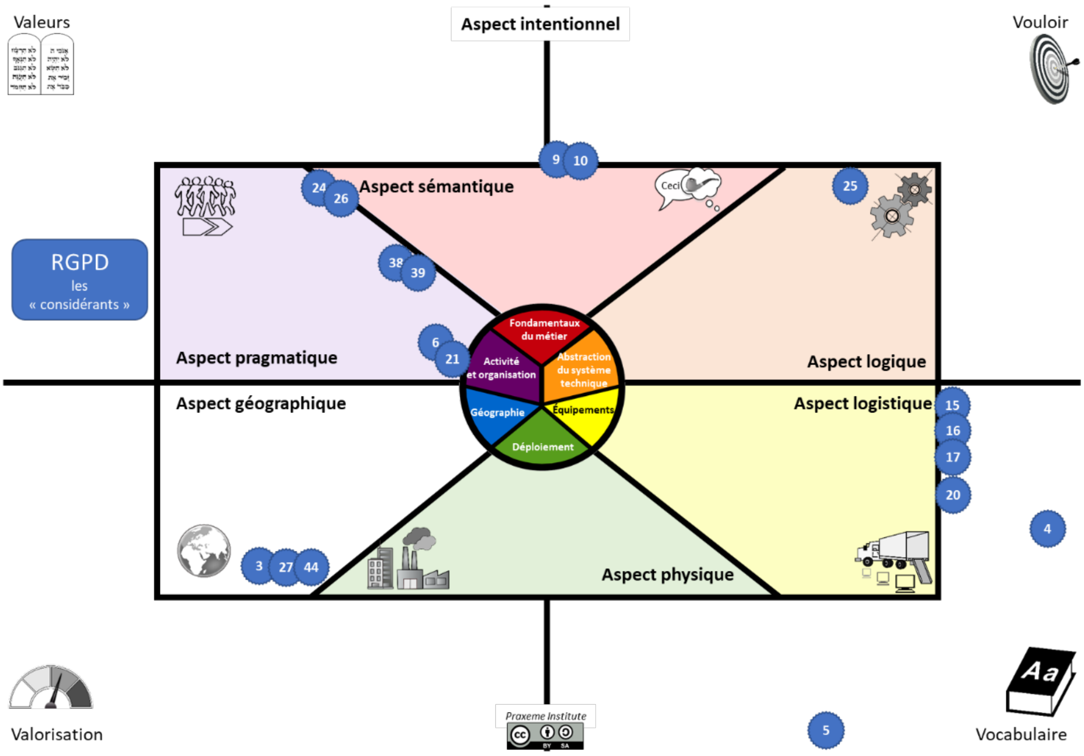


Avec ce repère, une contrainte réglementaire (i.e. un article du règlement, par exemple) peut être positionnée au sein du Système Entreprise. Systématiquement, nous nous demandons : à quel aspect la contrainte se réfère-t-elle ? Ou encore : quel impact peut-elle avoir sur les différents aspects ? Nous conservons ensuite le lien entre la contrainte réglementaire, d'un côté, et les dispositions prises pour la satisfaire.

Nous mettons ainsi en place des chaînes de traçabilité qui démontrent la conformité et assurent la cohérence de la construction, des aspects les plus abstraits aux plus concrets et ainsi s'assurer de l'alignement de l'ensemble des décisions. Par exemple, à la question « la pseudonymisation est-elle correctement respectée ? », nous pourrons répondre en parcourant la chaîne de traçabilité qui s'ancre sur cet élément d'intention (la règle), et court jusqu'à la solution physique d'hébergement. Cette chaîne peut passer par l'aspect sémantique – où sont repérées les informations concernées – et l'aspect pragmatique – où s'inscrivent les activités (production, administration, archivage…).

Cette vision d'ensemble ou d'architecture d'entreprise – c'est-à-dire le souci du tout – doit canaliser l'énergie mise dans les projets et la diriger vers le bien commun. Une dynamique de ce type, équilibrant le mode projet et la vision architecturale, permet de réaliser des économies considérables et une optimisation de l'investissement d'évolution des processus et de l'organisation. Elle s'appuie sur un nouveau jeu de rôles, au sein duquel le DPO doit trouver sa place de chef d'orchestre.

Figure 5. Les articles N du RGPD positionnés sur le Repère Praxeme (sélection)



Le tableau suivant indique les articles référencés dans cette figure.

Figure 6. Les articles du RGPD et leur nature en termes d'aspects (sélection)

N° article	Titre	Commentaire
Esprit du réglement	Les considérants	Ces considérations liminaires rappellent les motivations de la réglementation. Elles ressortent de l'aspect intentionnel, et se réclament de valeurs fondamentales, inscrites dans la Charte des Nations-Unies. « La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. » « Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. » Ces motivations prennent place dans le modèle axiologique de l'entreprise, son « système de valeurs ». Les garder à l'esprit aide à donner un sens fort et positif à l'effort nécessaire pour mettre l'entreprise en conformité au règlement. La confiance est le maître mot qui, à la fois, inspire le RGPD, et doit mobiliser l'entreprise.
3	Champ d'application territorial	Cet article concerne l'aspect géographique de l'entreprise. Peu importent la géographie de l'entreprise et le lieu du traitement, le RGPD s'applique dès lors que le traitement concerne des ressortissants de l'Union européenne. Cette caractéristique est d'ordre sémantique.
4	Définitions	Toutes ces définitions de termes utilisés dans le RGPD pourraient enrichir utilement la terminologie de l'entreprise. Pour la méthode, le vocabulaire est une des facettes de l'aspect intentionnel.

N° article	Titre	Commentaire
5	Principes relatifs au traitement des données à caractère personnel	Cet article comporte deux versants : ▪ Il énonce l'exigence générale applicable aux données (« Les données à caractère personnel doivent être… ». ▪ Il introduit un vocabulaire technique qui sera utilisé dans la suite du texte. Les exigences sont à loger dans la facette « Vouloir » de l'aspect intentionnel ; les termes deviennent des entrées du thesaurus.
6	Licéité du traitement	Consentement et finalité du traitement, à prendre en compte dans l'aspect pragmatique (associés à des activités identifiées).
9, 10	Traitement portant sur des catégories particulières de données à caractère personnel Traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions	Ces deux paragraphes définissent les données sensibles, et établissent les exceptions. Ceci entre dans l'aspect sémantique. Il n'y a pas de raison pour que l'entreprise s'inhibe dans la modélisation sémantique, c'est-à-dire dans la description précise des objets de la réalité. Cependant, le RGPD conduit à : ▪ évaluer la sensibilité des informations (sous la forme d'annotations inscrites dans le modèle) ; ▪ réserver l'exploitation de ces données aux usages prévus par la réglementation. Ce deuxième point appelle une vérification des activités manipulant ces données et, éventuellement, des droits accordés aux acteurs. Il y a donc un point de contact avec l'aspect pragmatique. Les droits et le contenu des activités devraient être exprimés dans les mêmes termes que les annotations mentionnées précédemment.
15, 16, 17, 20	Droit d'accès de la personne concernée Droit de rectification Droit à l'effacement (« droit à l'oubli ») Droit à la portabilité des données	Ces paragraphes impliquent des dispositions d'ordre organisationnel (identification d'un point de contact, prise en compte des demandes, relais à travers l'organisation, suivi des événements, etc.), à mettre en place dans l'aspect pragmatique de l'entreprise. Une modélisation rigoureuse en termes de processus et d'événements s'impose ici, pour ne rien laisser au hasard[15]. Ces paragraphes débouchent également sur des solutions informatiques, particulièrement : les services à proposer aux clients et usagers, via les sites Internet ; les outils d'extraction et de formatage des données. On touche alors à l'aspect logistique.
21, 24, 26	Droit d'opposition Responsabilité du responsable du traitement Responsables conjoints du traitement	En application au RGPD, l'entreprise ne peut faire autrement que de mettre en place l'organisation idoine : rôles, processus, prise en compte des demandes et des alertes… Dans l'aspect pragmatique, deux types de conséquences se lisent : ▪ d'une part, la création de nouveaux dispositifs (typiquement : le délégué à la protection des données, les nouveaux processus) ; ▪ d'autre part, l'adaptation des dispositifs existants pour qu'ils prennent en compte la perspective de la protection de données.

[15] À ce niveau de criticité, la notation d'un standard comme BPMN (*Business Process Model & Notation*) apporte toute sa puissance d'expression..

N° article	Titre	Commentaire
25	Protection des données dès la conception et protection des données par défaut	Cet article encourage une conception qui tienne compte, dès l'abord, des exigences propres à la protection des données. Une telle approche suppose une architecture logique parfaitement documentée et qui assure la lisibilité des traitements. Des décisions d'architecture logique peuvent, d'ailleurs, contribuer à protéger les données et sécuriser le système (compartimentage, maîtrise des interfaces, généralisation de règles sécuritaires sur la signature des services, refonte de l'architecture des données, etc.). Ce travail de conception porte sur l'aspect logique, alimenté pour l'essentiel à partir des modèles « métier » (sémantique et pragmatique).
27	Représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union	Aspect géographique de l'entreprise, au sens large, y compris ses partenaires et sous-traitants.
30	Registre des traitements	Le registre reste sur le plan de la description, par opposition à celui de l'exécution : il convient donc de documenter parfaitement le système informatique et le lien entre les traitements et les données. Ceci se réalise à travers des modèles, dont on pourra vérifier la fidélité par rapport à l'état du système. Le mieux, semble-t-il, est de répondre à cette exigence dans l'aspect logique… et d'en profiter pour concevoir une cible améliorée. À noter : le règlement ne réclame pas de journaliser les traitements exécutés. Ce point demanderait des décisions techniques (aspect logistique) et un suivi dans l'aspect physique.
38, 39	Fonction du délégué à la protection des données Missions du délégué à la protection des données	Précisions sur les rôles dédiés (aspect pragmatique ou organisationnel).
44	Principe général applicable aux transferts	Application aux échanges internationaux.

En conclusion, les travaux de mise en conformité par rapport au RGPD vont pouvoir bénéficier du Repère Praxeme. Il leur offre un schéma d'analyse, incitant à examiner toutes les facettes de cette problématique de la protection des données, en l'insérant dans l'approche holistique de l'entreprise. Comme outil de communication, il permet de restituer la cohérence des dispositions à prendre en réponse aux exigences réglementaires, telles que :

- les éléments de la politique des données (initiée dans l'aspect intentionnel),
- l'organisation et les différentes responsabilités (aspect pragmatique),
- le support des différents processus de management de la donnée (processus qualité, de protection des données, de collecte, de communication, de circulation des données),
- la connaissance des données (vocabulaire, dictionnaire, modèles – surtout dans l'aspect sémantique),
- les moyens techniques (aspect logistique).

Bref, la démarche d'analyse et de conception couvre toutes les dimensions dans lesquelles se déploie la gouvernance des données.

Les solutions et guides méthodologiques pour le DPO : les contributions de la méthode à l'écriture de la partition RGPD

Ce *Position Paper* a vocation à donner une vision d'ensemble de ce que vise la déclinaison du repère Praxeme pour devenir la partition du RGPD à l'échelle de l'entreprise.
Même s'il donne déjà une première vue d'application, il n'est pas directement un support à l'action.

Pour cela, il est nécessaire de s'appuyer sur des procédés et guides d'action (le COMMENT). Outre ceux qui existent déjà au sein de la méthode (voir en introduction), nous visons à les enrichir et en créer de nouveaux dans l'esprit de notre position.

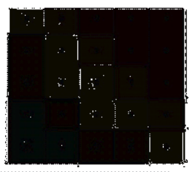
L'objectif est très pragmatique, et la mise en œuvre progressive. Le Repère Praxeme offre le support de base. Puis, suivant les besoins à couvrir, il est possible progressivement d'approfondir l'application de la méthode au travers des procédés et guides. Par exemple l'élaboration du vocabulaire pourra s'appuyer sur le guide de terminologie.

Pour atteindre cet objectif, différents travaux sont en cours, et ont vocation de compléter les procédés existants :

- Rédaction d'un procédé d'utilisation du Repère Praxeme décliné pour le déploiement du RGPD (déploiement, exécution et gouvernance). Et développement d'un outil de diagnostic/analyse (questionnaire) de situation vis-à-vis du RGPD projeté sur les aspects de la méthode[16].
- Rédaction d'un procédé de formalisation d'une démarche de *data lineage*.
- Enrichissement du procédé de définition d'une politique de la donnée – 2ème version (renforcement de l'articulation avec la gouvernance des données)

[16] Illustration : extrait de l'outil de diagnostic RGPD

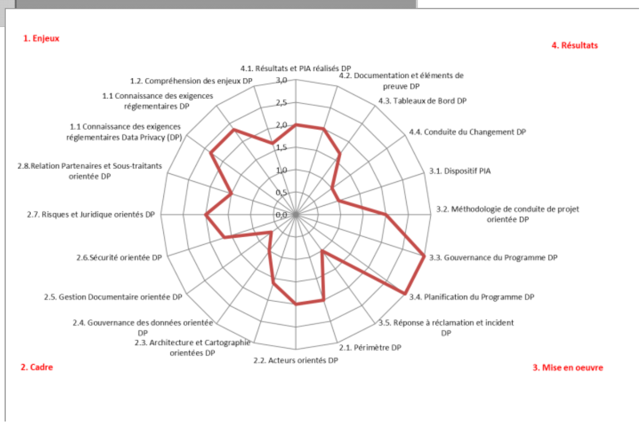
Questions ouvertes pour précisions, approfondissement	Article maître (Principal) RGPD/GDRP	Autres Articles RGPD/GDRP	Références / textes juridiques
Avez-vous mis en place des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement?	32 ; 35		Article 32 Sécurité du traitement, RGPD *1. c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;* Article 35 Analyse d'impact relative à la protection des données
Y'a-t-il une procédure de gestion des incidents sur DCP?	32 ; 35		Article 32 Sécurité du traitement, RGPD *1. c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;* Article 35 Analyse d'impact relative à la protection des données
Cette procédure prévoie-t-elle des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique?	32 ; 35		Article 32 Sécurité du traitement, RGPD *1. c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;* Article 35 Analyse d'impact relative à la protection des données
L'efficacité de cette procédure est-elle vérifiée au moyen de tests et des évaluations régulières?	32 ; 35		Article 32 Sécurité du traitement, RGPD



Matrice des Risques

Exemple de questions

- *Avez-vous formalisé une procédure de gestion des incidents sur les DCP?*
- *Cette procédure prévoie-t-elle des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés, en cas d'incident physique ou technique?*
- *L'efficacité de cette procédure est-elle vérifiée au moyen de tests et des évaluations régulières?*
- *Avez-vous des mécanismes permettant de garantir la sécurisation de l'exportation et la portabilité des DCP ?*

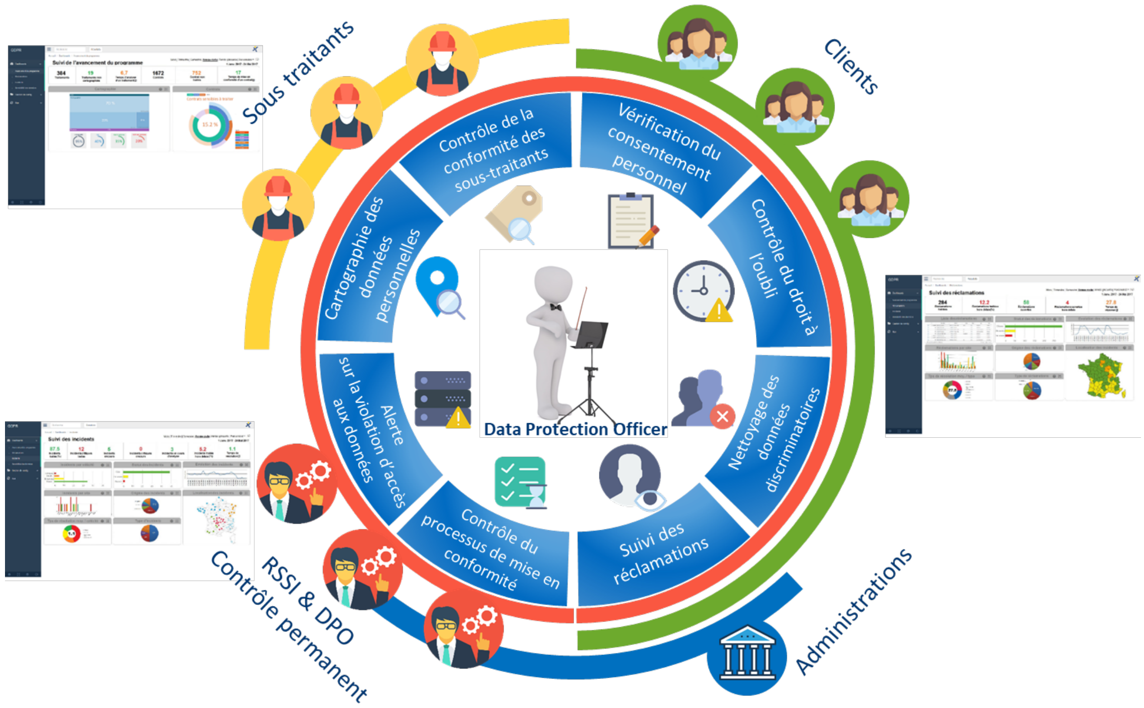


La méthode doit répondre aux préoccupations du DPO et des parties prenantes du RGPD :

- Comment aborder le RGPD ?
- Comment diagnostiquer la situation dont on part ?
- Quelle stratégie mettre en place ?
- Comment déterminer les priorités propres à chaque acteur tout en assurant la cohérence d'ensemble ?
- Comment capitaliser sur les initiatives et *best practices* existantes ?
- Comment, le 25 mai 2018, apporter la preuve des travaux engagés et de leur pertinence ?
- Comment définir le référentiel d'activités et l'organisation *Data Privacy* ?
- Comment mettre en conformité le S.I. ?
- Comment piloter la prise en compte du RGPD – quelle métrologie, quel cockpit ?
- …

Au final, le DPO devrait être en mesure, via son cockpit, de vérifier que la partition RGPD est correctement jouée au sein de l'entreprise.

Figure 7. Le tableau de bord – cockpit du DPO pour orchestrer le RPGD



Sur la base d'interviews réalisées auprès de DPO, nous avons dessiné le paysage des certitudes ou craintes ressenties sur tout ou partie des étapes du RGPD. La lecture de ces verbatims trouve écho dans les solutions que forment les guides méthodologiques et outils présentés dans ce Position Paper.

Annexe

Figure 8. Sélection de documents relatifs à l'approche par les données (fonds public Praxeme)

	Titre	Indice	Objectif
Documents de portée générale	**Synoptique de la méthode**	PxMDS-00	Cartographier le corpus méthodologique et expliquer sa structuration (présenter les principes du catalogue)
	Guide général	PxMDS-01	Introduire la méthode et en donner un panorama complet
	La Topologie du Système Entreprise	PxPRD-01	Elaborer la grille de lecture à appliquer aux systèmes étudiés [framework, cadre, aspect, point de vue, structure]
	Le Repère Praxeme	PxPRD-01f	Formulaire pour : Guider les réflexions stratégiques et architecturales [framework, cadre, TSE, analyse architecturale, stratégie]
		PxPRD-01i	Mode d'emploi du "Repère Praxeme"
Documents liés à l'approche par les données	**Approche de l'aspect sémantique**	PxPRD-10	Définir l'aspect sémantique du Système Entreprise et décrire son contenu (fondamentaux du métier)
	Introduction aux procédés de l'approche sémantique	PxPCD-20	Présenter l'ensemble des procédés de modélisation sémantique et faire le lien avec les guides
	Passer du langage au modèle	PxPCD-21	Exploiter un texte pour alimenter le modèle
	Structurer l'aspect sémantique	PxPCD-25	Décomposer l'aspect sémantique d'un système en utilisant un critère approprié
	Les procédés terminologiques	PxPCD-14	Présenter les procédés terminologiques [vocabulaire]
	Définir un terme ou une expression	PxPCD-14a	Produire une définition d'un terme donné, la plus concise, claire et efficace possible pour faciliter la communication et l'apprentissage [terminologie, vocabulaire, dictionnaire]
	Élaborer un thesaurus	PxPCD-14f	Conserver la terminologie sous la forme d'une structure navigable [terminologie, vocabulaire, dictionnaire, usage]
	Politique de la donnée	PxPRD-04f	Établir une politique de la donnée (data policy) Sommaire type
	Mode d'emploi du formulaire PxPRD-04f	PxPRD-04m	Présenter en détail le formulaire et expliquer comment élaborer une « politique de la donnée »

CONIX Consulting est une entité du Groupe CONIX : Groupe indépendant de 20 ans d'existence, fort de 210 collaborateurs, et d'un CA de 22.6 M€ en 2016.

Le groupe CONIX a choisi, depuis sa création en 1997, de s'appuyer sur l'expertise pour accompagner ses clients dans leur transformation imposée par l'ère numérique. Ses activités sont focalisées sur les stratégies d'évolution des entreprises et de leurs systèmes d'information, que ce soit en termes d'agilité et d'innovation, d'intégration des enjeux liés au réglementaire et aux risques, d'orientation data ou de maîtrise de la sécurité (le Groupe CONIX dispose d'une entité dédiée à la cybersécurité - CONIX est l'une des rares sociétés en France engagées dans les labels PASSI - Audits Sécurité et test d'intrusion, PDIS - cybersurveillance et PRIS - réponse à incident - http://www.conix.fr/nos-expertises/cybersecurite/)

CONIX Consulting est le cabinet de conseil du Groupe CONIX.
CONIX Consulting vise à la double expertise : Métiers risques et réglementaire ET Data.

Cette double expertise se décline au travers de deux offres :

Conseil Risques et Réglementaire Banque Assurance. Des profils métiers & risques provenant des éditeurs de GRC, du conseil ou ayant occupé des fonctions opérationnelles ou managériales sur du réglementaire bancaire. Gouvernance, conformité et contrôle. Risques de marché, de crédit, opérationnel.

Conseil en transformation et innovation des Systèmes d'Information. Deux piliers d'expertises : l'architecture d'entreprise (architectures métier-fonctionnelle-S.I., urbanisme, schéma directeur, process - case management, architecture de données – data lake - data centric) et les expertises "data" (référentiels et MDM, DQM, gouvernance des données, data science).

CONIX Consulting membre fondateur du Praxeme Institute, accompagne la méthode publique Praxeme (www.praxeme.org) depuis son origine, et a pris en charge des contributions à la méthode sur le volet Data (http://www.praxeme.org/telechargements/catalogue/).

CONIX Consulting de par son positionnement et expertise Réglementaire et Data participe à la construction de l'offre d'accompagnement du Groupe CONIX dans le déploiement du RGPD au sein des entreprises.
Fort de ses expertises Réglementaire, Data et Cybersécurité, le Groupe CONIX dispose d'une offre complète pour transposer le RGPD dans le cœur d'activité des entreprises.