GDPR

Protection des données personnelles
Se mettre en conformité : Pourquoi ? Comment ?
Avec quelle organisation ? Quels moyens ?

Une nouvelle réglementation européenne sur la protection des données personnelles (General Data Protection Regulation, GDPR) entrera en vigueur en mai 2018. Les sanctions peuvent aller jusqu'à 4% du chiffre d'affaires annuel mondial ou 20 M€ (le plus important des deux sera retenu).

Pour vous accompagner dans votre projet de mise en conformité avec ce nouveau règlement, IBM propose une démarche opérationnelle outillée, développée dans ce livre blanc.

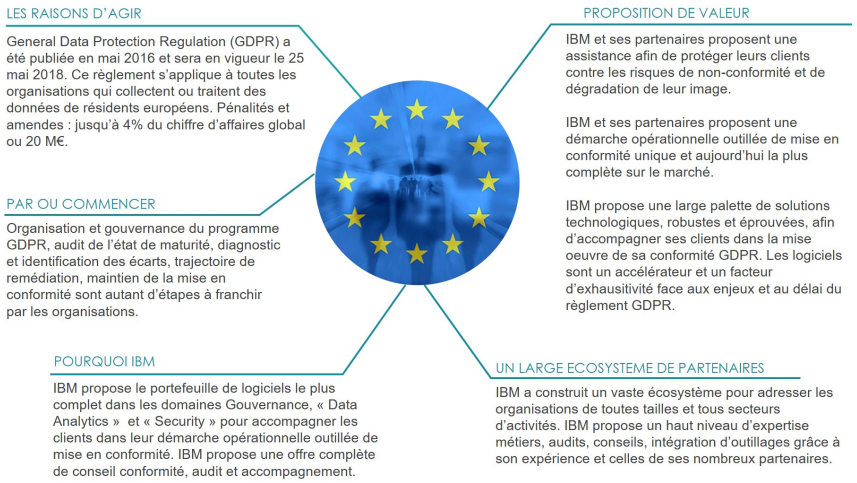
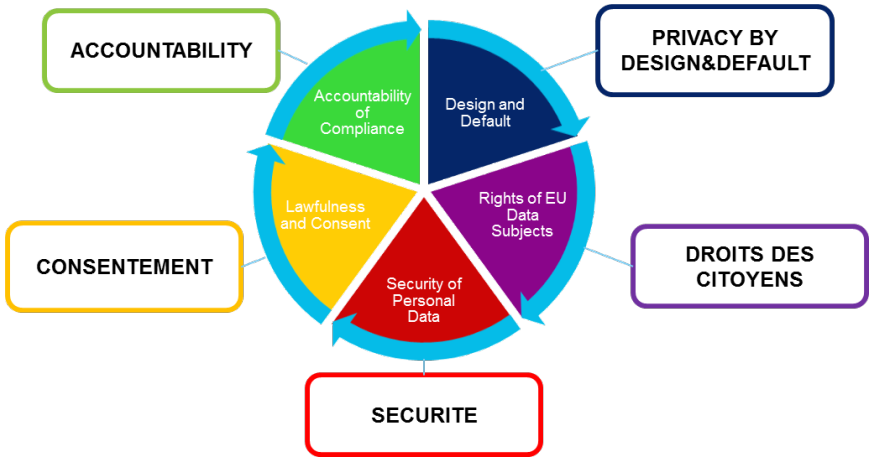


Figure 1 : GDPR & IBM en bref

1. Le point de vue IBM sur le règlement

L'analyse du règlement européen révèle les 5 catégories d'exigences suivantes *(Figure 2)*.

Figure 2 : GDPR, 5 niveaux d'exigences



1. **Accountability -** Le GDPR ne constitue pas une modification « à la marge » de la Loi Informatique et Libertés. Elle représente un véritable changement de paradigme en renversant la charge de la preuve de conformité qui devra être démontrée.

2. **Privacy by Design -** Ces exigences imposent aux entreprises d'intégrer la protection de la donnée personnelle dans la conception même des applications et des processus métiers. A titre d'exemple, la prise en compte au sein d'une future application des impacts du droit à l'oubli illustre un aspect sensible de cette exigence.

3. **Droit des citoyens -** L'analyse juridique est un préalable structurant à toute démarche de conformité. Elle permet, sur la base d'une connaissance approfondie de la réglementation, d'identifier la collecte et le traitement des données personnelles ainsi que les zones sensibles tant dans les applications back office que dans les opérations cœur de métier de l'entreprise, d'évaluer le risque (PIA : Privacy Impact Assessment) afférent, et de prioriser leur encadrement. Chaque personne doit être informée de ses droits (droit d'accès, droit de rectification, droit à l'oubli, droit à la limitation du traitement, droit à la portabilité, droit d'opposition) par l'entreprise qui les traite, que les données aient été collectées directement par l'entreprise ou indirectement.

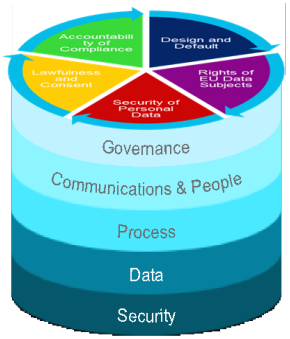
   L'analyse permet également d'évaluer le positionnement de l'entreprise dans la chaîne de traitement des données. Selon que l'entreprise est responsable de traitement, sous-traitant, ou co-responsable avec un ou plusieurs tiers, il faudra mettre en place des organisations et des structures contractuelles différentes.

4. **Sécurité des données -** La maîtrise des données personnelles et de leur confidentialité est un enjeu majeur. L'actualité est riche en nouvelles de fuites massives de données personnelles confidentielles, parfois suivies de leur publication sur des sites publics, voire de leur revente. La prévention de ces risques figure déjà dans le champ d'application des politiques de sécurité, mais, devant le fait établi, il faut être en capacité d'alerter les autorités de contrôle voire les personnes. Cette dernière exigence entre dans le champ d'application du GDPR.

5. **Gestion du consentement -** Le consentement d'un citoyen pour la collecte et l'utilisation - dans un but qui doit être clairement énoncé - de ses données personnelles doit être explicite et démontrable. Des processus de recueil et de contrôle de ce consentement doivent être mis en place.

La vision IBM est que le programme GDPR doit comprendre cinq niveaux complémentaires et indispensables pour adresser toutes les dimensions d'une transformation couvrant tant les métiers que l'IT *(Figure 3)*.

Figure 3 : Les cinq niveaux d'un programme GDPR



1. **La gouvernance GDPR**, couvre notamment le "Maturity Assessment", le "GDPR assessment", la démarche opérationnelle de mise en conformité et le suivi des activités.

2. **Communication & Personnes**, couvre la sensibilisation et la formation des employés ainsi que la communication interne et externe.

3. **Processus**, couvre la préparation et la construction de la feuille de route GDPR au regard des processus métiers.

4. **Données**, couvre l'exploration, le traitement (anonymisation, effacement, etc.) et la gestion du cycle de vie des données.

5. **Sécurité**, couvre la prévention et la gestion des failles et autres mesures de sécurité.

2. La démarche opérationnelle de mise en conformité

De nombreuses formalités auprès de la CNIL vont disparaître. En contrepartie, la responsabilité des organisations sera renforcée. Pour s'y préparer et les aider, la CNIL a proposé un guide en 6 étapes *(Figure 4)*.

Figure 4 : Démarche de la CNIL

Le GDPR est aussi un « voyage » vers la conformité qui nécessite une démarche opérationnelle outillée fondée sur un **état des lieux** relevant les écarts afin de les réduire dans une **trajectoire** *(Figure 5)*.

Figure 5 : Etablir un état de maturité, un diagnostic GDPR et définir une trajectoire

L'étendue des nouvelles actions à entreprendre et, en conséquence, des moyens à engager, peut être très importante. Ces actions nécessitent des compétences multiples, du pilotage à l'accompagnement au changement, en passant par l'expertise SI et sécurité numérique. Il est donc indispensable :

- D'évaluer initialement la complexité du projet au regard de l'organisation (notamment le nombre d'entités et de lignes métiers) et du système d'information puis d'analyser les conséquences de la réglementation afin d'évaluer la **maturité GDPR** de l'entreprise.

- De mesurer les écarts de conformité GDPR **au travers d'un état des lieux** sur différents axes tels que : le réglementaire, la maîtrise du cycle de vie des données personnelles et de leurs traitements, le devoir d'information auprès des personnes, l'accompagnement au changement, l'appropriation de la politique et le contrôle de son application. Cet état des lieux doit identifier les risques et les priorités.

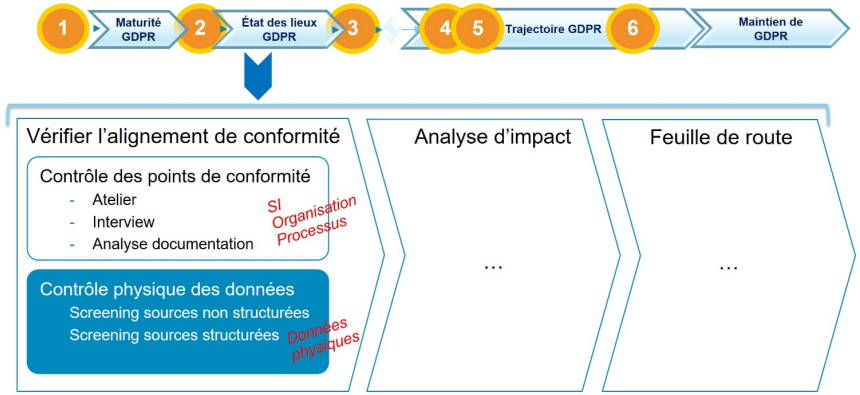
- De constituer une **trajectoire** viable basée notamment sur l'estimation des risques au regard de la criticité des données personnelles, leurs volumes, et leurs localisations sur des sources numériques « à risques ».

- Par la suite, d'instaurer les processus permettant la supervision et le **maintien** de la compliance GDPR.

L'état des lieux relève d'une démarche traditionnelle basée sur des entretiens et l'analyse de diverses documentations. Elle gagne dans de nombreux cas à être complétée par une approche outillée permettant notamment d'évaluer le degré réel de présence de données personnelles et de préciser ainsi les risques encourus *(Figure 6)*.

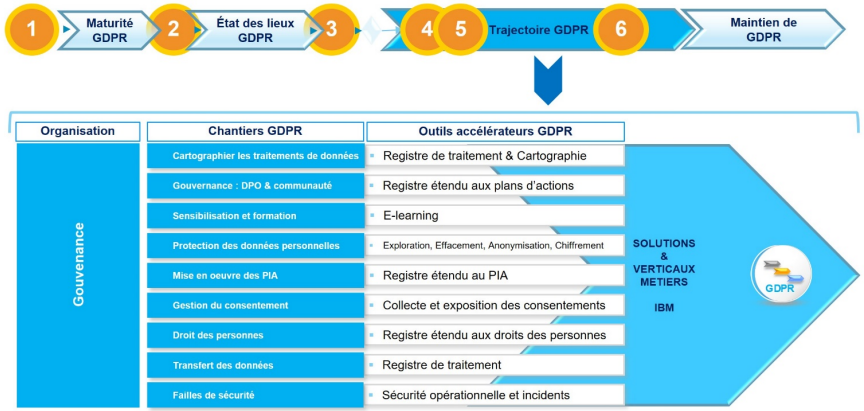
Cette recherche peut s'effectuer tant dans des bases structurées que sur des contenus non structurés (serveurs de messagerie, bases documentaires partagées par exemple).

Figure 6 : Le contrôle physique des données dans une démarche d'état des lieux



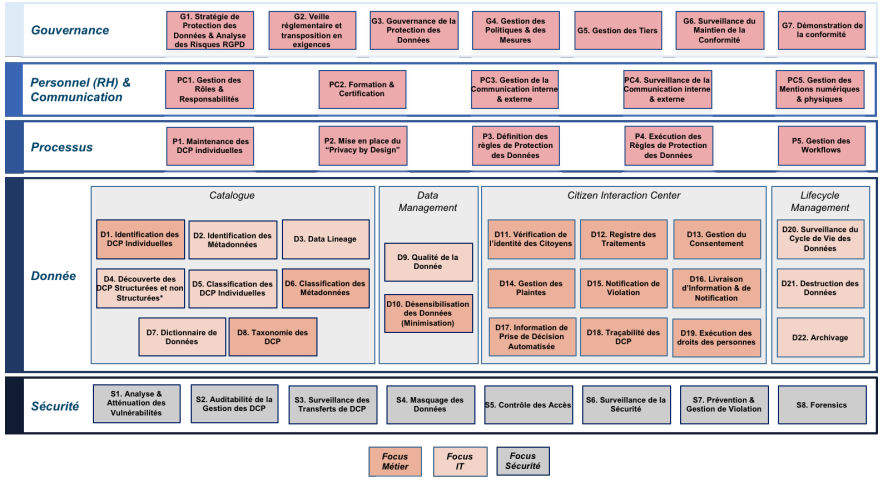
La trajectoire GDPR se décline en un certain nombre de chantiers d'importances relatives variables comme illustré sur la *Figure 7*. Cette trajectoire requiert la mise en œuvre d'outils soit dans une logique d'accélération, soit dans une logique d'industrialisation.

Figure 7 : Les outils au service des différents chantiers GDPR



Un référentiel GDPR est indispensable tant pour mener à bien un état des lieux que pour déterminer une trajectoire. Il permet de visualiser les éventuelles lacunes, de situer les zones de risques, de déterminer le degré de couverture par le système d'information par exemple. La « capability map » d'IBM (*Figure 8)* est un exemple de référentiel GDPR utilisable dans de multiples circonstances : évaluation des situations critiques, alignement des besoins métiers avec le système d'information… Le référentiel concourt à la complétude du projet GDPR et a également une valeur de visualisation.

Figure 8 : GDPR Capability MAP d'IBM

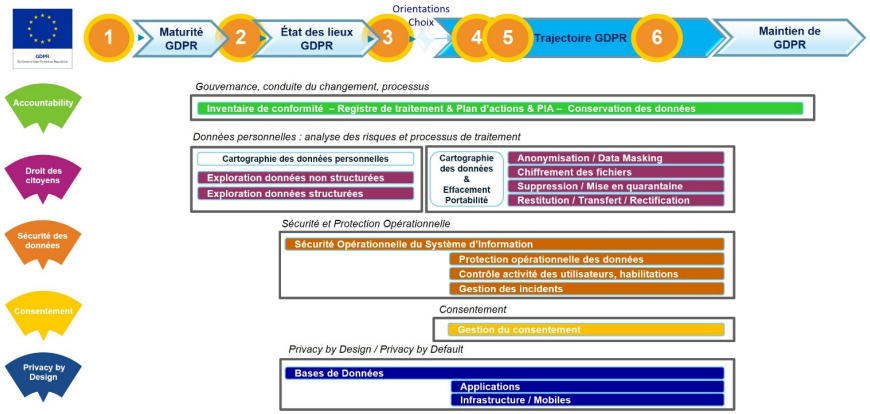


3. La mise en place des outillages : un accélérateur et un facteur clé d'une conformité durable

Du point de vue de la mise en œuvre du GDPR, l'application de la réglementation se traduit, selon IBM, par cinq domaines de transformation (cf. *Figure 2*) : le principe d'« Accountability », le droit des citoyens, la gestion du consentement, la sécurité des données personnelles et celui de « Privacy by Design ».

Pour chacun de ces domaines nous avons identifié des fonctions essentielles dans la phase d'état des lieux (analyse d'écart) tout comme dans la phase de trajectoire de mise en conformité. Chacune de ses fonctions pourra ensuite être appuyée ou accélérée par la mise en œuvre d'une solution technologique.

Figure 9 : Les fonctions technologiques pour relever les enjeux des 5 domaines GDPR



1. **Accountability -** Les règles définies pour la protection des données doivent être formalisées dans un référentiel. Les outils de **tenue de registre** et de **documentation des traitements** avec workflow sont les compléments indispensables des outils **d'enregistrement et d'exécution automatisée des règles de conservation**. En phase d'audit, on vérifiera l'existence et la documentation des règles alors qu'en phase de trajectoire on pourra aussi s'intéresser à leur automatisation.

2. **Droit des citoyens -** En phase d'état des lieux, une des tâches d'un projet de mise en conformité GDPR est de **situer les données**, notamment en explorant les zones à risque. Par exemple, des informations sensibles au sens GDPR se trouvent fréquemment dans des emails ou des serveurs de fichiers (shadow IT, données non structurées, notes d'interaction client, ...). Des solutions d'exploration de données à base de reconnaissance de catégories (numéro de sécurité sociale, appartenance syndicale…) permettent cette **cartographie**.

En phase de Trajectoire de mise en conformité GDPR, des processus de traitement nécessaires à cette mise en conformité pourront être définis. Les principaux processus sont :

- ✓ **Anonymisation ou Data Masking** : Utilisé surtout lorsque des données quittent un environnement sécurisé servant au métier pour copie vers d'autres environnements techniques. Il s'agit, par exemple, des données de production recopiées en environnement de test pour mener des tests de non-régression logiciels. La problématique de ce processus est de transformer les données afin qu'elles soient représentatives (pour la qualité des tests) mais non réelles (pour respecter les obligations). Il s'agira également de transformer les données de manière à préserver l'intégrité du jeu d'essai (par exemple sans casser les liens d'intégrité dans une base relationnelle).

- ✓ **Chiffrement** : Il s'agit de protéger les supports de stockage au niveau du stockage physique. Le GDPR insiste sur l'importance de chiffrer les informations pour les protéger. En effet, une fuite de données chiffrées est illisible et ne pourra donc pas être exploitée. Le règlement GDPR mentionne même explicitement ce cas comme une exception à l'obligation de communication d'un incident aux personnes concernées (Article 34 - 3a). Le chiffrement des fichiers, des bases de données ou des environnements Big Data est donc une des pratiques de base de la protection de l'information.

- ✓ **Suppression** : il s'agit de répondre à la demande d'un citoyen d'effacer les données le concernant de manière cohérente et auditable. De plus, si une donnée ne peut pas être conservée plus d'un certain temps (ex : carte de crédit après un achat) ou si l'entreprise a découvert que sa présence se révèle inutile, il faudra l'effacer de manière cohérente (sans mettre en péril le comportement de l'application), auditable (démontrer qu'un effacement a eu lieu) et permanente (irréversible).

- ✓ **Mise en quarantaine des données** : ce processus permet de limiter l'accès à un document dont le contenu est soupçonné d'être en écart de conformité du point de vue GDPR, le temps de l'analyser pour décider de l'action à prendre.

- ✓ **Restitution & Transfert** : un citoyen peut faire valoir son droit à l'oubli, son droit de rectification ou celui de portabilité des données personnelles. Des processus doivent être mis en place pour collecter les informations puis les mettre à jour ou les transférer vers un tiers (nouvel opérateur téléphonique par exemple) afin de pouvoir effectuer les traitements qui dérivent de l'exercice de ces droits. Ces processus doivent être auditables.

3. **Sécurité des données -** Pendant l'état des lieux, on analysera la sécurité des données : Il faudra vérifier que les processus de protection sont bien définis et mis en œuvre puis contrôler leur bon fonctionnement. En phase de trajectoire de mise en conformité on devra organiser la sécurité opérationnelle :

   - ✓ **Mettre en place une protection opérationnelle des données** : suivre en temps réel l'accès aux données et empêcher les accès non conformes.
   - ✓ **Gérer les incidents** : à chaque incident détecté un processus d'alerte doit être déclenché (selon le cas : vers l'autorité de contrôle, la victime et/ou les services concernés pour remédier au problème).
   - ✓ **Contrôler l'activité des utilisateurs** : il faudra vérifier que les utilisateurs de données, y compris les utilisateurs privilégiés, disposent d'un accès qui soit adéquat vis-à-vis des règles définies et de leurs rôles. Par exemple, on ne pourra pas accepter d'un administrateur de bases de données qu'il s'attribue des droits pour effectuer des actions qui n'entrent pas dans son champ d'action.

4. **Gestion du consentement** - La gestion du consentement se traduit par deux mécanismes asynchrones :

   - ✓ Le premier consiste à **présenter, obtenir et enregistrer la position du client** vis-à-vis d'un groupe de données personnelles et d'un traitement lui correspondant. Cette position doit pouvoir être révisée par le client.
   - ✓ Le deuxième consiste à **vérifier** lors des traitements **la licéité de ce traitement** au regard de la position du client pour éventuellement l'exclure. Ce mécanisme peut également fonctionner sur un principe de filtrage.

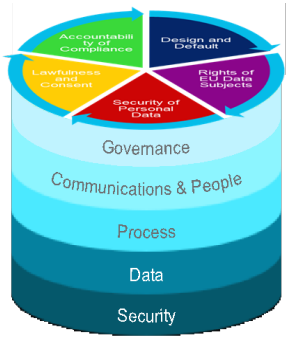
5. **Privacy by Design -** Les applications doivent être conçues de manière à intégrer la protection des données personnelles. Les développeurs doivent être sensibilisés au sujet. De plus, l'outillage de développement et de test pourra prendre en compte les problématiques de failles de sécurité. De la même manière, les données et l'infrastructure (par exemple les terminaux) doivent faire l'objet d'une protection permanente dès la phase de conception du système.

Le délai pour se conformer aux exigences de la nouvelle réglementation est très court. Pour accompagner les entreprises, IBM propose une offre unique associant une expertise méthodologique et une expertise technologique qui est à ce jour une des plus développées sur le marché français.

4. Les points sensibles de la mise en conformité

L'état des lieux et la démarche : la difficulté de passer à l'échelle - Comme déjà évoqué plus haut, l'état des lieux et la démarche de mise en conformité comprennent cinq niveaux complémentaires et indispensables qu'il faut adresser (Figure 3). En fonction de l'entreprise, du rôle du leader de la démarche et de la gouvernance du programme, certains niveaux sont privilégiés dans un premier temps dans la phase d'inventaire. Néanmoins, tous devront être couverts afin d'atteindre un degré de conformité satisfaisant. La prise en compte de ces cinq dimensions témoigne véritablement du passage à l'échelle du programme. Nous avons observé que cette transition est plus ou moins rapide selon les entreprises.

Figure 3 : Les cinq niveaux d'un programme GDPR



L'audit technique des données personnelles : une option méthodologique qui s'avère souvent payante sur l'univers non structuré - L'audit technique des données personnelles, consistant à les identifier et les situer au sein du SI, est un complément précieux à l'état des lieux déclaratif. Il permet de mieux apprécier les risques, donc les priorités, ainsi que l'évaluation des chantiers de remédiation. Cet audit peut être conduit tant sur des données structurées que non structurées. Cependant l'importance prise par le travail collaboratif (messagerie, groupe de collaboration, partage documentaire, …) et parfois le « shadow IT » le rendent très utile voire indispensable sur l'univers non-structuré.

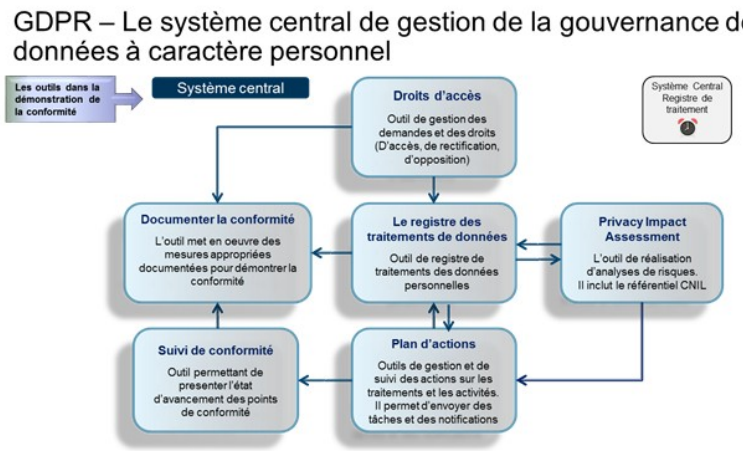
Le registre de traitement des données personnelles : la première pierre de « l'accountability » - Selon l'article 30 du règlement, la tenue du registre des traitements des données personnelles est obligatoire. La mise en œuvre de ce registre est une priorité pour l'immense majorité des organisations. En effet, le registre sera l'outil de démonstration de la conformité et le tableau de bord du DPO (Data Protection Officer) à échéance mai 2018. Pour répondre à cette obligation, nous observons trois approches : le développement spécifique, l'usage d'outils bureautiques ou le choix d'un progiciel métier dédié à la protection des données personnelles.

Parmi les exigences du règlement, nous répertorions 4 exigences fonctionnelles proches du registre :

- L'analyse de risques (Privacy Impact Assessment – PIA)
- La formalisation du plan d'actions et le suivi de la conformité,
- La documentation de la conformité,
- La gestion des demandes de droits des personnes.

C'est ainsi que la notion de « **Registre étendu** » incluant ces 4 fonctions en sus du registre apparaît sur le marché.

Figure 10 : Le système central de registre de traitement



Le « Registre étendu » ne saura être une solution isolée du système d'information et apparaît comme étant à intégrer dans ce dernier :

- Synchronisation avec l'annuaire d'entreprise,
- Remontée des preuves des systèmes de détection de failles,
- Liens avec les canaux de collecte des demandes des droits des personnes et recueils des consentements,
- Collecte des preuves de traitement des données (effacement, anonymisation, encryption, etc.).

La gestion du consentement : un point sensible visible de l'extérieur ? - La gestion du consentement est une préoccupation complémentaire au « Registre étendu ». Elle nécessite trois fonctions principales dont deux ont déjà été évoquées dans le chapitre précédent : la collecte multi-canal et la formalisation des consentements des personnes, la capacité à exposer ces consentements aux applications dont l'usage en nécessite l'autorisation.

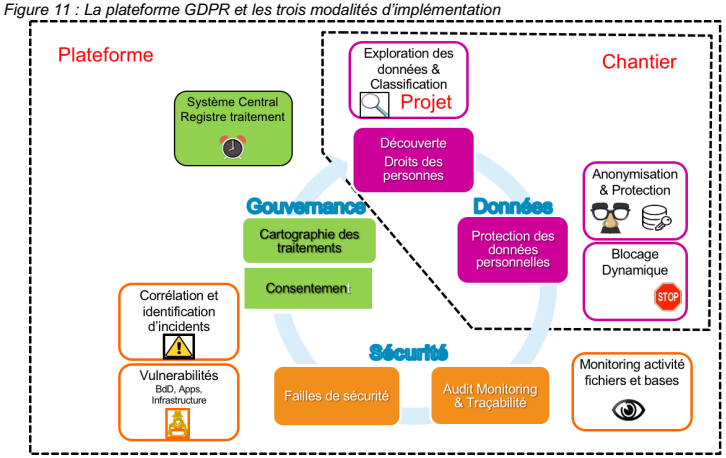
Un troisième aspect tend à se développer : la vue à 360° des consentements d'une même personne et les reportings associés. En particulier, pour créer la confiance et se différencier, certaines études suggèrent de rendre cette vue accessible sans requête spécifique de la part du client (via le site web par exemple).

La maitrise des données non seulement facteur de réussite mais également facteur de différentiation - Répertorier les données manipulées par les applications, par le biais de dictionnaires existants par exemple ou d'outils de gouvernance de données, facilite l'identification et la maitrise des données structurées. Cependant GDPR exige plus. En particulier le principe de minimisation des données (« ne collecter que les données nécessaires à la finalité du traitement ») accroit l'exigence de rigueur dans la gestion des données personnelles. Pour y répondre, de nouvelles démarches de découverte de données outillées et plus sophistiquée émergent. Elles visent à identifier, non seulement les données personnelles, mais également leur contexte d'utilisation. Ainsi, dans une perspective de minimisation de données, il est possible de déterminer si celles-ci sont légitimes. On voit également apparaître ici un point de réconciliation possible avec la description des types de données consignée dans le registre de traitement. La capacité à correctement minimiser les données collectées et à le faire savoir, combinée à une bonne gestion des consentements laquelle sera visualisable est un axe de différentiation du point de vue de l'expérience client.

Trois approches d'implémentation de GDPR co-existent. Elles sont dépendantes du contexte et des ambitions de chaque acteur – Nous observons trois modalités d'implémentation de GDPR :

- « Projet » : des fonctions unitaires, par exemple anonymisation de données, sont mises en œuvre en général à grande échelle l'une après l'autre. Cette approche résulte souvent d'une priorisation urgente sur un domaine identifié comme sensible avec la volonté d'anticiper ou bien dans un contexte de ressources financières limitées
- « Chantier » : un groupe de fonctions est implémenté pour servir une thématique, par exemple la thématique des données avec des fonctions d'anonymisation, de découverte, d'archivage. La volonté est en général de reprendre en main tout un domaine (dans le cas cité la gouvernance des données). L'approche chantier permet de répartir entre acteurs fonctionnant relativement indépendamment les resposanbilités. Il faut veiller dans ces cas à préciser les frontières (par exemple la protection des données peut avoir une lecture gouvernance de données avec l'anonymisation et une lecture sécurité avec la protection et le monitoring des accès)
- « Plateforme » : tous les aspects sont adressés dans une optique de mise en œuvre de plate-forme de services interne ou proposée à des clients externes. Typiquement certains grands groupes internationaux, disposant de nombreuses activités variées s'engagent dans cette voie pour rationaliser l'effort de compliance et homogénéiser les pratiques. La vue d'une plateforme GDPR avec ces trois grands chantiers : données, gouvernance et sécurité est représenté ci-dessous.

Figure 11 : La plateforme GDPR et les trois modalités d'implémentation



Evaluation budgétaire : quel budget allouer ? - GDPR exige tant un programme de conformité juridique (inventaire, organisation, sensibilisation, …) qu'une transformation du système d'information. Etant donné la proximité de l'entrée en vigueur de ce règlement, une des priorités actuelles de nombreux clients consiste à évaluer les budgets de ressources, d'assistance, et de mise à niveau du système d'information (études d'impacts, développement/mise en œuvre d'outils, …).

Certaines organisations adoptent un programme global comprenant les cinq niveaux décrits plus haut et son financement. Ce dernier est dimensionné proportionnellement aux risques financiers et de réputation encourus. En fonction du niveau d'exposition du risque à la collecte et au traitement des données personnelles, l'ordre de grandeur peut varier d'un facteur de un à dix. Par ailleurs il existe bien entendu une corrélation entre la complexité de l'organisation (chiffre d'affaires, pays, type d'activités, poids des activités européennes) et le budget GDPR.

Dans ce budget, la transformation du système d'information représente une part majoritaire de l'investissement.

Concernant les outils, la multiplicité des technologies et des interactions rend plus complexe l'estimation des coûts d'investissement, de fonctionnement et leur maîtrise dans les trois prochaines années. En parallèle, une complexité peut naître de la nécessaire intégration des différents outils retenus.

Ainsi, certains clients se posent la question de la mise en place d'un « framework » GDPR unifié regroupant les technologies requises. L'unification technologique du framework, présente un avantage indéniable concernant la maîtrise technique et l'intégration de l'outillage. D'autre part, un framework GDPR apporte un bénéfice tangible de massification financière pour l'acquisition des technologies et leur intégration mutuelle.

Pour en savoir plus sur le GDPR, vous pouvez nous contacter :

IBM est acteur majeur en matière de nouvelles technologies et d'innovation dans les domaines du Cognitive Business et du Cloud. IBM propose notamment une offre de services et des technologies pour adresser les problématiques du GDPR et plus largement celles de la gouvernance des données.
N'hésitez pas à consultez notre site Internet : ibm.biz/GDPR_fr

- **Pascale ASCIONE**, GBS GDPR Leader, pascale.ascione@ibm.com
- **Thierry BRUN**, GDPR Ambassador**,** thierrybrun@fr.ibm.com @IBMThierryBRUN
- **Bruno FERNANDES**, GDPR Solutions & Services, bruno.fernandes@fr.ibm.com

IBM's commitment to GDPR readiness
IBM is committed to providing our clients and partners with innovative data privacy, security and governance solutions to assist them on their journey to GDPR compliance.

Trust in Data
Data and its protection are becoming increasingly important to individuals and society. Enterprises must earn the public's trust in their ability to steward information. As IBM's long history of security and privacy leadership demonstrates, IBM understands that protecting privacy is essential to gaining trust. IBM was one of the first companies to appoint a Chief Privacy Officer, to develop and publish a genetics privacy policy, to be certified under the APEC Cross Borders Privacy Rules system, and to sign the EU Data Protection Code of Conduct for Cloud Service Providers. Now, IBM is continuing its long-standing leadership in the area of data privacy by responding proactively to the General Data Protection Regulation (GDPR).

IBM Commits to GDPR Readiness
IBM currently complies with privacy laws around the world. IBM is also preparing to comply with the European Union's new General Data Protection Regulation (GDPR) which will go into effect in May 2018. IBM has established a global project to prepare for GDPR, both for our internal processes and for our commercial offerings. IBM recognises that our customers will rely on IBM's offerings and technical assistance to achieve GDPR compliance within their own organisations and IBM is well-positioned to meet this critical need.
As part of its GDPR project, IBM is enhancing its ongoing commitment to privacy by design. IBM is working to embed data protection principles even more deeply into its business processes, with the objective that technical and organisational security measures limit, by default, the amount and use of personal data to what is specifically required. This work will also strengthen controls already in place to limit access to personal data, including with respect to mobile applications that rely on sensible default settings to prevent personal data from being inadvertently shared with others.

Compagnie IBM France
17 Avenue de l'Europe
92275 BOIS COLOMBES CEDEX

Imprimé en France
Novembre 2017