GDPR, LE NOUVEAU COMPTE A REBOURS DE LA GOUVERNANCE DE L'INFORMATION ?

Un Règlement Général sur la Protection des Données (RGPD) de portée mondiale, avec une date butoir de mai 2018, impose aux entreprises de se mettre en conformité sous peine de sanctions et d'amendes lourdes de conséquences pour leur rentabilité et leur réputation.

Les entreprises sont en effet contraintes sur un délai relativement court de revoir leur stratégie de confidentialité, d'accès, de sécurité et de gouvernance de l'information dès aujourd'hui. Ainsi le RGPD (ou GDPR en anglais) prendra effet le 28 mai 2018, autant dire demain. Et les données concernées sont nombreuses : identification, vie personnelle, comportement, localisation, données économiques et financières et celles dites sensibles. De quoi affoler les directions générales mais aussi juridiques, d'audit, du risque, de contrôle interne et informatiques.

Un règlement d'une centaine de pages a été publié en 2016 prenant appui sur une précédente directive européenne datant de 1995 la DPD (Directives sur la Protection des Données). Certains de ces articles impactent directement le Système d'Information, son organisation et ses processus clés de gouvernance et de management.
Les exigences de ce nouveau règlement général sont nombreuses et contraignantes tout en étant lourde de conséquences si elles ne sont pas respectées.

Les plus significatives sont les suivantes :

- Des évaluations, à partir des données, d'impact sur la vie privée, le PIA (Privacy Impact Assessment) ;
- Une confidentialité et une sécurité de l'information systématiques ;
- Des inventaires et une cartographie des données personnelles sur l'ensemble des bases de données, des applications et plus généralement des systèmes d'information en place ;
- La nomination obligatoire d'un délégué à la protection des données (DPO ou Data Protection Officer) ;
- La notification, auprès du législateur, sous 72 heures de la violation des données personnelles détectée ;
- Les preuves documentées permettant de valider des « efforts raisonnables » mis en avant dans tous ces domaines.

De plus, certaines exigences du RGPD impactent fortement la façon dont les entreprises vont récupérer l'information puis la spécifier en définissant un but précis et enfin préciser les termes de son utilisation, de son partage dans un temps défini afin de prévoir aussi son éventuelle suppression.

Indépendamment de la justification de la collecte d'information de la part de l'entreprise, les personnes concernées par cette collecte doivent de manière proactive « choisir de participer » et donner leur consentement d'une façon **spécifique, éclairée, univoque et libre**. On le voit ici, les problèmes vont rapidement se poser concernant le partage de données avec des tiers ou bien leur utilisation à des finalités différentes de celles initialement prévues.

Le système d'information impacté

Plusieurs questions doivent apporter des réponses précises avec preuves à l'appui au sein des directions informatiques des entreprises.

En voici quelques-unes avec leur début de réponse :

- Connaissez-vous ou maîtrisez-vous correctement les données personnelles que votre entreprise détient et leur lieu de stockage ou d'archivage ? **Un rapport d'audit et une cartographie précise des données sont indispensables à ce stade.**
- Avez-vous intégré dans votre référentiel de risques IT, le risque de non-conformité de la protection des données personnelles et avez-vous un processus d'analyse d'impact et d'évaluation de risques établis ? **Une gestion des risques dédiée au GDPR est nécessaire et doit être alignée avec le référentiel de risques de l'entreprise.**
- Qui gère la sécurité de l'information en général dans l'entreprise et auprès de qui reporte-t-il ? **Un RSSI est généralement identifié portant une responsabilité assignée sur le sujet sécurité et est souvent rattaché à une DG.**
- Avez-vous une politique liée à la sécurité de type cryptage, anonymisation, pseudonymisation des données personnelles de l'entreprise ? **Dans le cas contraire une démarche dans ce sens devra être mise en place.**
- Qui possède précisément dans votre entreprise des droits d'accès aux données privées et plus généralement qui a accès à quoi, quand et pourquoi **? Un processus formalisé sur la gestion des accès déterminant avec clarté les autorisations nécessaires est incontournable.**

GDPR, LE NOUVEAU COMPTE A REBOURS DE LA GOUVERNANCE DE L'INFORMATION ?

- De quelle manière surveillez-vous et contrôlez-vous les accès aux données personnelles de votre entreprise, seriez-vous susceptible de détecter, d'analyser puis de notifier un éventuel piratage ou une tentative d'intrusion et pouvez-vous en apporter la preuve ? **Une démarche justifiée doit faire l'objet d'un avertissement aux autorités dans les 72 heures suivant l'identification ou la confirmation de l'événement.**
- Datez-vous systématiquement la durée de vie des données au sein de votre entreprise ? Si oui, êtes-vous en capacité de réduire significativement le volume de données privées utilisé dans vos systèmes d'informations, bases de données ou fichiers non productifs ou actifs ? **Réduire au maximum la conservation des données et savoir éliminer ces dernières de manière légale.**
- Pouvez-vous prévenir l'accès ou le transfert de bases de données en dehors du pays ou de l'UE ? **Réduire les transferts de données personnelles au maximum en dehors de l'UE ou vers des pays tiers de façon à préserver le niveau de protection des personnes garanti par la réglementation en vigueur.**

Une première bonne pratique dans ce contexte

La CNIL, le régulateur en France a, fort à propos, publié une check-list appréciable permettant de dérouler une approche identifiant les étapes indispensables à respecter, pour un premier niveau, de mise en conformité du GDPR.

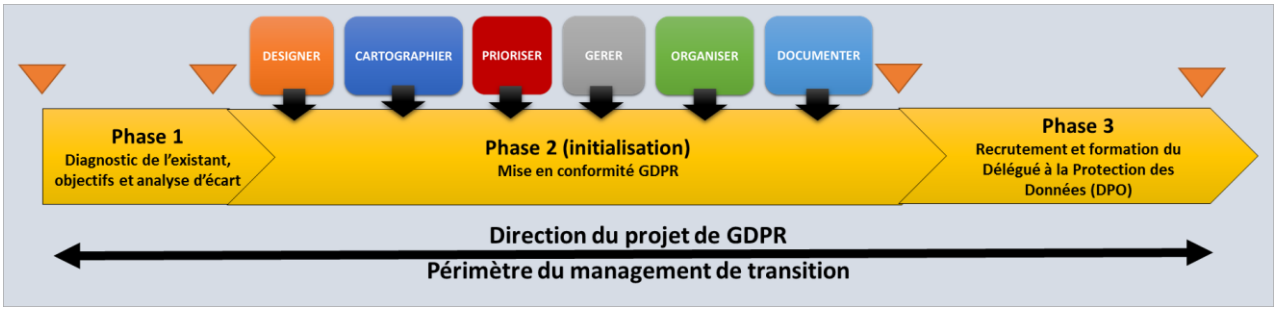
Elle repose principalement sur 6 étapes pour mener à bien un projet de cette ampleur :

Néanmoins, une démarche de conformité ne s'improvise pas simplement à travers la compilation de livres blanc et un corpus de bonnes pratiques. Un projet doit être mené et un pilote identifié.

Un mode projet et un manager de transition expérimenté pour initier et formaliser la démarche de conformité GDPR

Avant de recruter son futur DPO ou de faire monter en compétence son CIL (Correspondant Informatique & Libertés) s'il existe, un manager expert en gouvernance, risque et conformité peut idéalement piloter le projet en lui donnant toute sa légitimité dans l'organisation demandeuse.

Trois phases indispensables pour mener à bien sa mission :



Ces phases seront à détailler en fonction de la maturité estimée et des résultats de l'analyse d'écart issus de la Phase 1.

« Bien dire et bien penser ne sont rien sans bien faire … »

©*Pierre Calvanèse, 24 avril 2017*