WAVESTONE

RGPD,
1 AN DE TRAVAUX, QUEL BILAN EN TIRER ?

Avril 2016, mai 2018, 2 ans pour se mettre en conformité, et il ne reste déjà plus que 8 mois pour mener les travaux exigés par le Règlement Général sur la Protection des Données (RGPD ou GDPR). Où en sont les grands acteurs concernés, seront-ils conformes d'ici mai 2018 ? Quels sont les chantiers les plus complexes aujourd'hui ? Qu'apprendre des travaux déjà réalisés ?

Notre retour d'expérience s'appuie sur un échantillon correspondant à nos interventions auprès de 20 grands comptes présents internationalement (Banques, Assurances, Transports, Énergie, Services, Grande distribution, etc.) et plus de 40 donneurs d'ordre.

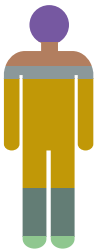
DES PROGRAMMES IMPORTANTS MOBILISANT TOUTES LES DIRECTIONS DE L'ENTREPRISE

Les programmes de mise en conformité au RGPD impliquent très largement dans les entreprises : de quelques dizaines à quelques centaines d'acteurs. Les charges consolidées vont de 3 à 4 ETP (équivalent temps plein) pour les environnements les plus petits et les plus conformes ; jusqu'à plusieurs dizaines d'ETP pour les environnements les plus complexes et les plus éloignés de la cible.

CONTACT

RAPHAËL BRUN
raphael.brun@wavestone.com
YOURI DUFAU-SANSOT
youri.dufau-sansot@wavestone.com

Cette charge de mise en conformité est généralement répartie comme suit :



15% pour le pilotage
10% pour le DPO
5% pour le juridique
45% pour l'IT et le Digital
20% pour les métiers
5% pour le RSSI

15 % pour l'équipe en charge du pilotage du programme, de la coordination et de la communication/formation

10 % pour les équipes DPO, risques ou conformité afin de formaliser les politiques, directives et process, définir l'organisation cible, et s'assurer de la conformité des solutions déployées par les équipes métiers et IT

5 % pour l'équipe juridique afin d'interpréter le texte, proposer des clauses et mentions légales conformes et arbitrer sur des points juridiques identifiés au cours du projet (notamment les durées de conservation)

45 % pour les équipes IT et Digital, dont environ 10% de création de nouveaux services et de définition de solutions IT de conformité (en particulier, exercice des droits, consentement, suppression et portabilité des données) et 35% de mise en conformité nécessitant de faire évoluer les systèmes existants et d'intégrer les exigences du RGPD dans les développements en cours

20 % pour les équipes métiers/business en vue de cartographier leurs processus, les mettre en conformité et faire évoluer les parcours clients et les modalités de fonctionnement avec partenaires et collaborateurs

5 % pour les équipes du RSSI et la filière cybersécurité afin de faire évoluer les programmes existants de surveillance des systèmes et de notification d'incidents de sécurité, de revue des droits ou de mise sous contrôle du process de gestion des habilitations pour inclure la problématique des données personnelles, ainsi que pour participer à la construction du Privacy by design en apportant son expérience sur l'intégration de la sécurité dans les projets

Contrairement à certaines idées préconçues, la charge pour les équipes juridiques et le RSSI reste donc limitée au regard de la charge globale. En effet, les travaux d'analyse du règlement ayant occupés les premières semaines des programmes sont aujourd'hui généralement terminés ou presque, et remplacés par des chantiers plus opérationnels à la dimension juridique plus faible. Pour les chantiers de cybersécurité, ils se révèlent souvent non directement portés par les programmes RGPD mais plutôt par les programmes cybersécurité existants.

Les charges IT ne doivent pas être sous-estimées en ce qu'elles représentent près de la moitié des charges globales du programme. En effet, si ces charges n'apparaissent pas nécessairement dès le début, elles sont nécessaires pour décliner opérationnellement les évolutions des process métier, et les exigences des départements juridiques et des équipes du DPO.

Cette répartition des charges sera sujette à évolution une fois le programme RGPD achevé et la mise en œuvre des projets commencée. En particulier, les équipes du DPO vont se focaliser de plus en plus sur un rôle de formation, de contrôle et d'accompagnement des projets qui prendra un poids plus important, tandis que la part de la DSI diminuera une fois terminés les travaux de mise en conformité de l'existant et d'intégration des exigences dans les développements futurs.

Quelques exemples

ASSURANCE
+ de 40 Business Units
Près de 300 acteurs sollicités
Pilotage en central par 4 ETP

BANQUE
~ 50 entités
Plus de 250 acteurs sollicités
Pilotage en central par 3 ETP

DISTRIBUTION
Une dizaine de Business Units
Plusieurs dizaines d'acteurs sollicités
Pilotage en central par 3 ETP

ÉNERGIE
Un maillage régional très fort
Plusieurs centaines d'acteurs sollicités
Pilotage en central par 7 ETP

5 PANS DU PROGRAMME RGPD QUI CONCENTRENT LES INVESTISSEMENTS…

La mise en œuvre de la conformité au RGDP peut aujourd'hui se décliner au travers de 5 axes principaux :

1 **Le pilotage du programme et l'expertise** à apporter sur les points durs (15 %) **:** cadrage des chantiers, construction budgétaire, suivi des actions, reporting, coordination avec les autres projets et initiatives, veille, etc.

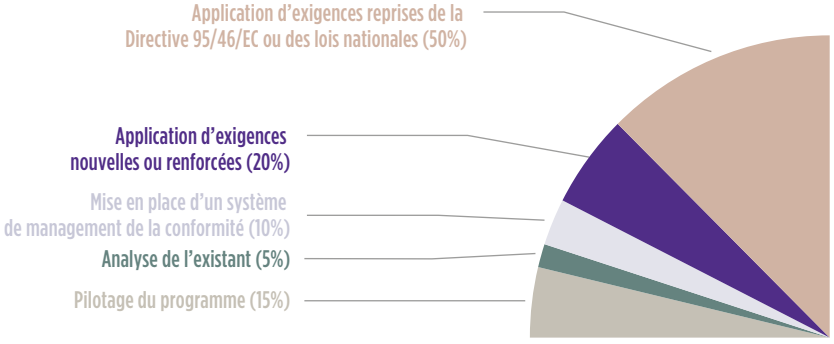
2 **L'analyse de l'existant** via notamment la construction d'un registre des traitements de données et l'identification des points sensibles ou de non-conformités majeures (5 %, majoritairement métiers et DPO). Une attention particulière devra être accordée au process de constitution du registre et de priorisation des traitements à analyser afin de ne pas surinvestir dans ce pan du programme.

3 **La mise en place d'un système de management de la conformité** comprenant la définition des politiques, directives, méthodologies et outils de conformité, la mise en œuvre d'une organisation autour du DPO, l'instauration de contrôles et d'audits de conformité ainsi que la formation et la sensibilisation des acteurs concernés (10 %, majoritairement DPO).

4 **L'application des exigences nouvelles ou renforcées** autour de la gestion du consentement, de la construction de l'accompagnement des projets IT en Privacy by design, ainsi que de la mise en œuvre de la portabilité (20 %, majoritairement métiers et IT).

5 **L'application d'exigences existantes et déjà connues issues de la directive 95/46/CE ou des lois nationales** sur la protection des données à caractère personnel telles que l'information des personnes et l'exercice des droits (accès, suppression…) et la capacité à retrouver et à supprimer toutes

Répartition du budget par chantier



les données associées à une personne au sein de l'organisation une fois les durées de conservation définies expirées, l'encadrement des transferts (à des tiers ou hors UE), l'amélioration des mesures de sécurité existantes, l'anonymisation des données hors production… (50 %, majoritairement métiers et IT).

Sur la plupart des programmes accompagnés, la moitié des investissements concernent des actions de mise en conformité déjà exigées par les lois nationales et communautaires (directive 95/46/CE) antérieures.

…POUR 5 POINTS DURS COMMUNÉMENT CONSTATÉS…

Une fois les cadrages de programme réalisés, les premiers résultats des analyses d'écarts produits, les sujets difficiles émergent. Nous constatons que quel que soit le contexte, le secteur d'activité, la nature des données manipulées ou le niveau de conformité existant, ces 5 points durs ressortent chez la majorité de nos clients.

La position du régulateur sur certains sujets, les difficultés d'interprétation du texte et le manque de maturité des acteurs. Plusieurs thématiques du RGPD, comme par exemple le droit à la portabilité, n'ont pas vu leurs dispositions d'application être clairement définies. Sur ces exigences nouvelles ou difficiles à mettre en œuvre, les organisations pionnières courent donc le risque de devoir défaire ce qu'elles auront entrepris si cela s'avère contraire à l'interprétation finale. Cela peut entraîner un effet de latence autour de la mise en œuvre opérationnelle de ces exigences difficilement appréhendables en l'état par les organisations. De plus, pour certains sujets plus techniques, en particulier la classification des données ou l'anonymisation, de nombreuses solutions du marché ne sont pas encore complètement matures.

L'application des délais de rétention et du droit à l'oubli au sein des systèmes informatiques existants. En effet la situation est souvent complexe du fait de choix historiques : données personnelles utilisées comme identifiant unique dans les systèmes de base de données, champs obligatoires techniques non indispensables d'un point de vue business… Ce sujet requiert un investissement pouvant être important sur des applications historiques (généralement de 40 k€ à 200 k€ par application). La contrainte de suppression est parfois quasi impossible à mettre en œuvre au regard des impacts non maitrisés sur le SI, et l'ensemble des données concernées est souvent difficile à identifier. Ce problème peut être traité au travers d'un remplacement des données par une autre valeur voire par de la tokenisation.

La gestion de la relation avec les sous-traitants afin d'assurer une conformité de bout-en-bout. En particulier, l'effort de collecte, de recensement et d'adaptation des contrats avec les fournisseurs peut prendre une ampleur importante suivant le degré de décentralisation de la gestion des contrats. Il s'agit alors d'appliquer des solutions simples et efficaces en se concentrant sur l'intégration des clauses RGPD dans les contrats à venir. Et pour l'existant ? Il est possible de communiquer vos exigences (mentions légales d'information par exemple) aux fournisseurs en leur rappelant l'obligation d'application du règlement sans forcément renégocier tous les engagements contractuels. La bonne application des contrats doit également faire l'objet d'une attention particulière qui peut entraîner la réalisation de contrôles voire la conduite d'audits de fournisseurs.

La mise en œuvre d'une méthodologie d'accompagnement des projets (Privacy By Design) et des outils d'analyse de risques sur la vie privée (PIA) appréhendables en autonomie par les chefs de projets et réalistes en termes de charge et de contraintes. Même si certaines organisations avaient déjà mis en œuvre des processus d'intégration de la sécurité dans les projets, il est nécessaire de refondre ces processus et de former les acteurs concernés. Quelles bonnes pratiques ? Construire des méthodes qui visent la simplicité et le pragmatisme plutôt que l'exhaustivité et ne pas vouloir dérouler les méthodologies sur tous les projets en mettant en place un tri initial afin de focaliser l'attention sur les plus sensibles.

L'identification de ressources expertes du sujet et à même de contribuer aux chantiers ou d'intégrer l'équipe DPO. Ces ressources sont aujourd'hui extrêmement rares et difficiles à trouver, que ce soit en interne ou auprès de sociétés de services, de cabinets de conseil ou d'avocats. Il convient donc de bien répartir les tâches et ne pas chercher à positionner des experts sur toutes les dimensions du programme et à tous les postes. Les directeurs de programme peuvent par exemple venir de la DSI, les juristes en droit de contrats être formés rapidement à la problématique vie privée, les équipes contrôle interne peuvent aider à l'évolution des processus afférents. En sus, dans des environnements très concernés par des réglementations clients, il conviendra d'intégrer ou partager les initiatives afin de mutualiser au mieux les travaux et livrables produits. À la vue des enjeux et de l'ampleur des programmes, un pilotage rigoureux et réaliste est un prérequis. Il peut être confié de façon temporaire à une équipe spécifique, indépendante de la future organisation DPO.

Concernant le poste de DPO, suivant les contextes, il attire à la fois des convoitises dans les filières conformités ou CIL existantes, mais aussi des appréhensions pour des profils qui ne souhaitent pas endosser ce rôle parfois vu comme apporteur de contraintes et relayant rarement des messages positifs. Ainsi, à l'exception des DPO en place avant la publication du RGPD, la plupart des grands comptes n'ont pas aujourd'hui de DPO identifiés, et ceux-ci ne seront pas nommés avant fin 2017-début 2018.

> « Les programmes ont donc mis du temps à se lancer et avec des réserves budgétaires faibles. L'avancement des états des lieux, des analyses d'écarts et de la complexité des mesures à mettre en œuvre amène nos clients à augmenter régulièrement et très fortement leurs budgets »

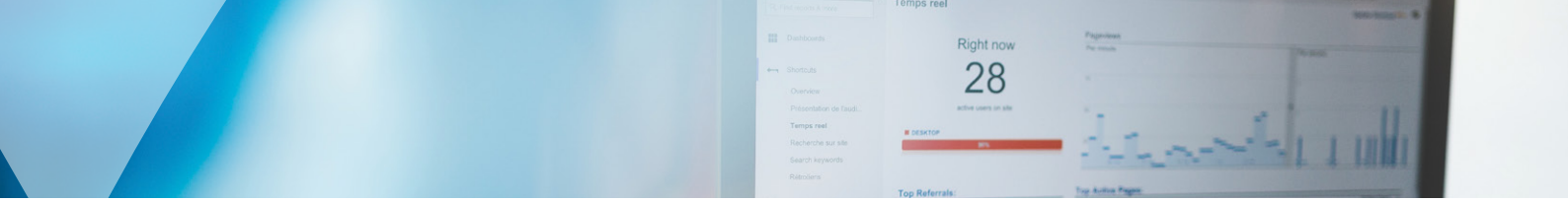
… ET DES BUDGETS EN CONSTANTE AUGMENTATION

Le RGPD est un nouveau sujet. La protection de la vie privée ne l'est pas. La Loi Informatique et Libertés existe par exemple depuis 1978. Cet historique a dans un premier temps fait croire (à tort) à un bon niveau de conformité des organisations et limité la crainte d'un risque important de sanctions.

Les programmes ont donc mis du temps à se lancer pour la plupart des grands comptes : souvent pas avant fin 2016 pour les premiers, et réellement au premier semestre 2017 pour la majorité d'entre eux. Comme pour d'autres sujets de cette ampleur, l'avancée des programmes RGPD a pâti de la complexité de répartition des rôles et responsabilités entre les directions centrales des groupes, dont les ressources mobilisables sur le sujet sont limitées, et les entités locales, souvent en attente de lignes directrices précises des directions centrales pour démarrer les chantiers.

Si nombre de programmes ont démarré avec des réserves budgétaires faibles, l'avancement des états des lieux, des analyses d'écarts et la complexité des mesures à mettre en œuvre amènent de plus en plus nos clients à augmenter régulièrement et très fortement leurs budgets.

Les programmes RGPD se chiffrent aujourd'hui pour de grands groupes internationaux dans des fourchettes de 1 à 5 millions d'euros pour les organisations, principalement B2B, utilisant un nombre raisonnable de données personnelles et peu mobilisées sur le big data ou le profiling ; de 20 à 50



millions d'euros lorsque que l'entreprise, généralement B2C, a plusieurs métiers et de très nombreuses entités/filiales. Pour certains très grands acteurs internationaux, dans les secteurs de la banque ou de l'assurance par exemple, les premiers engagements budgétaires ont même été de plusieurs centaines de millions d'euros, aujourd'hui en cours d'optimisation et de priorisation. Autre facteur de coût, les évolutions en profondeur de multiples applications font grimper rapidement les montants.

Au regard de ces coûts importants, les directions générales exigent de plus en plus des directions métiers et IT de dé-prioriser d'autres budgets ou d'absorber les chantiers identifiés au sein de programmes existants, en particulier de cybersécurité, de revue contractuelle, d'archivage des données ou d'évolution de la relation client.

> « Mai 2018 ne sera pas la fin de la conformité, mais une 1re étape »

L'impact financier particulièrement important des programmes RGPD, et la charge nécessaire pour les déployer, implique aujourd'hui que de revoir le planning initialement envisagé (mai 2018) afin de lisser cette charge et ces budgets dans le temps. Mai 2018 n'est plus une échéance de mise en conformité, mais plutôt la fin de la première étape de la mise en conformité, où il faut avoir réalisé les travaux les plus importants et disposer d'une feuille de route claire pour la suite.

COMMENT SE METTRE EFFICACEMENT SUR LA VOIE DE LA CONFORMITE D'ICI MAI 2018

Quelques règles simples sont à suivre afin de bien engager sa mise en conformité :

Piloter utile. Construire une structure de pilotage au niveau du groupe qui ne vise pas uniquement à exiger et contrôler, mais plutôt à s'assurer de pouvoir proposer des outils opérationnels aux entités pour les aider dans leur mise en conformité, et de le faire rapidement afin de ne pas ralentir ou inhiber les initiatives locales. Par exemple : ne pas attendre fin 2017 pour proposer sa méthode PIA.

Identifier et prioriser les traitements à risque : certains sont faciles à identifier (manipulation de données de santé, gestion de la fraude…) et d'autres nécessitent expertise et une certaine expérience du sujet (comme par exemple les fichiers RH de « jurisprudence interne », théoriquement anonymisés, et en pratique uniquement remplacés par un pseudonyme, et donc souvent facilement ré-identifiables).

Ne pas chercher à analyser tous les traitements d'ici mai 2018. En effet, constituer un inventaire prend du temps, mais analyser les traitements qui le constituent encore plus (à minima 4 à 5 fois plus de temps). Cette analyse, qui nécessite une forte expérience et expertise en data privacy, ne peut être menée exhaustivement d'ici mai 2018 (pour des raisons de coûts, mais également de manque de ressources sachantes à même de les mener). Il convient donc d'analyser les traitements les plus à risques dans un premier temps (20 à 30% des traitements) et de disposer d'une feuille de route claire pour l'analyse des suivants.

Traiter les thématiques en parallèle pour être plus agile. Le programme ne doit pas être un programme Top Down où les opérationnels attendent des mois des outils et politiques du groupes avant de pouvoir commencer leurs travaux de conformités. Tous les acteurs impliqués (métiers, conformité, IT, CISO, Legal etc.) doivent pouvoir avancer en parallèle et s'alimenter les uns les autres dans une démarche souple et agile. Les équipes IT n'ont pas exemple pas besoin d'attendre que les métiers identifient des durées de rétention et demande à les appliquer dans les systèmes pour identifier les solutions applicables et les outils associés (notamment tokenisation irréversible).

Mutualiser tout ce qui peut l'être. En effet, rien ne sert de réinventer la roue. Les équipes centrales peuvent contribuer à construire et proposer des accélérateurs. Ainsi, plutôt que de demander à toutes les entités de constituer leur inventaire, il est souvent pertinent de proposer un modèle avec les 70 à 80 % de traitements communs à l'ensemble des entités. Le programme s'en trouvera facilité et la charge de mise en conformité réduite de façon importante.

Expliquer, expliquer et ré-expliquer. Le RGDP et sa déclinaison est un sujet complexe, aux multiples ramifications et qui sollicitent de nombreux acteurs de l'organisation qui ne connaissaient rien au sujet il y a encore quelques mois. Il faut donc faire preuve d'une pédagogie sans faille et ne pas hésiter à accompagner au plus près les équipes en charge des chantiers afin de les aider à comprendre les exigences et imaginer les solutions.

Faites de la conformité un atout pour votre relation client. Un programme RGPD est avant tout perçu comme une contrainte par les opérationnels. Pour autant, la protection de la vie privée est aujourd'hui un sujet majeur de préoccupation des citoyens que ce soit les clients ou les collaborateurs (idée que nous avons développé dans une précédente publication sur la vie privée dans le numérique avec la vision exclusive des postures de citoyens dans 6 pays : wavestone.com/privacy). Il convient donc d'intégrer le programme au cœur des initiatives autour de la DATA et des chartes associées. La communication autour du programme devra ainsi valoriser les travaux menés afin d'en faire un atout dans la relation client ou collaborateurs.

QUE RETENIR DE L'ANNÉE ÉCOULÉE ?

Les programmes ont mis du temps à se lancer, et la prise de conscience des impacts du règlement, de la taille des programmes et des budgets à déployer en a été d'autant plus retardée.

Pour autant, depuis le début de l'année 2017, de nombreux programmes sont maintenant dans leur phase de remédiation et de premières solutions émergent. Mais tous les chantiers ne pourront être terminés pour mai 2018. Les grands comptes internationaux ne seront donc pas tous 100% conformes à cette date, mais les risques les plus forts seront certainement couverts.

Ainsi, dès à présent, en plus des efforts mis en œuvre pour déployer le maximum d'actions de remédiation d'ici mai 2018, nos clients s'organisent pour disposer d'une organisation DPO opérationnelle rapidement. L'objectif est que celle-ci dispose des budgets adéquats pour conduire l'ensemble des actions identifiées et mettre en place des processus pérennes, garants de la conformité dans la durée.

WAVESTONE

www.wavestone.com

Wavestone est un cabinet de conseil, issu du rapprochement de Solucom et des activités européennes de Kurt Salmon (hors consulting dans les secteurs retail & consumer goods en dehors de France).

La mission de Wavestone est d'éclairer et guider ses clients dans leurs décisions les plus stratégiques en s'appuyant sur une triple expertise fonctionnelle, sectorielle et technologique.