147

Octobre 2017

Patrimoine Data : repenser la gestion des données à l'heure du GDPR

En bref

CIO a organisé une Matinée Stratégique « Data : de la protection au GDPR » le 17 octobre 2017 à Paris avec de nombreux témoins et experts.
Etienne Papin, avocat associé au Cabinet Feral-Schuhl / Sainte-Marie, a présenté les nouvelles règles sur les données. La première table ronde, « Comment abriter le patrimoine de données ? », a réuni Antoine Meissonnier, Conservateur du patrimoine au Ministère de la Justice, et Thierry Milhé, VP International Production of IT Services chez Safran. David Ruiz, juriste au sein de la Direction de la Conformité de la CNIL, et Anne-Sophie Nibert, Group Data Privacy Officer de Total, ont été réunis sur la seconde table ronde « Comment respecter les règles sur les données en développant leurs usages ? » Et le Grand Témoin a été Pascal Courthial, DSI du groupe mutualiste de protection sociale Humanis.

Sommaire

Repenser la gestion des données à l'heure du GDPR

La Matinée Stratégique « Data : de la protection au GDPR » a été organisée par CIO le 17 octobre 2017 à Paris.

Le 17 octobre 2017, CIO a organisé une Matinée Stratégique « Data : de la protection au GDPR » à Paris avec de nombreux témoins et experts. Cette conférence a été réalisée en partenariat avec ASG, Axway, Elée, Information Builders, Ivanti, Pitney Bowes et ReachFive.

La moitié des répondants de l'étude *Comment bien gérer ses données à l'heure du GDPR ?*, réalisée par CIO, ne connaissent pas suffisamment, de leur propre aveu, le règlement général européen sur la protection des données personnelles (RGPD), plus connu sous l'acronyme anglais GDPR. Pourtant, il s'appliquera fin Mai 2018. Les non-conformités pourront dès lors être sanctionnées d'amendes jusqu'à 4 % du chiffre d'affaires mondial de l'entreprise coupable. Ce règlement renforce les obligations classiques de protection et de gestion du patrimoine de données, même s'il n'y a pas réellement de novation par rapport aux grandes lignes des règles qui s'appliquent (ou plutôt devraient être respectées) depuis 1978 en France.
L'étude a été présentée en ouverture de la Matinée Stratégique « Data : de la protection au GDPR » organisée le 17 octobre 2017 à Paris par CIO en partenariat avec ASG, Axway, Elée, Information Builders, Ivanti, Pitney Bowes et ReachFive. Cette conférence visait à détailler les meilleures pratiques en matière de gestion et protection des données ainsi, bien entendu, que de mise en conformité avec le GDPR.

Des données qu'il faut considérées comme juste prêtées

« Serez-vous privés de données privées ? » a ainsi interrogé, un brin ironique, Jean Claude Bellando, Director, Product Solution Marketing, MFT, Axway. Pour lui, il faut en effet considérer que « les données ne sont plus données mais prêtées, les entreprises devenant débitrices des données qui leur sont confiées et qu'il va falloir, comme l'argent

ique, être en mesure de restituer. » Le RGPD implique en effet un

consentement éclairé à la remise de données dans un objectif précis, l'autorisation pouvant être révoquée à tout moment. Le deuxième pilier du RGPD est bien sûr le contrôle. Or la donnée circule. Il faut donc sécuriser la circulation de la donnée au sein d'un réseau d'expérience client. Cela peut être réalisé grâce à une « API de gestion du consentement » et une traçabilité stricte des autorisations et des usages.

« RGPD - Serez-vous privé de données privées ? » s'est interrogé Jean Claude Bellando, Director, Product Solution Marketing, MFT, Axway

L'intervention d'Etienne Papin, avocat associé au Cabinet Feral-Schuhl / Sainte-Marie, s'est logiquement inscrite dans la suite de la précédente. Il a ainsi réalisé un focus sur les principales problématiques juridiques posées par un texte, issu d'un vaste compromis, qui est tout sauf simple. Même si une réelle et totale conformité à la Loi de 1978 entraîne une quasi-conformité au RGPD.

Etienne Papin, avocat associé au Cabinet Feral-Schuhl / Sainte-Marie, a présenté les nouvelles règles sur les données.

Eviter les copies multiples des données

Mais le patrimoine de données est, en réalité, rarement maîtrisé. « 80 % des volumes de données gérés sont hors production » a ainsi asséné Alain Marbach, Président de Elée. Ces données sont en fait des copies des données de production pour de multiples usages connexes : développement, test, décisionnel, etc. Le RGPD peut servir de prétexte à une reprise en main de ce patrimoine. A la question « où sont les données ? », Alain Marbach a proposé de répondre au travers d'une interface unique de contrôle et un stockage en un exemplaire unique, seules des « copies virtuelles » étant réalisées avec mentions des modifications opérées par tel ou tel dans le seul

exemplaire destiné à cet Untel.

Alain Marbach, Président de Elée, a stipulé : « Protégez vos données hors production »

Des données en échange d'un meilleur service

Malgré tout, l'usage de données personnelles peut bien avoir un but positif. « On oublie un aspect important : le point de vue du client qui veut des offres personnalisées en échange de ses données » a ainsi relevé Jérémy Dallois, CEO de ReachFive. Maisles données confiées par les clients sont mal exploitées et le client n'en a pas pour le prix qu'il accepte de payer en empiètement sur sa vie privée : la connaissance client par les entreprises est médiocre car silotée. Pour Jérémy Dallois, « autant pour exploiter les datas que pour la conformité GDPR, il faut casser les silos. »

« Baromètre connaissance client : unification des identités, entre ambitions et réalité » a été présenté par Jérémy Dallois, CEO de ReachFive.

Antoine Meissonnier, Conservateur du patrimoine au Ministère de la Justice, et Thierry Milhé, VP International Production of IT Services chez Safran, ont ensuite témoigné de leurs expériences sur la première table ronde, « Comment abriter le patrimoine de données ? ».

La première table ronde, « Comment abriter le patrimoine de données ? », a réuni Antoine Meissonnier, Conservateur du patrimoine au Ministère de la Justice, et Thierry Milhé, VP International Production of IT Services chez Safran

Le GDPR, un bon prétexte

Sur un chantier d'exploitation de la data, Christine Brocard (Directeur Conseil Réglementaire banques finances chez CGI France) a déploré : « la difficulté est la multiplication des interlocuteurs ». Le GDPR, avec ses sanctions qui font peur, peut donc être une opportunité pour lancer des chantiers de maîtrise et d'exploitation de la données avec des projets de Data Driven Business, de Client Centric voire même de modernisation du SI. Pour Eric Hubert (Consultant Customer Information Management chez Pitney Bowes), le premier bénéfice du GDPR est précisément cette maîtrise de la data, avec une harmonisation de la vision sur les données et une reconnaissance des données stockées.

Christine Brocard (Directeur Conseil Réglementaire banques finances chez CGI France) et Eric Hubert (Consultant Customer Information Management chez Pitney Bowes) ont expliqué comment le GDPR était un levier pour une approche centrée sur le client

La peur du gendarme pour accroître la sagesse

« Les risques d'une non-maîtrise des données sont clairs, avec 4 % du CA en amende mais aussi -surtout, même- une atteinte à l'image de l'entreprise » a insisté Julie Charrier, Business Value Assessment Manager chez Information Builders. Cette peur du gendarme peut permettre de remettre à plat la gouvernance du patrimoine de

Etienne Papin : « GDPR a oublié la réalité technique des services cloud »

Maître Papin, avocat-associé au cabinet Feral-Schuhl / Sainte-Marie ouvre la conférence (photo Bruno Levy).

CIO a organisé une Matinée Stratégique, « Data, de la protection au GDPR », le 17 octobre 2017, avec, en ouverture, l'analyse de Maître Etienne Papin, avocat associé au cabinet Feral-Schuhl / Sainte-Marie.

« *Les nouvelles règles sur les données* », c'était le titre de l'intervention d'Etienne Papin, mardi 17 octobre, lors de la conférence CIO. Un thème large, traité parfois avec humour, pour une assistance de DSI et de responsables IT en pleine intégration de GDPR dans leurs systèmes d'information et dans leur organisation. Une intervention destinée à donner des clés de compréhension et un premier retour d'expérience réalisé par le cabinet.

« *Ce GDPR aura peut être au moins une vertu, nous rappeler qu'il y a une règlementation qui s'applique en matière de protection des données. Beaucoup de choses se disent, mais on a une loi relative à la protection des données personnelles depuis 1978, quand même, ça commence à dater. Donc, si vous êtes en conformité avec la loi de 1978, en forçant un peu le trait, vous l'êtes avec GDPR. Le problème c'est que personne n'est en conformité avec la loi de 1978. On a 40 ans de retar*d », note d'entrée Maître Papin.

« *GDPR, ce Règlement pris le 27 avril 2016, c'est une horreur pour un juriste, avec 173 considérants et 99 articles. Il n'y avait pas de raison de faire aussi compliqué, on aurait pu faire plus souple. Pour vous donner une clé de comparaison, la règle sur les relations entre distributeurs, c'est important, fait 10 articles, 10 considérants en une dizaine de pages* ».

« On tombe dans un abime de perplexité »

On trouve plein de choses dans ce règlement, par exemple, l'article 11.2. Etienne Papin ne résiste pas au plaisir de lire un extrait : « *Lorsque le responsable du traitement n'est pas à même d'identifier la personne concernée », (déjà, on tombe dans un abime de perplexité) « il en informe la personne concernée si c'est possible ». Donc, c'est pas possible puisqu'on n'a pas pu l'identifier. Ça vous donne une idée de la complexité de la mise en conformité ».*

Au-delà de cette boutade, beaucoup d'éléments nécessitent de prendre le sujet à bras le corps. Ce Règlement laisse au droit national la possibilité de prendre des mesures pour réformer la loi de 1978, et d'intégrer ses dispositions. Normalement, pas besoin de transposition, avec un Règlement européen, pas besoin d'une loi nationale de transposition. Malheureusement, ce Règlement prévoit des transpositions (voir Encadré).

Si ces lois en France ont peu d'équivalent, le DPO malgré ce Règlement va devoir se « coltiner » des lois nationales liées à la protection des données personnelles. Au niveau communautaire aussi, on attend des actes d'application du Règlement, ils renvoient à la notion de code de conduite ou de délivrance de certifications. Le Règlement est complexe et, pour aider les entreprises à l'appliquer, on a mis en place des processus de certification, pour démontrer votre capacité à appliquer ce Règlement. Mécanismes de certification et codes de conduite vont être adoptés, faut se tenir à l'écoute, ce seront des outils intéressants pour montrer sa conformité à GDPR.

Pas de changements trop forts non plus

Heureusement, les grands principes que nous avons l'habitude de manier depuis 1978, on les retrouve presque textuellement dans le GDPR, détaille Maître Papin. Pas de nouveauté. Des raffinements, des complications, mais pas de changements trop forts non plus : les définitions n'ont pas évolué. Qu'est-ce que le traitement, par exemple ? Il n'y a pas de changement, « *mais on aurait pourtant aimé le voir évoluer* » !

Plusieurs points méritent de l'attention. Le principe du consentement des intéressés au traitement de leurs données personnelles, par exemple, avec le renforcement des informations à délivrer. Comme pour la loi de 1978, les données doivent être traitées pour des données licites, pas plus que vous n'en avez besoin pour le traitement à réaliser. Comme le stockage n'est ni un problème, ni un coût, la démarche inverse fonctionne pour GDPR. Les droits des personnes ? Ceux d'avant sont toujours là et le GDPR consacre des droits nouveaux, comme la portabilité des données.

« *La durée de conservation est le sujet n°1 pour les entreprises et les organisations, nous le voyons quand nous faisons des audits, les entreprises stockent tout et ne suppriment jamais rien. 1er point : il faut définir des durées de conservations, c'est absolument nécessaire. Pour la sécurité des données, toujours présente, il faut la garantir, mais le problème juridique est d'assurer les transferts à étranger, le législateur européen raisonne de la même façon qu'avant.* »

La question des services cloud

« *Quand on lit le GDPR, on est étonné que le législateur ait refusé de prendre en compte la réalité technique, notamment celle des services de cloud, SaaS et IaaS. Le*

GDPR raisonne comme si vous identifiiez l'endroit où les données sont stockées à l'étranger, mais pour envoyer des données dans un pays en dehors de l'Union Européenne, il faut un contrat spécifique de transfert de données, pour réaliser cette opération de manière licite. Même avec le GDPR, alors que les solutions existent pour la localisation des données, cette disposition n'est plus pertinente, informatiquement parlant. Malheureusement cette réalité technique n'est pas prise en compte, vous devez toujours réfléchir comme si les datacenters étaient tous en Europe ».

GDPR repose aussi sur le mythe que le responsable du traitement est tout puissant et doit pouvoir de manière contractuelle engager les sous-traitants, sur ce que le sous-traitant doit faire en matière de gestion des données personnelles. Et le responsable de traitement doit pouvoir auditer son sous-traitant à tout moment. Dans toutes les solutions cloud ce n'est pas l'utilisateur mais le fournisseur qui fait la loi et qui fait l'audit. Quand on va imposer à Microsoft ou d'autres d'auditer ses datacenters, ce sera un peu en décalage avec ce que le GDPR demande.

GDPR présente toutefois des nouveautés. C'est d'abord la notion d'accountability, tellement étrangère au droit français qu'on a du mal à la traduire. Les aspects déclaratifs sont supprimés et on entre dans autre logique, l'entreprise doit démontrer qu'elle a mis en place des processus et des contrôles pour respecter les règles du GDPR, donc mettre en place des règles internes pour montrer le respect du Règlement. Toutes les entreprises doivent entrer dans cette logique de préservation de preuve en interne, donc on doit toujours documenter ce qu'on en fait.

Le délai de 72 heures

Autre point important, le privacy by design pour les responsables métiers. Une entreprise ne peut plus se doter d'un nouvel applicatif sans demander combien de données personnelles sont traitées, accessibles, ou transmises à l'étranger, donc il faut un pré-requis pour présider au choix de tout nouvel applicatif et ne plus le mettre sous le tapis. Avant, on pouvait tout stocker, maintenant la loi bloque. Ce n'est pas pour tous les traitements mais pour ceux dont vous identifiez s'ils ont un risque important pour les libertés des personnes, avant avec la CNIL de faire une analyse d'impact. Il faut aussi notifier la violation de données personnelles dans un délai de 72 heures.

Autre question, faut-il nommer un DPO ? Pas forcément, mais un sponsor est indispensable, si personne n'est identifié ou ne dispose des pouvoirs nécessaires, vous n'allez pas vous en sortir. Il faut mettre en place un centre de traitement de données, dans les PME c'est faisable, dans les grandes entreprises, il faut se doter d'outils spécifiques, pas seulement d'un tableau Excel.

En ce moment, GDPR impose une grande renégociation des documents contractuels, « *je pense aux hébergeurs et aux personnes qui fournissent des solutions en SaaS* ». Le Règlement impose de classer dans ces documents, notamment le sous-traitant ne peut recruter un autre sous-traitant sans l'accord du client. « *C'est un peu kafkaïen et ridicule. Il faut s'y pencher, c'est l'une des premières étapes de la mise en conformité* ».

Pour conclure, qu'est-ce qu'on fait aujourd'hui, qu'est-ce qu'on fera après, cette conformité ? Il faut plusieurs choses : désigner le sponsor interne, dresser la cartographie des traitements, prioriser les actions de mises à jour, mettre à plat les rapports avec les sous-traitants, définir les prérequis « privacy by design », définir les processus internes pour : la gestion de la confidentialité, la gestion des droits des

personnes concernées, la gestion des violations de données, enfin, tenir à jour le registre.

Les actes d'application au niveau national

Des actes d'application au niveau national restent à définir pour compléter le GDPR :
- pour les données biométrique, génétique et les données de santé
- pour consultation préalable des autorités de contrôle pour les traitements qui relève d'une mission de service public
- pour les pouvoirs des autorités de contrôle
- pour le régime des sanctions autre que les amendes administratives
- pour la conciliation avec la liberté d'expression et la liberté d'information sur le NIR
- sur les données traitées dans le cadre des relations de travail
- sur les personnes soumises à des obligations de secret
- sur le traitement des données de mineurs

(***source : Etienne Papin, 17 octobre 2017, conférence CIO***)

En savoir plus :
- Etude Comment bien gérer ses données à l'heure du GDPR ?.
- Télécharger les contenus associés à la conférence *Data : de la protection au GDPR* (mises à jour régulières).

Didier Barathon
Journaliste

Numériser ses documents au Ministère de la justice et chez Safran

Antoine Meissonnier, à gauche, Ministère de la Justice et Thierry Milhé, Safran (photo Bruno Levy).

Lors de la Matinée Stratégique, « Data, de la protection au GDPR », le 17 octobre, CIO donnait la parole au Ministère de la justice et à Safran, lors d'une première table ronde consacrée au patrimoine de données.

Antoine Meissonnier, chef du département des archives, de la documentation et du patrimoine, au Ministère de la Justice et Thierry Milhé, vice-président International production of IT Services, chez Safran, composaient la première table ronde de la Matinée Stratégique du 17 octobre organisée par CIO. Une Matinée consacrée au thème « Data, de la protection au GDPR ».

Conservateur du patrimoine, Antoine Meissonnier est à ce titre membre d'un corps très particulier de la fonction publique, chargé de la conservation en général, et plus particulièrement le concernant des archives, donc des écrits. Son sujet principal porte le doux nom de NF Z42-026, une norme sur la numérisation fidèle des documents papier qu'il a contribué à construire. L'objet de cette norme est, quand on a un patrimoine papier, de le transformer en un patrimoine dématérialisé, mais avec la même valeur.

Les bonnes pratiques d'une numérisation dite « fidèle » consistent en quoi ? Elles permettent d'avoir une base unifiée pour construire un seul canal, un seul endroit, sous une forme agile et numérique, c'est donc une organisation fidèle des documents du patrimoine informationnel. C'est assez simple, la plupart des organisations en font un enjeu, car l'objectif à terme c'est de détruire le papier, donc l'enjeu est la valeur probante du document. La qualification est celle de copie fiable, on doit pouvoir le

t d'application volontaire, il faut garder une souplesse dans l'application

des textes pour avoir la conformité du décret et pouvoir sans risque détruire le papier".

Il faut avoir des contrôles

Le prestation de numérisation peut être le fait d'une chaîne de numérisation ou d'un tiers ou une prestation décentralisée. Au guichet d'un hôpital, par exemple, les secrétaires médicales vont numériser puis stocker. Tous ces cas sont pris en compte par la norme, des réglages techniques sont nécessaires, donc on fait des tests pour bien réaliser et prendre des outils de numérisation puis passer à la qualification de la chaîne avec un flux d'information donnée.

Ensuite, l'information est testée et documentée, « *vous faites un lot de documents de textes et ensuite vous lancez la production et toutes les chaines de traçabilité de la production, traitement centralisé ou décentralisé. Le but est de savoir ce qui rentre et ce qui sort. Il faut avoir des contrôles, soit procéder par échantillonnage, soit par exhaustivité* ».

Enfin, il convient de délivrer, contrôler les traitements sur les chaînes de scanner, vérifier, pas de faiblesse sur la suppression des pages blanches, par exemple, j'ai des alertes il faut contrôler soi-même plutôt que de supprimer des pages blanches. Pour prouver sa fiabilité, on prend un risque si la numérotation ne suit pas, le risque est quand même de se retrouver devant le juge.

Le sujet est aussi celui de la conservation, de garder une trace d'intégrité, contrôler ensuite facilement que la cote numérique ne soit pas modifiable dans le temps. L'aspect conservation vient ensuite, c'est l'enjeu le plus complet, en étant capable de démontrer son intégrité et son authenticité. Donc des normes et des process très précis.

Dans un contexte de société internationale

Concernant Thierry Milhé, sa préoccupation est celle du responsable d'une entreprise très sensible, Safran, qui dispose de tout un corpus de règles venues des autorités de l'aviation française, européenne et américaine créant dès le début une organisation et un casse-tête pour répondre aux règles. La mise en oeuvre un système de stockage pour répondre aux contraintes, préserver le patrimoine data et le conserver. Le tout dans un contexte d'une société internationale.

Safran est soumis aux réglementations ITA (Institut du transport aérien) particulièrement pour le transport et l'accès aux Etats-Unis, ils ont localisé des SI dédiés avec les américains, les canadiens et les anglo saxons en général qui ont répliqué ce système. Depuis 12 mois, la localisation physique est moins importante, le chiffrement fait qu'on a plus du tout de dépendance. Thierry Milhé discute avec l'ANSSI et au niveau franco-français pour mettre en place ce système-là : on a ainsi une maîtrise de l'accès chiffré suffisamment puissante pour préserver le patrimoine des données, quel que soit l'endroit du stockage.

95% des données sont sans garantie

On conserve les données en observant comment elles sont utilisées. Une architecture à la fois agile et sécurisée. Il y a 2 ans, Safran a défini une politique orientée cloud avec une organisation pour structurer les données avec plusieurs niveaux de criticité pour

coller aux destinations voulues, 95% des données sont aujourd'hui sans garantie, pas accédées, pas manipulées, pas transformées. Safran est un groupe industriel, donc il a beaucoup de données techniques, mais les données personnelles sont celles qu'on retrouve partout. Dans les processus mis en place, il faut toujours faire attention aux données. Pour avoir des avancées significatives, Safran a travaillé avec beaucoup de partenaires qui apportent des solutions en SaaS et a ainsi bénéficié d'un certain savoir-faire. Ces entreprises ont traité le périmètre.

Pour les données techniques, c'est un autre problème. Si un procès a lieu aux Etats-Unis, on a besoin de connaître les niveaux de décision. Il faut tenir compte des données devant être archivées plus de dix ans. Et il faut savoir quelle règle appliquer, européenne ou américaine.

Pour Antoine Meissonnier, les mails sont toujours un vrai problème, un sujet de conformité pour les conserver. « *Mais ce n'est pas ce qui me stresse le plus, car ce sont les données pas structurées ou découpées, celles que l'on a du mal à les conserver* ». Il reste un message mail avec un code précis et des méta données, tout le problème vient des pièces jointes. « *Conserver des données mail ne m'inquiète pas, les bases de données production m'inquiètent plus* ». On est au Ministère au niveau de la macro évaluation : les collaborateurs les plus importants vont voir leurs mails conservés.

En savoir plus

- Etude Comment bien gérer ses données à l'heure du GDPR ?.
- Télécharger les contenus associés à la conférence *Data : de la protection au GDPR* (mises à jour régulières).

Didier Barathon
Journaliste

Pascal Courthial (Humanis) : « la première chose que nous avons faite est de sortir les informaticiens de leur tour d'ivoire »

Pascal Courthial, DSI du groupe mutualiste de protection sociale Humanis, a été le Grand Témoin de la Matinée Stratégique « Data : de la protection au GDPR »

Lors de la Matinée Stratégique CIO « Data : de la protection au GDPR » du 17 octobre 2017, Pascal Courthial, DSI du groupe mutualiste de protection sociale Humanis, a été Grand Témoin.

Dix millions de personnes issues de 700 000 entreprises clientes sont protégées par le groupe mutualiste de protection sociale Humanis agissant dans le périmètre de la prévoyance, de l'action sociale mais aussi de la retraite AGIRC-ARRCO. Le DSI de cet organisme, Pascal Courthial, était le Grand Témoin de la Matinée Stratégique CIO « Data : de la protection au GDPR » du 17 octobre 2017. En effet, Humanis traite des données d'une grande sensibilité tout en mettant en oeuvre un important programme de gestion de la Data.

« Pendant très longtemps, chacun d'entre nous a largement remis ses données, notamment aux réseaux sociaux, et nous commençons à comprendre que nous avons des droits sur celles-ci » a relevé Pascal Courthial. Au niveau d'Humanis, sont gérées des données contractuelles, remises par les entreprises clientes, mais aussi toutes les données concernant la vie professionnelle et ses aléas pour chaque salarié protégé. Les données sont conservées très longtemps. Pascal Courthial a observé : « la réglementation est schizophrénique, d'un côté Solvency 2 nous oblige à maîtriser les risques financier en justifiant les analyses en se basant sur le passé, de l'autre le RGPD nous impose des dispositions antérieures. »

Résoudre la schizophrénie juridique et mettre en forme les données

Résoudre la crise schizophrénique n'est pas la seule difficulté rencontrée par le DSI. Le RGPD oblige à communiquer à quelqu'un, sur simple demande, toutes les informations relatives à cette personne en la possession de l'entreprise. Mais Pascal Courthial a pointé : « cette remise de données ne doit pas être une simple extraction de base SQL mais doit se faire sous une forme compréhensible, donc remises en forme ».
Ces données sensibles doivent être protégées, sécurisées et malgré tout exploitées pour remplir les différents objectifs de l'organisme. Le groupe Humanis commence ainsi à mettre en place Atlas, un programme Big Data prévu pour durer cinq ans et coûter 20 millions d'euros. « Ce n'est pas un projet informatique mais un projet d'entreprise associant la direction des risques, la direction marketing et la DSI » a précisé Pascal Courthial. L'ambition d'Atlas est bien de doter Humanis d'un SI totalement centré sur la donnée.

La data doit être gérée

Mais Pascal Courthial a observé : « aujourd'hui, les applications ne gèrent pas la data, elles l'utilisent. Les bases de données les gèrent sur un plan technique mais aucune application, par exemple, n'impose de règles de gestions sur les données. » Le programme Atlas implique donc de déverser les données dans un système intermédiaire sur lequel vont être posées des règles de gestion, de traçabilité, de qualité, d'auditabilité... La qualité, en particulier, est un pré-requis à toute analyse. « Beaucoup de data-scientists passent en fait leur temps à traiter la qualité des données » a déploré Pascal Courthial. L'importance de la qualité de la donnée n'est malheureusement pas encore comprise par tous et « il faut faire preuve de beaucoup de pédagogie » comme a expliqué le DSI.
Chacun doit se sentir responsable des données qu'il manipule. Bien saisir un SIRET, cela prend du temps à quelqu'un qui créé un dossier d'entreprise sans qu'il soit bien conscient de l'importance de cette saisie. Pourtant, c'est essentiel. Chaque collaborateur ne voit que la donnée dont lui-même a besoin et cherche à gagner du temps, d'autant qu'il est souvent jugé sur sa capacité à traiter rapidement des dossiers. Encore une fois, les entreprises sont schizophrènes car les interfaces de saisie ont été rendues permissives pour éviter les blocages, même justifiés ! Résultat : les SI sont truffés de données fausses, incomplètes ou dupliquées dans diverses versions ou sous divers noms. Pascal Courthial plaide ainsi régulièrement : « si vous voulez des données justes dans les tableaux que vous produisez, il vous faut des données justes en entrée. »

Des systèmes bancals

Pendant des années, des systèmes bancals ont donc été tolérés. Et on essaye de créer de nouveaux systèmes à partir de ces anciens systèmes. « Certaines données étaient signifiantes dans l'ancien système mais ne le sont plus comme d'autres sont signifiantes aujourd'hui mais ne l'étaient pas hier » a regretté Pascal Courthial. Les incidents sont donc courants. Par exemple, un ancien système, chez Humanis, a été migré il y a quatre ans. Et, dans celui-ci, les taux de remboursement étaient en zone commentaires... La migration d'une zone commentaires n'est pas censée normalement retraiter ce genre de données signifiantes ! De tels errements ne sont évidemment plus acceptables aujourd'hui mais, de toute évidence, il faudra du temps pour régler ce genre de problèmes. Pascal Courthial a insisté : « cela implique un engagement de

tous et de chacun ! »
Et ce n'est pas tout. En effet, les habilitations des accès aux données sont gérées à partir des annuaires de collaborateurs, par exemple sous Active Directory. Mais il n'est pas rare qu'il y en ait plusieurs. Donc avec de potentielles incohérences. Et il est impossible de demander à chaque collaborateur de s'identifier en permanence pour accéder à chaque application : la productivité s'écroulerait dans l'entreprise. « La vision des problèmes doit être à 360°, en intégrant la dimension juridique, la dimension financière, la dimension client, la dimension données... » a rappelé Pascal Courthial qui en a déduit que la sensibilisation doit être totale pour chacun.

Gérer le changement

Mais responsabiliser, cela implique aussi de tenir compte des obligations de productivité des commerciaux, des opérateurs de centres d'appels, etc. Pascal Courthial a expliqué : « la première chose que nous avons faite est de sortir les informaticiens de leur tour d'ivoire et de les envoyer sur le terrain, de les confronter aux métiers. Ceux qui font le SI doivent avoir la disposition d'écouter ceux qui vont l'utiliser. » Il s'agissait d'aller au delà de l'habituel cycle long avec cahier des charges, validation des cahiers des charges, etc. au point que l'application était parfois obsolète avant même d'être développée. Humanis a donc mis en place DevOps pour s'adapter au cycle du métier. Le digital implique des cycles courts. Dès lors qu'il y a des préoccupations réglementaires sur de gros systèmes, la démarche doit être plus lente et plus structurée. Et même si Humanis développe son propre SI, il doit veiller à se sourcer aussi à l'extérieur, via des prestataires divers, pour rester au meilleur niveau de l'état de l'art. Un bon chef de projet doit donc, avant tout, « créer du lien » pour assembler toutes les compétences IT comme métier pour mener à bien tout ce qui doit être fait.

En savoir plus

- Etude Comment bien gérer ses données à l'heure du GDPR ?.
- Télécharger les contenus associés à la conférence *Data : de la protection au GDPR* (mises à jour régulières).

Bertrand Lemaire
Rédacteur en chef de CIO

S'organiser pour respecter les règles sur les données personnelles

David Ruiz, juriste au sein de la Direction de la Conformité de la CNIL, et Anne-Sophie Nibert, Group Data Privacy Officer de Total, ont témoigné lors de la Matinée Stratégique « Data : de la protection au GDPR »

Lors de la Matinée Stratégique CIO « Data : de la protection au GDPR » du 17 octobre 2017, la deuxième table ronde sur le thème « Comment respecter les règles sur les données en développant leurs usages ? » a réuni David Ruiz, juriste au sein de la Direction de la Conformité de la CNIL, et Anne-Sophie Nibert, Group Data Privacy Officer de Total.

« Comment respecter les règles sur les données en développant leurs usages ? » Cette vaste question a été l'objet de la seconde table ronde de la Matinée Stratégique « Data : de la protection au GDPR » organisée par CIO le 17 octobre 2017 à Paris. Elle réunissait David Ruiz, juriste au sein de la Direction de la Conformité de la CNIL (Commission Nationale Informatique et Liberté), et Anne-Sophie Nibert, Group Data Privacy Officer de Total. Ainsi, la « théorie » juridique a été confrontée à la « pratique » en entreprise.

Créée en 1978, la CNIL est la première autorité administrative indépendante instituée en France. Elle a pour mission de garantir les droits des personnes en matière de données personnelles mais aussi d'accompagner les entreprises pour les amener à la conformité en la matière. En cas de manquements, la CNIL, qui pratique des contrôles, a aussi une mission de sanction. La Direction de la Conformité, à laquelle appartient David Ruiz, a d'ailleurs comme mission d'accompagner les structures et de répondre à leurs questions, à l'initiation des traitements ou au cours de la vie de ceux-ci.

Aucun bouleversement avec le RGPD

« Je suis conforté dans mon analyse de la situation, à savoir que le RGPD amène les se mettre en conformité avec des principes qui sont réaffirmés et

renforcés depuis 1978 » a soupiré David Ruiz. Le RGPD (ou GDPR en Anglais, le Règlement général européen de protection des données) n'amène aucun bouleversement fondamental. Mais, comme il s'agit d'un texte de compromis, effectivement, il est assez complexe et renvoie souvent à d'autres textes, y compris nationaux. La Loi Informatique et Libertés ne va donc pas disparaître mais être rénovée.
David Ruiz a mentionné : « la loi va être rénovée sur deux volets : l'intégration des données spécifiques nationales au cadre européen (droit de la santé, droit du travail...), avec maintien possible de mesures préalables, et au contraire la suppression de toutes les redondances entre le droit national et le droit européen. » La directive de 1995 pouvait connaître des applications différentes selon les pays européens, mais, avec un règlement général, les mêmes dispositions vont bien s'appliquer partout. Mais ces dispositions ne couvrent pas tout le périmètre.

Une conformité dynamique en continu

Comme, de toute évidence, les entreprises ne sont pas prêtes et ne seront pas prêtes en mai 2018, comment peut réagir la CNIL ? « Accompagner les entreprise est le rôle de la Direction de la Conformité et nous avons déjà publier des guides, notamment une méthode en six étapes pour aider à être en conformité en suivant un fil conducteur » a relevé David Ruiz.
Une étape particulièrement importante, selon David Ruiz, est « documenter la conformité ». Ce point est lié au principal changement amené par le RGPD. Avec ce mécanisme, la mise en conformité doit être continue et dynamique, au fil des évolutions du système d'information. Il s'agit, à tout moment, d'être en mesure de décrire tous les traitements et tous les impacts de ceux-ci sur les personnes qui en sont les objets. Dès lors qu'un traitement est susceptible d'entraîner un risque, l'étude d'impact est strictement obligatoire. Le RGPD donne un certain nombre de critères pour définir les traitements à risque : données sensibles (biométrie, condamnations...) par exemple. Cette étude doit inclure les mesures prises pour combattre ces risques. La CNIL publie d'ailleurs des documents pour montrer comment réaliser de tels documents.

Un long programme délicat et complexe

Anne-Sophie Nibert, Group Data Privacy Officer de Total, s'occupe de ces questions au sein du groupe Total mais sans, cependant, être réellement CIL (Correspondant Informatique et Liberté) ou DPO (Data Privacy Officer), bien qu'elle soit membre de l'AFCDP (Association française des correspondants à la protection des données personnelles). Total est quatrième groupe pétrolier et gazier dans le monde, avec des activités croissantes dans l'énergie renouvelable ou dans la distribution d'électricité. Le groupe compte 98000 collaborateurs dans 130 pays et réalise un chiffre d'affaires consolidé de 150 milliards de dollars. Et 98 000 collaborateurs ont nécessairement beaucoup de données personnelles...
« Comme on l'a dit, la protection de ces données n'a rien de nouveau et le groupe Total a mis en oeuvre des règles groupe en 1992 » a relevé Anne-Sophie Nibert. Ces règles ont abouti à la construction d'un programme de mise en conformité à ces règles. Exercice long, compliqué et délicat mais évidemment indispensable. Tout n'est pas terminé en 2017 alors que viennent s'ajouter les règles issues du GDPR. Anne-Sophie Nibert a constaté : « c'est un travail itératif et continu. » Les inventaires sont réalisés régulièrement par voie de questionnaires dans les différents services.

Tous responsables mais pas tous porteurs du sujet

La mise en conformité, a-t-elle confirmé, est la responsabilité de tout le monde. Au sein du groupe Total, c'est la direction juridique qui porte le sujet mais en s'associant à la DSI et aux directions de la gouvernance. Ainsi se construit petit à petit le concept non seulement de gouvernance des informations mais aussi celui de gouvernance des données. D'autant plus que le groupe, comme tout le monde, s'est lancé dans un vaste programme de digitalisation. « Il faut faire preuve de pédagogie et nous avons étudié durant des mois les impacts du GDPR sur nos différents métiers » s'est souvenue Anne-Sophie Nibert.
Si le GDPR est une contrainte compliquée, il peut aussi être une opportunité dans l'organisation de la donnée. Surtout, il fallait prouver que la stratégie digitale ne serait pas freinée par cette mise en conformité. Et une stratégie devait être mise en oeuvre. Ainsi, même si elle est membre de l'AFCDP, Anne-Sophie Nibert est ni CIL ni DPO, « deux fonctions définies par la réglementation ». Peut-être, demain, y aura-t-il un DPO chez Total mais, pour l'heure, il n'y a pas de CIL. Cela n'empêche pas d'avoir un important programme de mise en conformité. « Les responsabilités précises du CIL telles que définies par la réglementation ne semblaient pas faciliter les choses dans un groupe mondial comme le nôtre » a justifié Anne-Sophie Nibert.

DPO first or not ?

Faut-il commencer par nommer un DPO ? C'est ce que préconise la CNIL. Mais, chez Total, la logique a été de d'abord définir la gouvernance de la donnée avant de se préoccuper de nommer ou non un DPO. « Désigner un DPO ne vient pas nécessairement en premier temps mais la réglementation européenne prévoit des cas où c'est obligatoire » est intervenu David Ruiz. Du coup, selon lui, « si l'on n'a pas une vision claire de la situation, on ne va pas savoir si la désignation du DPO est ou non obligatoire dans le cas d'espèce de son entreprise ». Or, pour avoir cette vision claire, nommer le DPO est une bonne solution.
Mais mettre en place une gouvernance des données et réaliser toutes les tâches dévolues au DPO par une autre organisation ne pose pas de véritable problème. David Ruiz a ajouté : « et, à ce moment là, si la mise en place du DPO est obligatoire, on peut le nommer alors seulement. Ce DPO sera le chef d'orchestre de la conformité en lien avec l'organisation mise en place. »

En savoir plus

- Etude Comment bien gérer ses données à l'heure du GDPR ?.
- Télécharger les contenus associés à la conférence *Data : de la protection au GDPR* (mises à jour régulières).

Bertrand Lemaire
Rédacteur en chef de CIO

Pour toute demande concernant CIO.focus :
contact-cio@it-news-info.com

Une publication de IT NEWS INFO : 40 bd Henri Sellier 92150 Suresnes
Rédacteur en chef : Bertrand Lemaire, blemaire@it-news-info.com
Tél. : 01 41 97 62 10
Principaux associés : Adthink Media et International Data Group Inc.
Président : Bertrand Gros
Directeur de publication : Bertrand Gros
Directeur général : Jean Royné
Président du groupe Adthink Media : Sylvain Morel

CIO est édité par IT NEWS INFO, SAS au capital de 3000000 €
Siret : 500034574 00029 RCS Nanterre