



GDPR, LE GUIDE

Dossiers - Témoignages - Étude

ÉDITO

Dans près de neuf mois, le 25 mai 2018 pour être précis, le RGPD (règlement européen sur la protection des données personnelles ou GDPR en anglais) entrera en vigueur. Une échéance qui concerne plusieurs métiers dans les entreprises françaises : les informaticiens, les responsables de la sécurité mais également les juristes. Des changements sont attendus dans les entreprises pour former les salariés et mettre en conformité les pratiques. Mais si l'en en croit les récentes études – dont celle menée par Le Monde Informatique auprès de ses lecteurs – les entreprises françaises sont encore loin d'être prêtes à garantir la traçabilité des données où à nommer un DPO (Data Personal Officer). Elles craignent toutefois les sanctions financières (4% du son chiffre d'affaires et interdiction de traiter les données personnelles) qui pourront être imposées par l'autorité de contrôle – la Cnil – encore loin d'être capable de contrôler toutes les entreprises françaises. Il y aura bien un avant et un après GDPR.



Serge LEBLAL
Directeur des rédactions
IT NEWS INFO

Nous remercions les contributeurs qui ont participé à l'élaboration de ce document :

Alain Bensoussan, avocat à la cour, Chargé d'enseignement à l'École CentraleSupélec et à l'Institut d'études politiques de Paris

Polyanna Bigle, avocate à la cour, Directrice du département Sécurité numérique, Alain Bensoussan Avocats Lexing

Paul-Olivier Gibert, Président de l'AFCDP

Thierry Autret, Délégué Général du CESIN

Jean-Pierre Moreau, Président d'ADN Ouest

Stéphane Guidarini, Président du CIP PACA

Edouard Forzy, Président, La Mêlée

Ghislain Gagnoux, Président de Numica

Gérôme Billois, Directeur de la practice risk management et cybersécurité de Wavestone

SOMMAIRE

/ CABINET ALAIN BENSOUSSAN

Avant-propos..... 3

/ AFCDP ET CESIN

Les positions de l'AFCDP et du Cesin sur GDPR..... 5

Le CIL est mort, vive le DPO ! 5
GDPR : Evolution ou révolution ? 7

/ CLUBS DSI ET RSSI

GDPR en région : Les clubs DSI et RSSI témoignent 9

ADN Ouest : le RGPD dans l'ouest, entre attentisme et opportunités 9
CIP Méditerranée : Internet des objet et GDPR, un enjeu de taille en Provence 11
La Mêlée : GDPR, une aide pour structurer la transformation digitale 12
Numica s'empare de GDPR 12

/ POINT DE VUE DE LA RÉDACTION

GDPR, les enjeux : par les rédactions du Monde Informatique et CIO..... 13

LE POINT DE VUE DU MONDE INFORMATIQUE

GDPR, le compte à rebours est lancé 14
Le retard à l'allumage en France suscite des inquiétudes 16
Interview de Dominique Pourchet de Partner Magellan Consulting 18
Vers un recyclage d'outils déjà existants ? 20
Interview de Jean-Loup Guyot, directeur juridique d'ADLPerformance/ADLPartner 22

LA VISION DE WEBSTONE

GDPR : où en sont les grands comptes ? 24

LE POINT DE VUE DE CIO

GDPR : les Plans d'action tardent à se mettre en place 26

/ ÉTUDE

Résultats de l'Enquête Nationale GDPR 30

Avant-propos



Alain Bensoussan

Avocat à la cour, Chargé d'enseignement à l'École CentraleSupélec et à l'Institut d'études politiques de Paris, Alain Bensoussan Avocats Lexing



Polyanna Bigle

Avocate à la cour, Directrice du département Sécurité numérique, Alain Bensoussan Avocats Lexing

Protection des données à caractère personnel : en route vers mai 2018

Le choix du Monde Informatique et du groupe IT News Info de mettre en avant, dans le cadre de l'IT Tour 2017, la protection des données à caractère personnel comme clé de la performance IT des entreprises est un choix judicieux qui mérite d'être salué.

Alors qu'une réforme majeure s'annonce au plan européen à l'horizon 2018, réforme qui va impacter en profondeur l'environnement digital des entreprises, l'IT Tour offre l'opportunité aux entrepreneurs de tous horizons d'être sensibilisés à la question de la protection des données et au respect de la vie privée.

A l'heure de l'hyper-connexion et du Big Data, il s'agit assurément, pour l'entreprise, d'un facteur de transparence et de confiance vis-à-vis de son environnement avec lequel il faudra compter dans les prochains mois.

Rappelons en effet que le Règlement général sur la protection des données (« RGPD » ou « GDPR » en anglais), adopté le 27 avril 2016, sera directement applicable dans tous les Etats membres le 25 mai 2018. Il est urgent pour les entreprises d'anticiper ce nouveau texte qui va modifier en profondeur les règles applicables à leur environnement digital.

Le RGPD a pour objectif de moderniser le cadre européen de la protection des données personnelles afin de prendre en compte les avancées technologiques et de réduire, voire supprimer, les écarts juridiques entre les législations des Etats membres de l'Union européenne.

Il comporte près de 400 obligations dont le contenu est précisé dans 99 articles contextualisés dans près de 200 considérants.

Il s'agit d'un texte complexe et technique qui va imposer aux entreprises de plier à de nouvelles obligations, telles que :

- la réalisation d'analyses d'impact avant la mise en œuvre d'un traitement de données pouvant présenter des risques pour les droits et libertés des personnes ;
- la prise en compte de la protection de la sécurité des données, tant logique que physique, dès la conception du traitement de données concerné ;
- l'obligation d'être, à tout moment, en mesure de démontrer la conformité du traitement avec le RGPD.

La quasi-totalité des entreprises traitant des données personnelles de citoyens européens est donc concernée par le RGPD.

La mise en conformité avec le RGPD est un enjeu majeur : la Cnil, autorité de tutelle, pourrait être amenée à infliger des amendes pouvant atteindre 20 millions d'euros ou jusqu'à 4% du chiffre d'affaires mondial annuel.

Mais, on l'a vu, sa mise en application devrait aussi et surtout avoir un effet positif puisqu'il renforce les obligations de sécurité des entreprises, donnant ainsi à leurs clients l'assurance d'un niveau de protection accru pour le traitement de leurs données personnelles. Il permet ce faisant d'accroître également la confiance de ses partenaires et collaborateurs, et de renforcer sa position concurrentielle.

Le compte à rebours a bien commencé : il reste moins de 300 jours pour enclencher un véritable processus vertueux de mise en conformité. Et l'inscrire comme un véritable engagement sociétal au cœur de sa politique de RSE. ■

Alain Bensoussan

Avocat à la cour, Chargé d'enseignement à l'École CentraleSupélec et à l'Institut d'études politiques de Paris, Alain Bensoussan Avocats Lexing.

Polyanna Bigle

Avocate à la cour, Directrice du département Sécurité numérique, Alain Bensoussan Avocats Lexing



/ AFCDP ET CESIN

Les positions de l'AFCDP et du Cesin sur GDPR



Paul-Olivier Gibert,
Président de l'AFCDP

AFCDP : Le CIL est mort, vive le DPO !

Lorsque les premiers CIL ont été désignés auprès de la CNIL fin 2005, qui aurait pu prévoir l'importance qu'allait prendre ce nouveau métier, treize ans plus tard, à l'occasion de l'entrée en application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) qui nous fait entrer dans un nouveau paradigme ? Ce qui est certain, c'est qu'il est très vite apparu que cette formule de co-régulation, par la pratique, était la bonne pour espérer voir appliquées et respectées les règles d'or de la loi Informatique et Libertés au sein des organismes.

Le 25 mai 2018, la plupart des CIL seront confirmés dans leurs nouvelles responsabilités de Délégué à la protection des données et accompagneront leur responsable de traitement dans cette aventure qu'est le RGPD.

À l'heure où le CIL s'efface pour laisser la place à son successeur naturel, le Délégué à la protection des données (ou DPO, pour Data Protection Officer), il faut rendre hommage à ces précurseurs qui ont su inventer un nouveau métier, braver quelques fois l'indifférence ou le manque de soutien, mais qui ont maintenu le cap et réussi, avec abnégation et constance, à changer les mentalités, à faire évoluer les pratiques, à sensibiliser et convaincre. Aussi il convient de saluer tous les CIL pour ce qu'ils ont accompli et de souhaiter la bienvenue aux milliers de nouveaux professionnels qui vont, prochainement, découvrir ce métier passionnant sous une forme renouvelée, celle du Délégué à la protection des données

Mais qui seront les futurs DPO, et que seront leurs missions ?

L'association qui les représente, l'AFCDP (Association Française des Correspondants à la protection des Données Personnelles) espère ne pas voir la profession se réduire aux seuls profils juridiques, la pratique ayant démontré que, dans les pays qui ont opté pour le « Détaché

à la protection des données » dans le cadre de la directive 95/46/CE, l'hétérogénéité de l'origine des CIL était une véritable richesse (ainsi, en Allemagne aussi bien qu'en France, la majorité des CIL ont une formation initiale d'informaticien, et non de juristes). Pour l'AFCDP, la fonction de DPO doit rester ouverte à toute personne, quelle que soit sa formation initiale et son parcours, et l'exigence exprimée dans le RGPD peut être satisfaite même par des personnes dépourvues de diplôme en droit. Naturellement, cela implique un effort certain de formation initiale de la part des personnes qui se projettent dans le métier de Data Protection Officer, afin de compléter leurs connaissances. Sur son site Web, l'association liste les formations longues diplômantes qui préparent à ce métier.

Le maintien de l'hétérogénéité des profils permet aussi de répondre aux besoins des responsables de traitement qui doivent ces prochains mois trouver leur DPO. L'AFCDP, qui met à disposition le seul job board dédié à ce métier (www.afcdp.net/-Carrieres-et-Emplois-de-DPO-CIL), observe une tension certaine sur le marché du travail, due au déséquilibre croissant entre les offres de postes et les candidats. Une restriction aux seuls profils juridiques accentuerait cette tension. Pour aider les entreprises à désigner leur DPO, l'association met également à disposition un modèle de fiche de poste de DPO et un modèle de lettre de mission. L'AFCDP s'apprête également à dévoiler sa charte de déontologie du DPO, qu'elle compte promouvoir à l'échelle européenne.

L'AFCDP se réjouit de la nouvelle liberté laissée aux responsables de traitement de pouvoir désigner sans contrainte un DPO externe. Il faut rappeler que, sous l'empire de l'actuelle loi Informatique et Libertés, il est impossible de recourir à un CIL externe au-delà d'un seuil de 50 personnes qui sont chargées de la mise en œuvre ou qui ont directement accès aux traitements. Outre le fait que cette ouverture aura un effet marquant sur le marché du travail avec la création de nombreux postes de DPO externes, elle permet de choisir la meilleure approche. En effet, les formules de DPO externe et de DPO interne présentent chacune ses avantages et ses inconvénients. Le DPO interne est connu de tous, il connaît l'entreprise

sur le bout des doigts... et est mieux à même de découvrir l'existence d'un projet impliquant des données personnelles au détour d'une conversation anodine devant la machine à café. Le DPO externe, qui passe moins de temps dans les murs, n'a connaissance que de ce qui lui est présenté, à moins qu'il ne se lance dans des audits qui peuvent être ressentis comme intrusifs par le personnel. Par contre, il peut avoir plus de facilité que le DPO interne pour soulever les questions les plus délicates et pour formuler des constats sans fard.

Concernant leur indépendance, tout est question de personnalité. Certains CIL internes ont prouvé qu'il était possible de remplir leur mission sans avoir à faire de concessions et des CIL externes ont honoré leur contrat en n'hésitant pas exposer clairement les non-conformités. À l'inverse, qui peut dire que jamais un CIL interne n'a été tenté de détourner le regard ou de battre en retraite sous la pression d'une direction ? Qui peut assurer qu'un CIL externe n'a pas adapté son comportement à l'approche du renouvellement de son contrat ?

Pour les organismes qui découvrent le sujet, le mieux est sans doute de faire appel à un DPO externe afin de « nettoyer les écuries d'Augias » : selon la taille de la structure, il lui faudra 2 ou 3 ans pour découvrir « les cadavres dans les placards », procéder aux révisions les plus urgentes, changer drastiquement certaines habitudes, mettre en place les procédures indispensables. Une fois cette période critique passée, le chef d'entreprise peut alors désigner l'un de ses collaborateurs en tant que DPO interne, quitte à conserver une prestation de soutien auprès de l'ancien DPO externe. ■





Thierry Autret,
Délégué Général du
CESIN

CESIN : GDPR, Evolution ou révolution ?

Buzz Word des années 2016-2018 le RGPD ou GDPR n'est pourtant pas une surprise. De la loi française de 1976 en passant par la directive européenne de 1995 puis une adoption le 27 avril 2016, soit il y a déjà plus d'un an, les entreprises ne peuvent pas dire qu'elles n'ont pas eu le temps de se préparer.

Selon la maturité des entreprises, la mise en conformité au RGPD peut tenir de l'évolution ou de la révolution. Pour beaucoup d'entreprises, déjà sensibilisées à la loi de 1976, le changement porte sur le fait que la conformité en terme de déclaration à la CNIL n'est plus suffisante, encore faut-il démontrer que l'entreprise met en œuvre les moyens pour protéger ses données à caractère personnel. Ce qui était souvent loin d'être le cas. Un registre des traitements bien tenu à jour n'est plus un gage de conformité au GDPR. L'inventaire des traitements pourra être une quête sans fin lorsqu'on s'attaque aux données non structurées et en particulier celles contenues dans les environnements bureautiques. Un outillage sera pour le coup parfois nécessaire.

Pour celles qui ne respectaient déjà pas les exigences de la loi de 1976, et personne ne jettera la pierre aux PME PMI, auto-entreprises dont la force de travail ne permet pas de consacrer beaucoup de temps à ces questions en dehors de la production elle-même, la marche sera haute même si des moyens de mutualisation existent pour se doter d'un DPO. A l'inverse, une start-up ou entreprise en création qui va concevoir et construire son SI dans une approche "By Design", si possible déclinée en Privacy, Security, PCA by design, devrait pouvoir rapidement se mettre en conformité. Le cas le plus complexe reste celui des entreprises moyennes ayant des "legacy applications"

bâties sur des informatiques anciennes pour lesquelles la protection pourra être beaucoup plus dure à mettre en place.

Les données personnelles sont-elles plus sensibles qu'avant ? Non au sens premier du terme. Mais la différence entre 1976 et 2017 est qu'en 40 ans les données à caractère personnel ont pris de la valeur pour devenir un actif financier de l'entreprise, une valeur marchande qui s'achète et qui se revend, le plus souvent sans le consentement de son propriétaire.



Le projet de mise en œuvre de la conformité aux exigences du RGPD est un projet structurel d'entreprise. La prise de conscience collective doit se faire au plus haut niveau par le fait que le responsable de traitement est au bout du compte le dirigeant de la société et pas seulement le chef de projet. C'est bien aussi l'entreprise dans son unité juridique qui devra régler les pénalités en cas de poursuites judiciaires. C'est donc un projet structurant qui, au-delà de la mise en conformité, peut faire changer l'approche de la conception des applications dès la phase de marketing des nouveaux projets. Concevoir des applications "fun" sur smartphone dans lesquelles on demande des données personnelles peut avoir ses limites

induites par les contraintes du consentement et le fait de pouvoir vérifier a posteriori que ce consentement a bien été donné.

Quelle est la place du RSSI dans ce projet ? Le RGPD c'est la protection de l'information avant tout. Le rôle du RSSI est de protéger le SI quelle que soit la nature de l'information, à caractère personnel ou autre patrimoine informationnel de l'entreprise. Comme le souligne Édouard de Geffray, Secrétaire Général de la CNIL, le chef d'orchestre de la protection des données personnelles est le DPO (Data Privacy Officer) qui s'appuiera sans nul doute sur le RSSI mais également sur le responsable juridique, sur la DSI et, qu'ils le veuillent ou non, sur les métiers. Ceux-ci seront directement concernés par les études d'impact sur la vie privée (EIVP ou PIA Privacy Impact Analysis) des recueil et traitement des données à caractère personnel au regard du RGPD. Le savoir-faire du RSSI pour l'analyse des risques devrait être d'un grand secours pour le DPO. Ses connaissances en matière d'organisation de la sécurité et des technologies de protection et de prévention seront essentielles à la mise en œuvre des exigences du GDPR. Le DPO, le DSI

et, dans une moindre mesure le RSSI devront prévoir les modalités pour une éventuelle notification de violation de la sécurité des données à caractère personnel qui doit être faite dans certains cas sous 72h. Ceci ne s'improvise pas et doit donc être prévu à l'avance par des procédures organisationnelles et techniques, voire par la mise en place d'une cellule de crise.

Le DSI et/ou le RSSI vont devoir également recenser les traitements externalisés chez des tiers dont des clouds et en informer le DPO. Les juristes auront certainement un travail de mise à jour des contrats pour refléter les impacts du RGPD sur les sous-traitants et leur partage de responsabilités avec les donneurs d'ordres.

Le chemin vers la conformité reste long et complexe selon la situation où se trouve l'entreprise lorsqu'elle entame ce projet, et le 25 mai 2018 approche à grands pas. Une priorisation des actions semble nécessaire ainsi qu'une bonne répartition des rôles dans ce qui ne peut être qu'un projet d'entreprise où chacun doit prendre ses responsabilités. ■



/ CLUBS DSI ET RSSI

GDPR en région : Les clubs DSI et RSSI témoignent



Jean-Pierre Moreau
Président d'ADN Ouest

ADN Ouest : le RGPD dans l'ouest, entre attentisme et opportunités

Depuis le début de l'année 2017, les réseaux professionnels et la presse économique ont lancé des actions de sensibilisation au futur règlement sur la protection des données (RGPD). ADN'Ouest a déjà organisé plusieurs événements autour de ce sujet, notamment sous l'angle de la sécurité informatique et de la gestion des risques financiers. A la fin de l'été, de nombreuses entreprises veillent mais peu ont une vue limpide des chantiers qu'elles ont concrètement à mener. Insistant sur les sanctions potentielles et une lecture rigide des textes, des discours destinés à répandre la peur s'avèrent finalement contre-productifs. Parmi les membres d'ADN'Ouest, les avis divergent : certains estiment que le RGPD est simplement une évolution des pratiques déjà mises en œuvre pour respecter la Loi Informatique et

Libertés, d'autres perçoivent une véritable révolution qui impacte le cadre juridique, les outils techniques du SI et plus globalement l'organisation de leur entreprise.

Au sein des PME, les services rechignent à assumer le leadership et les responsabilités sur ce sujet épineux. La plupart des juristes d'entreprise, souvent spécialisés en droit social ou en droit des affaires, se tiennent à distance du sujet, maîtrisant peu le vocabulaire informatique et l'application de la Loi Informatique et Libertés. Les responsables informatiques, eux, deviennent l'ampleur des changements qu'une application stricte du RGPD nécessiterait... Cependant, habitués à lutter pour obtenir des moyens financiers et humains toujours insuffisants, certains abordent le RGPD non pas comme une contrainte mais comme une opportunité rare de sensibiliser et convaincre leurs dirigeants, qui souhaitent avant tout se prémunir des risques d'image ou financiers. Une constatation s'impose : moins la taille de la structure est importante, plus le rôle du responsable informatique est central pour porter la démarche RGPD. Dans les PME, si tout le monde fait l'autruche, c'est le responsable informatique qui va le mieux deviner les réels enjeux

pour demain et le lien avec la transformation digitale. Le plus souvent, dans les PME, c'est lui qui va s'autosaisir du chantier et réunir un groupe de travail pluridisciplinaire autour de lui.

Sur la ligne de départ, rares sont les organisations qui savent par où commencer. Les 6 étapes, proposées par la CNIL pour se préparer, restent théoriques ! Une PME débute généralement son projet RGPD par un état des lieux de sa conformité, en sollicitant un avis extérieur, qui va lister les chantiers à dérouler (juridique, technique et organisationnel). L'enjeu est de trouver le bon partenaire, capable d'adresser à la fois l'angle juridique et l'angle technique du sujet. Les usurpateurs qui s'improvisent sur ce sujet devenu à la mode sont légions : chaque juriste est devenu un expert du RGPD, chaque vendeur de solution en cybersécurité se présente en sauveur pour aider à la mise en conformité ! Il convient surtout de prendre de la hauteur avant de se lancer dans des investissements parfois inutiles. Au plus près du terrain, les demandes d'accès aux données, de rectification, même de suppression, par des personnes, restent rarissimes... Les entreprises qui traitent des données sensibles sont peu nombreuses. Il convient de ne pas se tromper de cible : les acteurs industriels peuvent rapidement atteindre la conformité requise. L'histoire peut nettement se complexifier pour les acteurs de l'assurance, les administrations, le monde de la santé, les centres de services BtoC ou les e-commerçants, ... Pour les éditeurs de logiciels, des défis particuliers sont à surmonter.

La CNIL doit encore publier des clarifications sur l'application de nombreux articles du RGPD, ce qui explique l'attentisme de certains, avant d'initier toute démarche concrète. Cependant, le futur règlement valorisera l'opportunité des précurseurs, dans un monde numérique qui favorise les écosystèmes basés sur la confiance. ■





Stéphane Guidarini
Président du CIP PACA

CIP Méditerranée : Internet des objets et GDPR, un enjeu de taille en Provence

GDPR concerne aussi les données collectées par les objets connectés. De fait comme un objet connecté est associé à son utilisateur, il est porteur de données personnelles, toutes les données générées et transmises à partir d'un objet connecté sont considérées par défaut comme des données personnelles.

La problématique des Objets connectés de la protection des données est apparue très tôt en Provence, car la filière IoT y est très fortement représentée.

Fort de 8 milliard de CA et de 44 000 experts du numérique, la Provence affiche comme filière de pointe l'IOT avec plus de 100 entreprises et 75 start up spécialisées dans le domaine.

La filière de l'IOT dans les Bouches du Rhône dispose d'une chaîne de valeur complète allant du support (Micro électronique) en passant par la sécurité des données, leurs hébergement, le contenu et les applicatifs notamment autour de la Smartcity.

La présence historique des grands donneurs d'ordre de la Microélectronique (Atmel, St Microelectronics, Gemalto...) a permis la création de deux organismes majeurs le pôle de compétitivité international SCS (Solutions communicantes sécurisées) et le CNRFID (Centre Nationale RFID).

Dès 2013, le CNRFID signe une convention avec la CNIL. Cette convention vise à renforcer les relations entre les deux organismes autour des questions de respect de la vie privée dans les applications RFID et autres protocoles de transfert de données sans contact. Depuis lors, le CNRFID travaille au côté de la CNIL en animant un groupe d'expert chargé de l'écriture de la future norme européenne.

Début 2017, le CNRFID lance IdO Privacy, un groupe de travail "Objets Connectés & protection des données personnelles" chargé de créer un référentiel et des guides de bonnes pratiques pour la protection des données personnelles des applications des objets connectés professionnels.

Depuis 2015, le CIPMed et ses partenaires ont organisé de nombreuses manifestations afin d'expliquer la nouvelle réglementation que ce soit auprès des entreprises toutes filières confondues, start up, décideurs, DSI. L'objectif étant de sensibiliser très tôt les acteurs à la mise en œuvre du GDPR, et en particulier les DSI.

Pour se faire, le CIPMed participe activement à la commission Smart City de la French Tech Aix Marseille, s'appuie sur les compétences de 2 cabinets d'avocats membres du CIPMed et sur un rapprochement avec le CNRFID.

Depuis début 2017, 5 ateliers CGRP ont été animés par le CIPMed, sous différents aspects (descriptif, mise en œuvre, sécurité...) , dans différents territoires (Sophia Antipolis, Aix Marseille, Avignon), auprès de différents public (DSI et prestataires), à différentes occasions (1 plénière, 3 déjeuners DSI, 1 dîner DSI).

D'ici la fin de l'année le CIPMed organisera une journée DSI sur le thème de l'IOT / Smartcity afin de découvrir l'ampleur de la filière en Provence avec – entre autre - la visite de projet emblématique comme The Camp (Premier campus européen consacré aux technologies émergentes et aux nouveaux usages de la smartcity sur 17 ha) et celle de ConnectWave 2 la plateforme d'essai et un espace de démonstration nationale du CNRFID. Au cours de cette journée, seront évoquées les problématiques du GDPR appliquée au transfert et à la collecte de données via les objets connectés. ■



Edouard Forzy
Président de La Mêlée

La Mêlée : GDPR, une aide pour structurer la transformation digitale

Les dirigeants de certaines entreprises en Occitanie n'ont pas identifié l'évolution réglementaire comme un risque pour leur activité. Le tissu économique de la zone Midi-Pyrénées est maillé de TPE/PME, principalement positionnées dans un secteur industriel B-to-B et très peu d'entre elles sont amenées quotidiennement à manipuler des volumes importants de données à caractère personnel : elles ne tombent donc pas directement dans les cas de nomination obligatoire d'un DPO et préfèrent sans doute investir dans des compétences plus directement utiles à leur cœur de métier.

Pourtant, plutôt que de se focaliser uniquement sur la conformité et la contrainte, les TPE/PME doivent voir GDPR comme une mesure d'aide pour structurer leur transition digitale aujourd'hui incontournable : il permet de poser un cadre sur l'essentiel en matière de recueil et d'exploitation des données.

De plus, la mise en conformité au Règlement européen génère du crédit d'intention, la confiance est un élément cardinal dans la relation avec ses clients, ses collaborateurs et ses partenaires. Maintenir et entretenir cette confiance numérique passe donc par le déploiement de bonnes pratiques en matière de gestion de la "data". ■



Ghislain Gagnoux
Président de Numica

Numica s'empare de GDPR

Le 22 juin 2017, le club des professionnels IT en Champagne-Ardenne Numica a organisé un événement annuel majeur sur le thème du RGPD avec 4 interventions mêlant angle juridique (Isabelle Renard, avocate), angle méthodologique (Le cabinet Infhotep), angle solution IT (EOS Informatique et l'éditeur Varonis) et retour d'expérience du DPO d'Alsace E-Santé. Plus d'une centaine de participants ont assisté à cet événement. ■

« La plupart de nos membres ont maintenant une bonne connaissance du sujet et ont pris la mesure des enjeux liés au règlement. Nos membres disposent maintenant de toutes les informations pour démarrer leur chantier, et nous estimons que très peu seront en mesure d'être 100% "compliant" en Mai 2018, mais beaucoup auront entamé une démarche »

GDPR, les enjeux par les rédactions du Monde Informatique et CIO

LE POINT DE VUE DU MONDE INFORMATIQUE



un dossier de **Benoît Huet**, Journaliste

GDPR, le compte à rebours est lancé	14
Le retard à l'allumage en France suscite des inquiétudes	16
Interview de Dominique Pourchet de Partner Magellan Consulting	18
Vers un recyclage d'outils déjà existants ?.....	20
Interview de Jean-Loup Guyot, directeur juridique d'ADLPerformance/ADLPartner.....	22

LA VISION DE WAVESTONE



un article de **Jérôme Billois**,
Directeur de la practice risk management et cybersécurité de Wavestone

GDPR : où en sont les grands comptes ?.....	24
---	----

LE POINT DE VUE DE CIO



un article de **Didier Barathon**, Journaliste

GDPR : les Plans d'action tardent à se mettre en place	26
--	----

Dans moins d'un an, le règlement européen sur la protection des données personnelles RGPD (GDPR en anglais) sera opérationnel. Sur le terrain, le chemin pour respecter la conformité du GDPR est encore long, la grande majorité des entreprises s'en désintéressent encore même si elles sont conscientes, vu les sanctions envisagées, de l'importance de ce règlement. A coups de communiqués, de réunions informatives et d'emailing, les fournisseurs, les prestataires (ESN, cabinets de conseil, etc.) et même les médias ne ménagent pas leurs efforts pour rappeler et informer les entreprises

sur l'arrivée du GDPR. Si ce règlement est avant tout un projet d'entreprise qui concerne les services juridiques dont le DPO sera le chef d'orchestre, les décideurs IT, complémentaires, sont aussi impliqués. Ils se doivent de mettre en règle leur système d'information avec ces nouvelles obligations légales. D'autant que les solutions techniques existent déjà pour la grande majorité. En complément, des applications plus récentes dans la préparation au GDPR, autour de l'anonymisation, de la cartographie et de la gestion des données personnelles vont, bien sûr, se multiplier.



/ LE POINT DE VUE DU MONDE INFORMATIQUE

GDPR, le compte à rebours est lancé

Dans quelques mois, le règlement européen sur la protection des données personnelles (GDPR en anglais ou GDPR en français) entre en vigueur alors qu'une large majorité des entreprises, à en croire les multiples études réalisées depuis quelques mois sur ce sujet, méconnaissent encore ce règlement (voir partie 2). Par exemple, pour le cabinet KPMG, qui a réalisé une étude sur GDPR au printemps dernier, ce sont plus de 70 % des entreprises qui n'ont pas une bonne connaissance du règlement. Un point plutôt inquiétant d'autant que les entreprises qui ne respectent pas GDPR sont potentiellement soumises à de fortes amendes, lesquelles peuvent atteindre 4 % du chiffre d'affaires, jusqu'à un montant maximal de 20 millions d'euros. Concernant ces sanctions, Vincent Maury, CTO de DenyAll, tempère : « A mon avis, en cas de fuites de données, les premiers blâmes, après audits, ne seront pas donnés avant 2019, les autorités afficheront une certaine souplesse la première année. » A ne pas douter que quelques gros acteurs, notamment du web et de nationalité américaine, seront les premiers surveillés par les autorités européennes. A en croire certains experts, ils feront potentiellement les frais d'une sanction pour montrer l'exemple... En attendant, la dernière sanction infligée au loueur de

véhicules Hertz par la CNIL sur des manquements à mieux protéger les données de ses utilisateurs (en vigueur de la loi pour une République numérique du 7 octobre 2016, présentée par Axelle Lemaire) laisse augurer de ce qu'il adviendra aux entreprises qui négligeraient de protéger les données personnelles après la mise en application du GDPR.

Rappelons que ce nouveau règlement, qui remplace l'actuel régime de déclaration des traitements à la CNIL (rendu public depuis peu), oblige les entreprises, mais aussi leurs prestataires et sous-traitants, à tenir un registre de mise en conformité des données personnelles. Ce règlement recommande aussi aux entreprises concernées de faire appel à un DPO. La désignation de ce dernier est même obligatoire pour les organismes publics et pour les entreprises dont l'activité exige un suivi régulier et systématique à grande échelle des personnes concernées ou dont l'activité consiste en un traitement à grande échelle de données particulières (données de santé, données sur l'opinion politique ou religieuse, l'orientation sexuelle, etc.). En dehors de ces cas, la désignation sera facultative mais encouragée par les membres du G29, groupe des CNIL européennes.

Le DPO, d'abord un spécialiste du droit

Pour les grandes entreprises privées et publiques, la nomination d'un DPO (Data Protection Officer) devrait juste apparaître comme une simple formalité. En effet, celles-ci disposent très souvent d'un service juridique ou d'un correspondant informatique et libertés (CIL), souvent bien formé en droit, qui, bien avant l'entrée en vigueur prochaine du GDPR, était déjà en charge de la problématique des données personnelles. A titre indicatif, 33 % des répondants à l'enquête de KPMG sur GDPR indiquent que leur direction juridique est en première ligne pour initier la mise en conformité du règlement européen contre seulement 12 % pour le RSSI. Quant au DSI, son rôle est tout aussi important puisque le système d'information se doit d'être en règle avec ces obligations légales. « Le juriste, quand il existe dans l'entreprise, est le principal garant du respect de la conformité. Le DSI, complémentaire, se met, quant à lui, en obligation par rapport à ce règlement en effectuant une vérification et un suivi rigoureux, notamment auprès des prestataires, lesquels se doivent aussi de nous fournir un registre », indique Olivier Cavrois, DSI à temps partagé chez Référence DSI. Bien sûr, le décideur IT (DSI, RSSI, etc.) peut aussi devenir un DPO, des formations vont d'ailleurs se multiplier, dès la rentrée, pour acquérir les compétences nécessaires, elles sont généralement dispensées par la CNIL, des universités (Paris II ASSAS, Paris Nanterre, etc.), des écoles supérieures ou même des centres de formation comme Anaxil-DPMS, ce dernier dispensant des formations labellisées CNIL et Bureau Veritas dédié aux CIL/DPO internes, externes et mutualisés.



Un budget considérable pour les gros manipulateurs de données personnelles

Pour les PME, la solution la plus simple est de faire appel à un DPO externe comme le font déjà certaines pour leur comptabilité avec un expert-comptable tiers. Des prestations de ce type fleurissent déjà sur le web, ces DPO externes se chargent des déclarations préalables auprès de la CNIL, de la rédaction du registre obligatoire, du suivi ou encore de la sensibilisation auprès de tous les collaborateurs. Bref, ils doivent répondre aux exigences de l'article 39 du GDPR qui définit leurs missions. Concernant le budget alloué à la mise en place du règlement, les premiers retours montrent déjà un montant de plusieurs millions pour les grandes organisations. Wavestone s'est d'ailleurs livré à quelques estimations plutôt édifiantes : de 1 à 5 millions d'euros pour les entreprises disposant d'un nombre raisonnable de données personnelles et de 20 à 50 millions d'euros pour les structures possédant plusieurs métiers et de très nombreuses entités/filiales. A noter que pour certains très grands acteurs internationaux, les premiers engagements budgétaires ont même été de plusieurs centaines de millions d'euros. ■



Le temps est compté pour mener un projet complexe



Une action de mise en conformité a-t-elle été initiée ?

Pensez-vous que le projet de mise en conformité sera terminé en mai 2018 ?



47%
Il ne sera probablement pas terminé

42%
Il sera probablement terminé

6%
Il ne sera pas terminé

5%
Il sera terminé

Un effort important à fournir pour
67%
des entreprises

72%
des entreprises n'ont pas une bonne connaissance du GDPR

/ LE POINT DE VUE DU MONDE INFORMATIQUE

Le retard à l'allumage en France suscite des inquiétudes

« A un an de l'entrée en vigueur du GDPR, les entreprises n'abordent pas encore cette problématique », nous confirme à son niveau local Alexandre Barreau, directeur de l'intégrateur CG2J, situé dans le sud-est de la France. Selon l'étude sur GDPR réalisée par l'ESN Umanis en juin dernier, 50 % des entreprises françaises ignorent les problématiques induites par la mise en conformité du nouveau règlement et 67 % d'entre elles en sont même encore au stade de la veille technologique. De même, 70 % des sociétés sondées n'ont pas nommé de DPO et seules 7 % considèrent que la désignation d'un pilote GDPR est une priorité. D'autre part, si 77 % des répondants perçoivent GDPR comme une formidable opportunité pour créer de la valeur à partir de leurs données, 46 % des entreprises interrogées ne savent pas du tout si elles seront conformes à temps et 23 % pensent que ce sera impossible de l'être.

Le casse-tête du droit à l'oubli

Sur ces éventuels retards, s'ils restent à court terme, les pouvoirs publics devraient être très compréhensibles surtout pour les petites structures. Souvenons-nous du droit à l'erreur voulu par Emmanuel Macron lors de son élection à la présidentielle qui prône, pour une première faute, l'accompagnement de l'administration plutôt que la sanction. Il faut savoir que parmi les difficultés à la préparation du GDPR, les entreprises évoquent surtout la localisation et la cartographie des données personnelles dans leur SI, ce qui représente un réel problème concernant l'application de l'article 17 du règlement qui évoque le « droit à l'oubli. » En effet, les entreprises doivent être capables de localiser et cibler des données spécifiques afin d'automatiser leur suppression à la demande du consommateur. C'est un énorme chantier selon le cabinet Wavestone qui

estime que l'exercice des droits représente 20 % des budgets en raison des évolutions requises au sein des systèmes d'information.

Pour Veritas qui a récemment mené une étude sur GDPR, 16% des entreprises françaises admettent même que les données personnelles ne peuvent être supprimées ou modifiées en cas de demande. En attendant, certaines entreprises ont déjà pris les devants à l'image du fabricant américain de tracteurs agricoles John Deere qui a récemment envoyé des lettres de consentement à ses clients européens afin de leur demander une autorisation pour exploiter commercialement leurs données personnelles. Enfin, à en croire nos interlocuteurs, la majorité des entreprises admettent qu'il est difficile d'identifier et de signaler une faille de données personnelles dans les 72 heures, cette dernière est pourtant une exigence de la réglementation quand il y a un risque pour les individus concernés. Il faut savoir qu'il n'est pas rare dans les entreprises de découvrir certaines brèches de sécurité six mois après une attaque alors la signalisation dans les 72 heures les laisse perplexe... ■



16%

des entreprises françaises admettent même que les données personnelles ne peuvent être supprimées ou modifiées en cas de demande.





Dominique Pourchet de Partner Magellan Consulting

/ LE POINT DE VUE DU MONDE INFORMATIQUE

Interview de Dominique Pourchet de Partner Magellan Consulting

A moins d'un an du lancement officiel du GDPR, quelle est la situation des entreprises sur le terrain ?

Un climat anxieux s'est installé par rapport au GDPR car les entreprises estiment qu'elles ont énormément de choses à réaliser pour être en conformité avec GDPR. Dans la majorité des grandes entreprises, ce sujet s'inscrit déjà dans leurs priorités. C'est en revanche plus compliqué dans les PME et les ETI, certaines découvrent même le règlement et n'ont donc pas encore pris en compte l'impact des sanctions en cas de non-respect du règlement. C'est d'autant plus inquiétant pour les entreprises dont le métier est de traiter des données pour le compte de leurs clients. Pour accéder à la connaissance du GDPR, nous organisons régulièrement des matinées et des

petits-déjeuners. Pour l'heure, nous ne pouvons pas encore communiquer sur des retours d'expériences, GDPR étant toujours en cours de déploiement. D'ici à la fin du mois, voire début octobre, nous pourrions éventuellement lister les premiers cas d'usages.

Quels sont les principaux impacts du GDPR sur la DSI ?

Cette démarche de mise en conformité, c'est un triptyque entre le DPO, le DSI et le RSSI, le DPO faisant office de chef d'orchestre. Car au-delà des aspects juridiques, il y a un vrai travail pour identifier et cartographier les données personnelles dans l'entreprise et chez leurs prestataires, sans oublier la mise à jour des applications et des systèmes de sécurité. Il faut aussi prendre en compte l'analyse des risques (ndlr : comment sont gérées les données à caractère personnel ?) et le

déploiement de nouveaux outils. Bien sûr, le DSI peut aussi faire office de DPO s'il suit une formation juridique, tout dépend de l'organisation de l'entreprise. Quant aux directions métiers, elles sont également impliquées dans GDPR car elles traitent souvent des données personnelles. A ce titre, tout n'est pas négatif, ce règlement a vocation à élever le niveau de sécurité dans l'entreprise car l'ensemble des équipes est sensibilisé.

Quelles solutions proposez-vous pour accompagner les entreprises ?

Déjà de faire un bilan en binôme avec un cabinet d'avocat, nous travaillons à ce titre avec le cabinet Bensoussan spécialisé dans le droit numérique. Nous conseillons aussi aux entreprises d'avancer pas à pas et d'avoir une réelle approche de benchmarking avec les autres entreprises. De même, il est important de suivre les recommandations de la CNIL, du G29 ou de l'association des DPO (ADPO) -<https://www.data-protection-officer-association.eu/> - qui disposent de calendriers précis sur ce sujet. Pour les outils, les solutions (de cartographie des données, de chiffrement, de détection d'incidents, etc.) existent mais les entreprises doivent comprendre comment les mettre en œuvre. Enfin, nous faisons aussi office de DPO de transition pour les entreprises qui sont en cours de recrutement.

Quel est le coût de cette mise en conformité du GDPR pour une entreprise ?

Difficile de répondre, une récente étude estime le coût à 30 millions d'euros (ndlr : étude menée par Sia Partners) pour une entreprise du Cac 40. Tout dépend du niveau de maturité, le coût peut être de 10, 20 ou 30 millions d'euros. L'investissement reste très élevé, l'entreprise doit notamment revoir tous ses contrats pour atteindre cette mise en conformité. Elle devra aussi investir des sommes importantes dans l'outillage. Passée cette mise en conformité, cette charge diminuera. ■





Loïc Guézo, stratège Cybersécurité Europe du Sud chez Trend Micro

/ LE POINT DE VUE DU MONDE INFORMATIQUE

Vers un recyclage d'outils déjà existants ?

« GDPR se résume avant tout à des bonnes pratiques, les outils techniques existent déjà. Les fournisseurs de solutions de sécurité s'approprient cette thématique surtout d'un point de vue marketing », avoue Vincent Maury, CTO de DenyAll. Et d'ajouter : « Chez DenyAll, nous disposons déjà d'un portfolio qui répond directement au GDPR autour du chiffrement, de l'authentification, de la segmentation des réseaux, de la protection des applications, sans oublier le scan de vulnérabilités. GDPR va néanmoins obliger les entreprises à mieux prendre en compte la sécurité en général ». Un avis général que partage Loïc Guézo, stratège Cybersécurité Europe du Sud chez Trend Micro : « Pour être très clair, les DSI considèrent que GDPR est un sujet d'entreprise à l'instar du bug de l'an 2000 ou de la conformité PCI-DSS mais pas un sujet proprement lié aux solutions de sécurité. Et je partage ce point de vue, GDPR est d'abord un projet de consulting, de gouvernance et de gestion de projet.

Chez Trend Micro, les solutions techniques sont déjà matures comme nos systèmes d'anti-intrusion. Bien sûr, nous ferons aussi du marketing autour de l'utilisation à bon escient du règlement pour aider les clients à le comprendre. »

Des solutions sous forme d'aide à la préparation au GDPR

Un certain nombre de fournisseurs profite aussi de ce règlement pour porter des nouveaux services, le plus souvent des guides de préparation ou des solutions d'inventaires qui reprennent les points majeurs du GDPR à l'image de l'offre de services de Veritas GDPR Compliant qui s'appuie sur tous les articles du règlement. De même, Software AG a récemment lancé un framework GDPR permettant de se préparer dès maintenant à ce nouveau règlement. Ce framework

fournit des rapports, des workflows et des enquêtes directement exploitables pour la catégorisation des données, ainsi que l'évaluation des applications et de la progression de la mise en conformité. IBM, avec ces nouveaux outils qui s'appuie sur sa plateforme Resilient Incident Response (IRP), souhaite également accompagner les entreprises dans leur mise en conformité du GDPR. Ces solutions inclut notamment un guide de préparation étape par étape, une fonction d'aide pour répéter les actions que les entreprises devront potentiellement entreprendre à l'avenir en cas de violation, sans oublier le module de confidentialité qui répertorie les normes du GDPR et ses éventuelles mises à jour à venir jusqu'en mai 2018, la date d'entrée en vigueur du règlement.

L'intelligence artificielle au service du GDPR

Une autre catégorie d'outils va se démocratiser un peu plus avec l'arrivée du GDPR, c'est l'anonymisation des données basée sur diverses techniques (chiffrement, hash, variance, concaténation, mise à blanc, masquage, etc.), mais aussi sur de l'intelligence artificielle à l'image de la société britannique anon.ai présente sur le dernier salon Infosecurity à Londres qui utilise ces technologies pour sa propre solution d'anonymisation. D'ailleurs, les fournisseurs sont toujours plus nombreux à injecter une dose d'intelligence artificielle dans leurs solutions « GDPR Ready » à l'image de Box dont le machine learning aiderait les entreprises à mieux comprendre les données dont elles disposent en appliquant une intelligence au contenu. « Etre en conformité commence par comprendre les données et les informations que nous possédons en tant qu'entreprise. Les organisations internationales telles que General Electric ou AstraZeneca par exemple doivent faire face à un environnement ultra complexe (réglementations sectorielles, locales et régionales, enjeux liés à la confidentialité des données et la cybersécurité). En utilisant l'intelligence artificielle, Box souhaite simplifier au maximum le processus et ainsi permettre aux entreprises de mieux comprendre les données qu'elles hébergent dans la plateforme Box, puis appliquer les mesures de conformité adéquates à chacune de ces informations. Comment ? En adaptant automatiquement la donnée à toutes les

réglementations en vigueur dans la région où elle est stockée et utilisée. Pour ce faire, Box va développer un système adaptable et qui peut changer en fonction de l'endroit où travaille un utilisateur, du profil de la personne qui travaille sur la donnée ou encore du type de partenaire externe avec lequel cet utilisateur collabore », avait déclaré Aaron Levie, le CEO de Box lors du Box World Tour à Londres en avril dernier.

Quelles que soit les technologies utilisées, la compréhension et l'identification des données dans les entreprises sont essentielles pour respecter la conformité du GDPR. Et ce sur point, l'étude mondiale menée en 2016 par Veritas fait froid dans le dos. « Si 12% des données sont qualifiées de propres dans l'entreprise, 35% sont considérées comme obsolètes mais surtout 53% sont vues comme des dark datas (données obscures), les entreprises ne savent tout simplement pas ce qu'il y a dedans », s'alarme Frederic Viet, directeur channel chez Veritas Technologies pour l'Europe du Sud. ■





Jean-Loup Guyot, directeur juridique d'ADLPerformance/
ADLPartner

/ LE POINT DE VUE DU MONDE INFORMATIQUE

Interview de Jean-Loup Guyot, directeur juridique d'ADLPerformance/ADLPartner

Un CIL est-il le mieux placé pour devenir DPO ? Selon vous, un DSI ou un RSSI peut-il occuper ce poste ?

Dès l'entrée en vigueur du GDPR en mai 2018, le CIL (Correspondant Informatique et Libertés) cessera d'être l'interlocuteur de la CNIL s'il n'est pas désigné DPO. Le CIL a une vocation naturelle à devenir DPO car, bien que les responsabilités dévolues à ce dernier par GDPR soient beaucoup plus étendues que celles actuellement assumées par le CIL, les fonctions de l'un et de l'autre sont très proches. Mais bon nombre d'entreprises ne disposent pas de CIL puisque à ce jour cette fonction n'est pas obligatoire. Un DSI ou un RSSI pourraient faire d'excellents DPO, à condition toutefois qu'ils cessent d'occuper leurs fonctions de DSI ou de RSSI pour éviter tout conflit d'intérêts. A l'instar des profils assumant les fonctions de CIL, les futurs DPO peuvent être soit des juristes ayant une appétence avérée pour les systèmes d'information, soit des DSI ou RSSI sensibilisés aux aspects juridiques des données personnelles.

Quelle est la mission d'un DPO ?

A l'instar du CIL, le DPO est à la fois le garant et le coordinateur de la conformité en matière de protection des données personnelles au sein de l'entreprise. Il est dans cette perspective chargé d'une part, d'informer et de conseiller le responsable de traitement et d'autre part, de contrôler le respect du règlement et du droit national en matière de protection des données. Il a vocation à coopérer avec la CNIL et sera le point de contact de celle-ci au sein de l'entreprise qui l'emploie. Le DPO devra faciliter l'accès par la CNIL aux documents et informations soit lors d'échanges avec cette autorité, soit lors de l'instruction d'une plainte, soit en cas de demande de précisions sur un projet en cours ou bien encore dans le cadre d'un contrôle.

Avec l'arrivée du DPO, le rôle du DSI va-t-il évoluer, si oui, comment ?

Il m'est difficile de répondre à cette question. Toutefois, l'accroissement des responsabilités assumées par le futur DPO devrait conduire les DSI à prendre l'habitude de consulter le DPO et de l'associer à leurs processus de décision. Le DSI devra impérativement se former ou, à tout le moins, être sensibilisé au cadre réglementaire des données personnelles.

En tant que DPO, avez-vous suivi une formation spécifique ?

Je suis CIL et j'ai donc suivi à l'occasion de ma désignation les cycles de formation dispensés par la CNIL. Je dispose par ailleurs d'une solide formation de juriste à l'occasion de laquelle les fondamentaux de la loi informatique et libertés m'ont été enseignés. La CNIL devrait mettre prochainement en place des ateliers réservés aux personnes désignées DPO dans leurs organisations.

Les DPO redoutent-ils déjà l'entrée en vigueur du GDPR, si oui, sur quels points ?

GDPR est à notre avis redouté par les juristes français car il s'agit pour partie de droit mou. En effet, nous sommes habitués en France à travailler avec un cadre réglementaire clair, reposant sur un principe fondamental en application duquel « tout ce qui n'est pas expressément interdit est permis. » GDPR s'inscrit dans une logique beaucoup plus anglo-saxonne de compliance, dont les contours sont par nature difficiles à cerner. Une des notions centrales dans GDPR est le principe d'accountability dont l'entreprise est censée mettre en œuvre les bonnes pratiques formalisées par une politique interne qui doit être documentée. Par ailleurs et surtout, GDPR opère un renversement de la charge de la preuve : tout juriste sait que c'est en principe à l'accusation de rapporter la preuve de l'existence de l'infraction reprochée à

l'entreprise qui l'emploie. Avec GDPR, c'est l'inverse, et c'est l'entreprise poursuivie qui doit prouver que l'infraction qui lui est reprochée n'est pas constituée. Ce renversement est évidemment de nature à inquiéter les entreprises. Mais si elles l'envisagent comme une menace, il est également possible de voir GDPR comme une opportunité de professionnaliser et de sécuriser davantage les usages liés à la donnée pour le bien des consommateurs mais également le bien des entreprises elles-mêmes, souvent suspectées de négliger ces sujets. ■





Gerome Billois, directeur de la practice risk management et cybersécurité de Wavestone

/ LA VISION DE WAVESTONE

GDPR : où en sont les grands comptes ?

Le cabinet Wavestone publie une étude sur les priorités et les investissements des grands comptes sur GDPR.

Le cabinet conseil Wavestone publie une étude sur les priorités et les investissements des grands comptes sur GDPR.

Dans dix mois, toutes les entreprises détenant des données personnelles de particuliers européens devront être conformes au règlement GDPR. Le cabinet conseil Wavestone a synthétisé les réactions de vingt de ses clients grands comptes et d'une quarantaine de donneurs d'ordre, sur leur état de préparation et les moyens mis en oeuvre.

En termes de ressources humaines, GDPR mobilise entre trois et quelques dizaines d'ETP, équivalents temps plein, dans les entreprises. Une compagnie d'assurance parle de 40 business unit concernées, 300 personnes mobilisées, et 4 ETP en central. En première ligne, se retrouvent des IT managers : responsables IT ou digital et RSSI, qui concentrent

40% de la charge GDPR en entreprise « Contrairement à certaines idées pré-conçues, note l'étude, la charge pour les équipes juridiques et pour le RSSI reste limitée, au regard de la charge globale ».

Une 2ème phase plus opérationnelle

Le travail sur GDPR se fait en deux temps. Une première étape d'analyse est franchie, place à l'opérationnel. Désormais, « les coûts IT sont donc plus souvent liés à des problématiques d'exercice des droits, de suppression des données, de portabilité, de surveillance des systèmes, de revue des droits ou de mise sous contrôle du process de la gestion des habilitations pour certains pans du SI, etc », note Wavestone. La partie juridique devient moins importante, la cybersécurité développe des programmes déjà existants qui ne sont pas liés à l'origine à GDPR, mais le prennent en compte en cours de déploiement.

Après l'IT, les métiers, avec 25% de la charge globale, sont très impliqués dans GDPR, suivis du DPO et du juridique (20%), enfin, l'équipe de pilotage intervient pour coordonner, accompagner et former. Les ressources sont aussi budgétaires et Wavestone constate, qu'après une mise en route laborieuse, les budgets de ses clients ne cessent d'augmenter pour la mise en application du Règlement. Les analyses d'écart et la complexité du sujet poussent à cette augmentation.

Cinq points à travailler

Wavestone identifie d'ailleurs cinq points de blocage dans la mise en place de GDPR. D'abord, l'application des délais de rétention et du droit à l'oubli au sein du SI. Il en coûte de 40 à 200 000 euros par application. La mise en conformité des contrats existants, lui, bute sur la présence de milliers, voire de dizaines de milliers de ces contrats dans les entreprises. Troisième sujet, la méthodologie d'accompagnement de projets et les outils d'analyse de risques sur la vie privée (les PIA, Privacy Impact Assessment). La question des compétences venues de la DSI, du juridique ou du contrôle interne et de leur pilotage, vient après. Enfin, l'organisation de l'équipe DPO, qui ira bien au-delà de mai 2018, forme un cinquième chantier.

Une échéance qui sera respectée pour les risques majeurs, l'organisation DPO et ses budgets permettant de mettre ensuite l'entreprise en totale conformité. Ce sera la troisième grande étape. Les directions générales en prennent conscience, elles demandent actuellement, selon Wavestone, aux DSI et aux directions métier de « dé-prioriser » certains budgets pour les allouer à GDPR. Wavestone s'est livré à quelques estimations budgétaires édifiantes.

Des fourchettes budgétaires très larges

Le cabinet d'études livre trois fourchettes budgétaires. « De 1 à 5 millions d'euros pour les organisations manipulant un nombre raisonnable de données personnelles et peu mobilisé sur le big data ou le profiling

Entre 20 à 50 millions d'euros lorsque l'entreprise a plusieurs métiers et de très nombreuses entités/filiales. Pour certains très grands acteurs internationaux, 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 ».

Réaliste, Wavestone estime que les entreprises revoient le planning initial et le budget, les deux sont très liés, mai 2018 n'est plus une échéance, mais une étape. Les entreprises vont revoir leur budget pour être conformes avec un planning plus réaliste que celui initialement envisagé. ■





Sophie Nerbonne, Directrice de la conformité à la CNIL

/ LE POINT DE VUE DE CIO

GDPR : les plans d'action tardent à se mettre en place

« Tout va changer, tout va vraiment changer au 25 mai 2018 ». Celui qui assène tranquillement ce pronostic capte facilement l'attention, il s'agit de Maître Alain Bensoussan, du cabinet du même nom. Après quarante ans d'expérience, il fait comme on dit « autorité ». « GDPR (*) est un big bang » poursuit-il. Lui qui a connu, la Loi Informatique et Libertés peut livrer son diagnostic avec un certain recul. Au commencement était la Directive européenne du 24 octobre 1995 (article 94.1) relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Depuis, Internet, le cloud et le big data ont quelque peu rebattu les cartes. Surtout, cette directive n'imposait rien, donc chaque Etat, s'il la transposait en droit national était libre de ses définitions, par exemple sur ce qu'est un identifiant personnel.

La Commission, dans sa grande sagesse et son infinie lenteur a donc décidé en 2012 de mettre au point une nouvelle législation sur la protection des données personnelles. De cette idée, est née la fameuse GDPR.

Notons que dans le même temps, l'Europe lance des enquêtes sur les principaux acteurs du cloud américain, Microsoft et Google en particulier et, qu'en matière d'hébergement des données, les opérateurs télécoms européens, Deutsche Télécom et Orange en tête, se dotent d'infrastructures indépendantes des américains. Ce n'est pas tout à fait le même sujet, mais c'est le même état d'esprit européen : « nos structures deviennent robustes pour faire de l'Europe un système de protection différent de celui des Etats-Unis » souligne Maître Bensoussan.

Co-responsabilité avec les sous-traitants

Avec GDPR, les responsables d'entreprise ont un horizon balisé, mais contraignant. Qu'ils soient juristes, responsables sécurité, compliance, informatique, bref tous ceux qui voient GDPR tomber sur leurs épaules, ont une date butoir, le 28 mai 2018. Ils ne sont pas seuls dans ce cas, GDPR implique une notion de co-

responsabilité avec les sous-traitants, hébergeurs et partenaires cloud. La notion de responsabilité est essentielle, en interne avec plusieurs métiers concernés, comme en externe avec les sous-traitants (c'est la notion d'accountability). Un casse-tête pour toute entreprise qui travaille peu ou prou en Saas, un bonheur pour les avocats qui n'osent parler de parts de marché, mais c'est tout comme.

Sont concernées par le nouveau règlement, toutes les organisations : entreprises, administrations ou même associations détenant des données personnelles. Quelle que soit la taille, dans les faits, surtout les grandes organisations publiques ou privées détenant des comptes clients. Les banques et assurances ou l'administration des impôts sont des exemples parlants. Sont concernées, toutes les données personnelles. En clair, tout identifiant. Les vieux : numéros de téléphone, adresse postale, numéros de compte ou de dossiers. Et les nouveaux, ceux de l'Internet : adresses mails, données biométriques, données croisées, géographiques ou historique (sur une de vos activités). C'est le traitement de ces données qui va changer avec un impact sur les systèmes informatiques qui permettent de stoker et analyser ces données. Vaste programme.

La menace d'une forte amende

Comme sur beaucoup de sujets, il est question avec GDPR de gouvernance, en clair de passage au Comex du dossier. En fait, ce n'est pas parce qu'un dossier GDPR est soumis et approuvé en Comex que les moyens suivent ou qu'ils sont clairement dégagés. Et d'abord, comment est-il passé, avec quels arguments ? Un déroulé dense d'arguments juridiques et techniques ? Ou bien « l'argument choc qui va décider le dg », en clair la menace de sanctions. C'est plus parlant pour un « dg » d'entendre parler de dizaines de millions d'euros d'amendes. Et le membre du Comex qui fait passer le dossier a une chance de le faire approuver, s'il brandit la menace d'une forte amende.

Celle-ci varie jusqu'à 2 ou 4% du chiffre d'affaires. Jusqu'à 2 % pour mauvaise tenue des enregistrements (article 28), défaut de notification de l'autorité de surveillance et de la personne concernée à propos

d'une violation (articles 31 et 32), ou absence d'évaluations d'impact (article 33). Pour aller jusqu'à 4%, il faut être convaincu de violation des principes de base de la sécurité des données (article 5) et des conditions de consentement des consommateurs (article 7). Au passage, on apprend que c'est la CNIL qui perçoit l'amende et pas Bercy.



« Très peu d'entre vous seront prêt à la date butoir »

Si le projet est mis en route, l'entreprise fait face aux questions de méthodologie. Par où commencer ? Qui décide ? Rien d'évident. Pas d'affolement, les entreprises sont confrontées à de multiples obligations de compliance (voir encadré), GDPR est l'une des principales et touche une bonne partie des responsables, métiers, juridique-audit, IT et sécurité. Sophie Nerbonne Directrice de la conformité à la CNIL, n'exclut pas d'ailleurs, une délégation de responsabilité, du DPO (le Délégué à la protection des données) vers les métiers, essentiellement marketing, RH et R&D, qui détiennent le plus de données. La question des filiales et de l'international, risque de démultiplier l'impact de GDPR. « Rares seront les sociétés qui seront conformes au 28 mai 2018 » souligne Sophie Nerbonne, Alain Bensoussan le formule de manière plus provocante : « rassurez-vous très peu d'entre vous seront prêt à la date butoir, vous serez tous en retard » (propos tenus au Congrès BigData). Et tous concernés, GDPR s'applique à toute entreprise active en Europe, traitant des clients européens, quelle que soit sa nationalité d'origine.

Les entreprises sont aux prises avec GDPR qui se décline en plusieurs articles. Certains bien connus, l'amende éventuelle, la notification de violation ont fait l'objet d'une certaine médiatisation. Mais là n'est pas l'essentiel. « Pour bien comprendre, souligne Alain Bensoussan, il faut mettre en avant la nécessité de cartographier les données ». Une cartographie légale qui n'a rien à voir avec une cartographie technique. Pour lui, les entreprises vont saisir cette occasion pour regrouper des applications. Par exemple recrutements, contrats de travail, formation, seraient plus facile à cartographier pour GDPR, si elles ne formaient plus qu'une seule application.

Tout va dans le même sens

Les entreprises doivent intégrer d'autres contraintes. Leur client au sens large (consommateur ou citoyen) doit émettre un consentement « explicite » et « positif ». Il dispose d'un droit à l'effacement (« à l'oubli ») c'est l'article 17, ou de ne pas faire l'objet d'un profilage (article 22). D'un droit à la portabilité, donc de disposer de ses données dans un format structuré et courant. Tout est donc fait pour protéger les données de la personne. Elles doivent être sécurisées (article 25), dès la conception (privacy by design), ou par défaut. Toute violation des données doit être notifiée (article 33) à une Autorité nationale de protection. Enfin, l'entreprise est invitée à mettre en place le DPIA, Data protection impact assessment, pour évaluer les risques potentiels de protection des données.

Ce n'est qu'un bref aperçu de GDPR, il donne une idée de son impact sur le système d'information et l'organisation de l'entreprise. D'autres mesures seront prises en compte, comme la nomination obligatoire d'un délégué à la protection des données (DPO, Data Protection Officer en anglais). La CNIL souhaite que le CIL (Correspondant informatique et libertés) hérite de cette fonction. « Le CIL voit son rôle renforcé » souligne Sophie Nerbonne. Mais les CIL sont en dehors de l'organisation IT des entreprises, celle des DSI et des RSSI, à part également des fonctions juridiques ou audits. D'où le malaise qui perle dans plusieurs débats sur leur rôle. Les entreprises s'interrogent. Créer un poste ex nihilo avec un recrutement extérieur ? Les

ressources internes font défaut. De plus en plus de RSSI deviennent également compliance officer et peuvent revendiquer le titre de DPO. En fait, ce titre, cette fonction, semblent devoir s'ajouter à des fonctions déjà exercées, soit à un responsable IT comme le RSSI, soit à un responsable compliance. Ce dernier cas se rencontre dans les banques où la compliance est exercée par un directeur ad hoc, souvent membre du comité de direction.



Rien ne se fera sans le RSSI

Le DPO est obligatoire dans certains cas et pas des moindres, pour les organisations publiques, pour toutes celles qui font un suivi régulier des données personnelles, toutes celles qui traitent des données « sensibles », relatives à des infractions pénales. En fait, la question du DPO est l'une des questions relatives à la gouvernance du GDPR. Rien ne se fera sans le RSSI. Rien ne se fera sans le CDO, chief digital officer, quand ce poste existe. Quant au CIL, c'est aux organisations qui ont de tels responsables de décider et d'informer la CNIL de leur éventuelle transformation en DPO. Cette extension de leur rôle est combattue par plusieurs RSSI que nous avons rencontrés.

Le DPO peut être interne ou externe, et même mutualisé entre plusieurs organismes. On pense aux mutuelles qui pourraient ressentir ce besoin. Mais toutes n'ont pas le même niveau de préparation. La Maif, par exemple, a recruté pour son compte un expert de la CNIL, le chef du service des affaires économiques, Stéphane Grégoire au mois de septembre dernier. Les niveaux de maturité semblent effectivement très différents d'une entreprise à l'autre, d'autant que GDPR impacte plusieurs directions qui doivent collaborer ensemble. C'est peut-être l'obstacle principal.

« Nous sommes bien conscients de la marche à gravir » souligne Sophie Nerbonne, « GDPR n'est pas une mince affaire, il influe fortement sur les entreprises. Je retiens au moins trois axes : le renforcement des droits de la personne, la notion de responsabilité dans l'entreprise avec l'accountability et l'autorité de protection des données ». La directrice de la conformité de la Cnil recommande aux entreprises de mettre désormais au cœur de leur stratégie digitale, la logique de protection des données personnelles. Et souhaite, qu'avec GDPR, se mette en place des standards européens de protection des données. ■

(*) GDPR, General data protection regulation, est le terme anglais pour Rgpd, Règlement général sur la protection des données. Le terme anglais étant plus utilisé, nous l'avons privilégié. Il remplace à la fois la loi française Informatique et Libertés de 1978 et la Directive européenne de 1995, transposée en France en 2004. GDPR ne se transpose pas, ce règlement est d'application directe, il s'impose donc dans tous les pays et à toutes les entreprises dans les mêmes termes. GDPR est gérée par le G29 (les CNIL européennes).



Trop de compliance ne tue pas la compliance

Quand elles parlent de compliance, les entreprises évoquent principalement :

- **les lois sur les infrastructures :** la LMP, Loi de Protection Militaire et son article 22 qui s'applique aux OIV (les arrêtés sont pris, ils sont applicables depuis le 1er octobre 2016), NIS (Network and information security), l'équivalent de la LPM au plan européen qui s'appliquera aux OIV et un peu au-delà, d'ici au 9 mai 2018,
- **les lois sur les données :** par exemple Informatique fichiers et liberté en France.
- **les règlements sectoriaux,** par exemple : PCI DSS pour les banques, HDS (Agrément des hébergeurs de données personnelles de santé), Iso 27001 en sécurité.

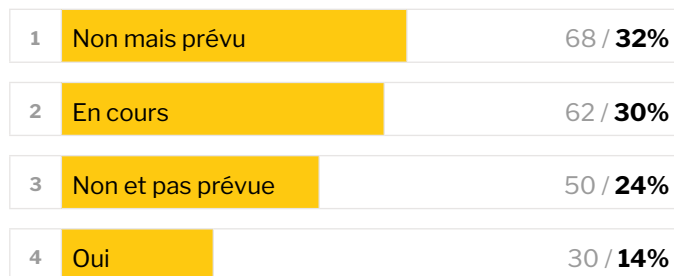
Résultats de l'Enquête Nationale GDPR

Le Monde Informatique a mis en ligne entre juillet et septembre 2017 une enquête pour cerner la façon dont GDPR est perçu au sein des entreprises françaises. 210 personnes y ont participé, dont plus de 25% de managers IT comprenant des DSI et des directeurs techniques. Alors que l'échéance du 25 mai 2018 approche à grand pas, 60% des répondants pensent que leur entreprise ne sera pas en conformité avec GDPR à cette date. Elles ont toutefois bien pris conscience de la nécessité de désigner un délégué à la protection des données personnelles (DPO), puisque 71% d'entre elles l'ont déjà -ou bientôt - fait.

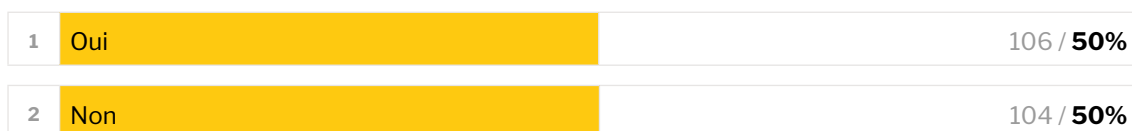
Votre entreprise sera-t-elle en conformité avec GDPR applicable à compter du 25 mai 2018 ?



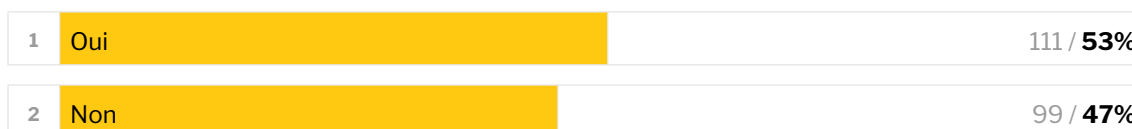
Avez-vous procédé à une analyse d'impact de vos données stockées ?



Avez-vous les ressources pour procéder à une analyse d'impact de vos données ?



Etes-vous capable de notifier à l'autorité de contrôle, dans un délai de 72 h, une atteinte aux données personnelles que vous conservez ?



Avez-vous désigné votre Délégué à la Protection des Données Personnelles (DPO pour « Data Protection Officer ») ?



1	Non et pas prévu	62 / 30%
2	Non mais prévu	62 / 30%
3	Oui	50 / 24%
4	En cours	36 / 17%

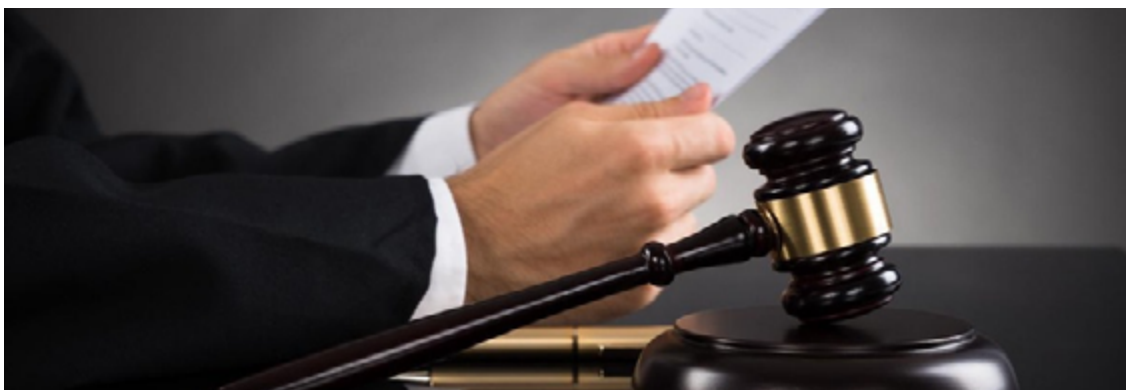
À qui sera rattaché votre DPO ?

1	Direction générale	88 / 42%
2	Autre	46 / 22%
3	DSI	36 / 17%
4	Prestataire externe	21 / 10%
5	RSSI	19 / 9%

Avez-vous impliquer vos fournisseurs (cloud) dans GDPR ?

1	Non et pas prévu	78 / 37%
2	Non mais prévu	56 / 27%
3	En cours	46 / 22%
4	Oui déjà (quasi) fait	30 / 14%

Craignez-vous des sanctions financières en cas de non-respect de GDPR ?



1	Oui	107 / 51%
2	Non	103 / 49%

Votre direction générale est-elle au courant de l'arrivée de GDPR ?

1	Oui	164 / 78%
2	Non	46 / 22%

Vos infrastructures (stockage, sécurité, réseau, hébergement privé ou public) sont-elles adaptées à GDPR ?

1	Des adaptations seront nécessaires	125 / 60%
2	Oui, elles sont adaptées	49 / 23%
3	De profonds changements seront indispensables	36 / 17%










Quelle est votre fonction ?

1	Manager IT (SI/IT)	29 / 14%
2	Manager IT senior (CIO/CTO/VP/Directeur)	27 / 13%
3	Chef de projet	18 / 9%
4	Consultant / Intégrateur systèmes	16 / 8%
5	Manager hors IT senior (CEO/DAF/VP/Directeur)	16 / 8%
6	Commercial / Marketing	14 / 7%
7	RSSI (CSO)	13 / 6%
8	Employé hors IT	11 / 5%
9	Autres (Gestionnaire / Administrateur Systèmes, Membre de l'équipe IT, Manager Gestion de risque / protection des données / conformité, Administrateur Bases de données, Gestionnaire / Administrateur Réseau, Analyste, Architecte, Chef de produit, Manager en charge des applications métiers, Formateur, Programmeur/ Développeur et Manager des Télécoms.)	65 / 30%

Quel est le nombre de salariés au sein de votre entreprise (dans sa globalité intégrant succursales, agences filiales....) ?

1	1000 et +	68 / 32%
2	0 à 49	63 / 30%
3	50 à 199	34 / 16%
4	200 à 499	27 / 13%
5	500 à 999	18 / 9%

Quel est le secteur d'activité de votre entreprise ?

1		High-tech, Télécoms	36 / 17%
2		Services	36 / 17%
3		Banque, finance, assurance	22 / 10%
4		Industries	21 / 10%
5		Conseil	19 / 9%
6		Administration & collectivités	17 / 8%
7		Secteur public	13 / 6%
8		BTP, immobilier	11 / 5%
9		Autres (Secteur association, Biens de consommation/luxe, Transports, logistique, Médias/entertainment, Distribution)	35 / 16%

Le Monde Informatique et CIO

sont des marques d'IT News Info, 1^{er} groupe d'information et de services dédiés aux professionnels de l'informatique en France.

IT News Info est un groupe d'information et de services dédiés aux professionnels des nouvelles technologies plus connu à travers ses marques : CIO, Le Monde Informatique, Distributique, France Entreprise Digital et IT Tour.

En 2007, IT News Info a fait le pari d'être le premier groupe de presse à basculer du print vers le web. Désormais 100% online, l'entreprise se place comme un acteur majeur sur l'information IT en France.

A son expertise média acquise depuis plus de 30 ans (LMI a fêté ses 35 ans au cours de l'IT Tour 2016) vient s'ajouter un pôle événement avec plus de 27 conférences et rencontres professionnelles organisées en moyenne par an dont son fameux Tour de France des informaticiens, l'IT Tour. Lancé en 2012, cet événement réalisé en étroite collaboration avec les clubs de DSI et RSSI français, réuni chaque année de plus en plus de professionnels.

Aujourd'hui, Le Monde Informatique est N°1 sur son marché et est le site média le plus consulté par les informaticiens en France.

IT NEWS INFO c'est :

