BAROMÈTRE RGPD
2ÈME TRIMESTRE 2017

Maturité en hausse, mais la conformité au 25 mai 2018 reste une chimère...

Par Marc Jacob, Emmanuelle Lamandé et Jean-Yves Pronier

AFCDP
Association Data Protection Officers
CLUSIF
Qualys. Continuous Security

Analyse du baromètre RGPD du 2ème trimestre 2017

Ce deuxième Baromètre montre, comme d'autres enquêtes, que la mobilisation progresse et s'organise dans les entreprises à l'approche du 25 mai 2018. Il reste toutefois surprenant qu'autant d'organisations ne se sentent pas prêtes, sans doute en raison d'une méconnaissance des enjeux, sinon d'un certain scepticisme vis-à-vis des sanctions.

On entend encore de nombreux responsables estimer, d'une part que « l'on a encore le temps pour s'occuper du dossier d'ici mai 2018 » et d'autre part, que « le montant des amendes n'est qu'un épouvantail ». Il s'agit là de deux erreurs manifestes.

Le texte du Règlement européen sur la Protection des Données (RGPD) dont l'AFCDP a publié une version annotée et indexée, disponible librement sur son site, indique clairement (article 99) qu'il est entré « en vigueur » le 25 mai 2016 (20 jours après sa publication au Journal officiel) et qu'il entrera « en application » le 25 mai 2018. De toute évidence, le délai de deux ans avant l'entrée en application a été prévu par le Législateur pour permettre aux entreprises de se mettre en conformité avant mai 2018, et non de commencer à réfléchir à cette date. À n'en pas douter, les autorités de contrôle, dont la CNIL, commenceront à vérifier le niveau de conformité réelle dès le 25 mai prochain. Elle y sera forcée en cas de plaintes déposées auprès d'elle par des personnes concernées. N'oublions pas non plus que la CNIL étant libérée du traitement des déclarations et de la plupart des demandes d'autorisation, ses ressources seront sans doute plus disponibles pour effectuer des contrôles.

En ce qui concerne les sanctions pécuniaires, le plafond de 20 millions d'euros (ou des 4 % du CA) est bien un… plafond. Même s'il ne sera probablement pas atteint d'emblée, il permettra de fixer des échelons intermédiaires. À titre d'exemple, le plafond actuel de 150 000 euros prévu par la Loi Informatique et Libertés n'a été infligé que deux fois par la CNIL. Selon le relevé des sanctions publiées sur Légifrance, les quarante sanctions pécuniaires prononcées par la Commission entre 2006 et 2017 varient surtout entre… un malheureux euro et 50 000 €. Avec un plafond à vingt millions d'euros, on peut s'attendre à ce que les sanctions augmentent fortement avec des montants en centaines de milliers d'euros. D'autant plus que le RGPD impose une certaine harmonisation des sanctions entre les pays de l'Union, et que les autorités qui pratiquaient des amendes importantes (comme les autorités espagnole et anglaise) risquent de contribuer à tirer la tendance vers le haut.

Ceci dit, l'esprit du RGPD s'attache bien plus à la responsabilité (« accountability ») des responsables de traitement qu'aux sanctions. C'est donc plutôt dans ce sens qu'il convient d'orienter la réflexion.

La tenue du registre des traitements est la première étape de cette responsabilité : comment une organisation peut-elle assurer la maitrise de ses traitements sans disposer d'un inventaire précis ? C'est tout l'intérêt d'un registre exhaustif, qui suppose une bonne connaissance de la cartographie des traitements. Et cela concerne tous les traitements, y compris ceux qui sont externalisés, hébergés, ou logés dans le « cloud ». Si 93 % des entreprises disent avoir un registre, ou être en train de le créer, l'information à ce sujet semble encore très imparfaite ; en effet, seuls 47 % des répondants pensent que le registre doit couvrir tous les traitements. Imagine-t-on un contrôleur aérien qui n'a connaissance que d'une partie des aéronefs en approche ?

La mise en conformité nécessite également un pilotage cohérent avec un Délégué à la protection des données (DPD, ou DPO dans sa version anglophone) dont c'est la mission. Ainsi, même si l'organisme n'entre pas sous le coup de l'obligation de désigner un DPD (selon l'article 37 du RGPD) l'AFCDP recommande de nommer sans tarder un Correspondant Informatique et Libertés (dans le cadre de la loi Informatique et Libertés), qui aura vocation à devenir DPD dès que la CNIL ouvrira la procédure de désignation, probablement avant la fin 2017. Le baromètre semble indiquer que les entreprises ont bien intégré cette orientation, puisque 78 % d'entre elles indiquent que le projet RGPD est pris en charge par le CIL, le DPD ou le futur DPD. Pour celles qui ne seraient pas encore convaincues, l'AFCDP a publié une série de témoignages de responsables de traitement qui expliquent tout l'intérêt qu'ils ont retiré de la désignation d'un CIL, futur DPD.

La troisième préoccupation sur laquelle il convient de se concentrer est la documentation des traitements : en contrepartie de la disparition des formalités préalables (déclaration à la CNIL, demande d'autorisation…) le principe de responsabilité exige que chaque traitement fasse l'objet d'une documentation formalisée qui permettra, en cas d'incident ou de contrôle, de démontrer que la mise en œuvre a bien respecté les obligations du Règlement.

Cette documentation englobe la grande nouveauté que constitue l'Analyse d'impact sur la protection des données (AIPD), prévue par l'article 35 du règlement. Si l'AIPD ne s'impose que si le traitement « est susceptible d'engendrer un risque élevé pour les droits et libertés », en cas d'incident (par exemple en cas de fuite de données), il faudra être en mesure de présenter les résultats de cette analyse, ou de montrer pourquoi on avait estimé qu'elle ne s'imposait pas. D'où la nécessité d'effectuer, dans tous les cas, une « mini analyse d'impact ». Une pratique à exiger, d'ores et déjà, de tous les chefs de projet. Et apparemment, il y a encore beaucoup à faire à ce sujet puisque 64 % des entreprises n'ont pas encore ouvert le chantier des AIPD. Rappelons qu'il s'agit bien ici d'étudier les impacts potentiels du traitement sur les personnes concernées, et non sur l'entreprise.

Mais finalement, toutes ces considérations ne doivent pas faire perdre de vue l'esprit du RGPD, dans la droite ligne de la Loi Informatique et Libertés. N'en déplaise à certains acteurs (cabinets de conseil, constructeurs, éditeurs, etc.) qui entretiennent une frénésie culpabilisante, de menaces de sanctions en solutions censées fournir une immunité rassurante, les professionnels de la protection des données que fédère l'AFCDP préfèrent concentrer l'attention sur les avancées positives qu'apporte le Règlement.

Non, le RGPD n'est pas qu'une question de sécurité des données ! C'est d'abord une affaire de posture qui doit commencer par la conviction que la protection des données (des prospects, des clients, des patients, des collaborateurs…) répond à une attente des individus, et qu'elle participe pleinement à la responsabilité sociétale des organisations. Devant l'avalanche de propositions commerciales qui finissent par semer le trouble dans l'esprit des décideurs, le Délégué à la protection des données est, plus que jamais, l'interlocuteur incontournable à même de définir les objectifs prioritaires et de sélectionner les réponses adaptées à la démarche de mise en conformité de son organisme.

Patrick Blum

Administrateur de l'AFCDP,
en charge de la Commission « métier »
CIL et RSSI de l'ESSEC Business School

Dis-moi avec qui tu partages tes données, je te dirais si tu es conforme au RGPD.

Ne pas mésestimer le risque associé aux tiers dans sa mise en conformité avec le Règlement Général sur la Protection des Données (RGPD). Les entreprises affairées à réorganiser de nombreux processus et systèmes pour se mettre en conformité ne doivent néanmoins pas négliger un élément clé de la conformité, à savoir le risque lié aux tierces parties. En effet, le Règlement Général sur la Protection des Données exige des entreprises qu'elles protègent de manière adéquate l'information personnellement identifiable (IPI) de leurs clients européens, qu'elles sachent où sont stockées chacune de ces données, ainsi que leur provenance et avec qui elles sont partagées. Cette dernière précision, « avec qui sont-elles partagées ? » est fondamentale car le RGDP étend la responsabilité des données des clients aux tiers avec lesquels l'entreprise partage ces données. En d'autres termes, si un quelconque membre de leur réseau de tiers (fournisseurs, partenaires, sous-traitants, consultants, prestataires...) agit de manière irresponsable et compromet les données de leurs clients, elles seront également impactées par les pénalités et amendes prévues. Par conséquent, il faut non seulement protéger les données des clients au sein de son propre environnement IT, mais aussi veiller à ce que les processus et pratiques des tierces parties soient conformes aux exigences.

Pour satisfaire aux exigences de conformité en matière de risques fournisseur, elles doivent disposer d'un système d'évaluation rapide, précis, et complet. Qualys a développé une solution éprouvée pour adapter et accélérer les audits de sécurité des fournisseurs et vérifier que ces derniers se conforment bien à la réglementation, au RGPD, à celles du marché et aux politiques internes.

Baptisé SAQ pour Security Assessment Questionnaire, ce service de vérification de la sécurité automatise et rationalise l'ensemble du cycle de vie de l'évaluation des risques tiers, notamment la conception de l'enquête, le suivi des réponses, le regroupement des données et la génération de rapports. Basé dans le Cloud, le service SAQ épargne les tâches manuelles fastidieuses aux administrateurs chargés de l'évaluation des risques et garantit une précision sans égale. Avec le service SAQ, une entreprise peut identifier avec rapidité et précision les lacunes en matière de sécurité et de conformité des tiers avec lesquels elle travaille, ainsi qu'en interne au niveau de ses employés. En outre, Qualys a développé un questionnaire entièrement dédié au RGPD qui simplifie davantage cette vérification de l'état de la conformité de son réseau de tiers à la réglementation de l'UE.

Eric Perraudeau
Managing Director SEMEA, Qualys

Maturité en hausse, mais la conformité au 25 mai 2018 reste une chimère...

Pour cette seconde édition du baromètre* RGPD, 112 entreprises hexagonales, tant du secteur privé que public, ont répondu de façon anonyme au questionnaire élaboré par Global Security Mag, avec le concours de l'AFCDP, du CLUSIF et de l'ADPO. Ce second questionnaire abordait deux éléments principaux de la mise en conformité RGPD : le registre des activités de traitement (article 30) et la mise en place des solutions techniques pour assurer un niveau de sécurité adapté aux risques (article 32). Au final, si la maturité des entreprises par rapport au RGPD semble en hausse, la parfaite conformité au 25 mai 2018 reste pour la plupart d'entre elles une chimère...

* Résultats au 28 juillet de l'étude réalisée du 1er mai au 28 juillet 2017

Avant d'entrer dans le vif du sujet, il faut noter que l'indice de compréhension personnelle des répondants relative au RGPD est en hausse avec 71 sur une échelle de 100, contre 62 il y a encore 3 mois. Cela montre un progrès notable dans la compréhension des enjeux et donc certainement dans la manière de conduire le projet de mise en conformité.
Le niveau de compréhension et de support de la part de la direction générale a, quant à lui, été évalué à 45 (sur cent), ce qui semble démontrer que le RGPD commence enfin à être pris sérieusement en compte au niveau du COMEX.

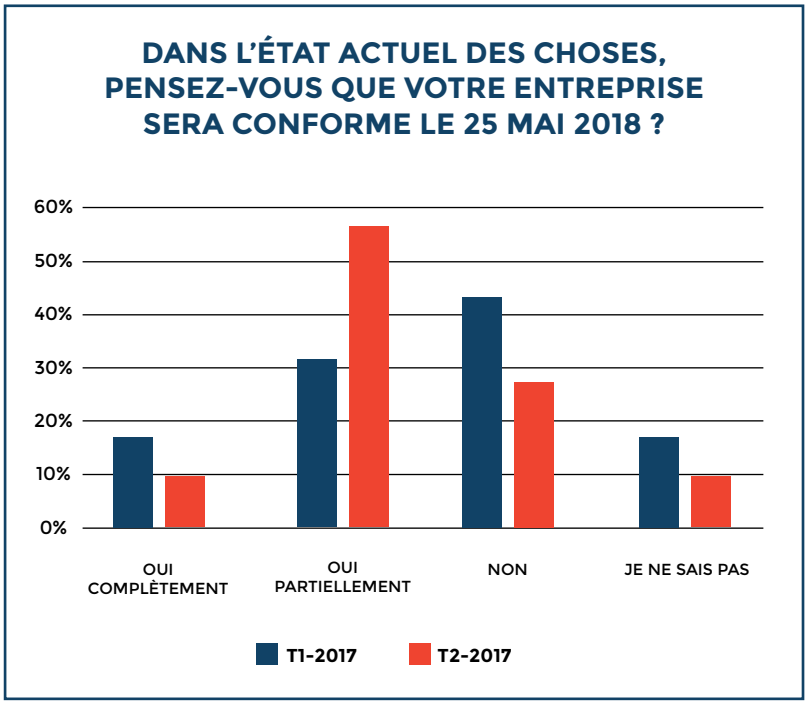
PRÉSENTATION DE L'ÉCHANTILLON

- **21% de grands groupes (plus de 5 000 employés)**
- **25% d'ETI**
- **Et 54% de PME/PMI de moins de 1 500 salariés**

- **50% en provenance du secteur privé**
- **43% du secteur public**
- **7% d'associations**

LES CATÉGORIES PROFESSIONNELLES LES PLUS REPRÉSENTÉES :

- **43% de RSSI/CISO**
- **32% de CIL et 21% de futurs DPO**



Toutefois, avec un indice quasi identique de 33 contre 35 précédemment, les répondants mettent en évidence une compréhension toujours très limitée de la part du reste de l'entreprise (peut-être au niveau des métiers ?).
De son côté, l'indice de confiance relatif à la possible conformité de leur entreprise avec le règlement au 25 mai 2018 s'effondre en passant de 19% au trimestre dernier à 11%. Dans le même temps, une conformité partielle serait envisagée pour 57% des répondants contre 33% il y a 3 mois. Il semble donc qu'une prise de conscience vis-à-vis de l'effort à réaliser ait eu lieu...

• QUI PORTE LE PROJET RGPD AU SEIN DES ORGANISATIONS ?

Le CIL (Correspondant Informatique et Libertés) reste l'élément le plus moteur dans la mise en conformité RGPD pour plus de 46% des répondants. Ce dernier est suivi de près par la DSI, en nette augmentation avec 39%, contre à peine 14% pour le baromètre

précèdent. Enfin, vient le DPO ou futur DPO avec 32% contre à peine 14% précédemment, à égalité avec le service juridique. En ce qui concerne le DPO, l'évolution est synonyme d'une augmentation rapide des nominations à ce poste.

• QUEL EST LE DEGRÉ D'AVANCEMENT SUR LES TRAVAUX LIÉS AU RGPD ?

Par rapport à la précédente enquête, on note une nette progression quant à la mise en place de groupes de travail dédiés. En effet, une entreprise sur quatre en avait un au 1er trimestre, alors que 43% en ont constitué un aujourd'hui ou sont en train de le faire.
Toutefois, les résultats montrent aussi que le chemin sera long. Au niveau de la sensibilisation des collaborateurs, 7% des entreprises ont d'ores et déjà mené des actions et 61% sont en cours de processus. 25% d'entre elles n'ont cependant toujours pas commencé et 7% ne savent pas de quoi il s'agit...
De son côté, la cartographie des données personnelles au sein du SI reste à effectuer pour 36% des entreprises. Quant à la protection des données by design, plus de 57% d'entre elles n'ont pas encore entrepris cette démarche, ce qui n'augure rien de bon dans un objectif de future conformité...

RGPD Survey
2nd quarter 2017

Preparations advancing but compliance by 25 May, 2018 looks unrealistic ...

By Marc Jacob and Emmanuelle Lamandé

For this second edition of the GDPR survey*, 112 private companies in France, both public and private, replied anonymously to a questionnaire developed by Global Security Mag, with the assistance of AFCDP, CLUSIF and ADPO. This second questionnaire addressed two main elements of GDPR compliance: the records of processing activities (Article 30) and the implementation of technical solutions to ensure a level of security of processing adapted to risks (Article 32). All in all while the preparedness of companies in relation to the GDPR seems to be advancing, achieving effective compliance by the 25 May, 2018 deadline remains for the most part unrealistic ...

** Results as of 28 July, of the study conducted from 1 May to 28 July, 2017*

QUEL EST LE DEGRÉ D'AVANCEMENT DE VOS TRAVAUX RELATIFS AU RGPD ?

	FAIT	EN COURS	PAS COMMENCÉ	NE FERA PAS	DE QUOI S'AGIT-IL ?
Les groupes de travail transverses multi-métiers	11%	32%	46%	7%	4%
Sensibilisation interne des utilisateurs	7%	61%	25%	0%	7%
La cartographie des données personnelles dans votre SI	7%	57%	36%	0%	0%
La Protection des données dès la conception et par défaut	11%	29%	57%	4%	0%
Les Analyses d'impact (PIA/AIPD)	7%	21%	64%	4%	4%
Adaptation ou révision des politiques de sécurité au RGPD	4%	36%	57%	0%	4%

En outre, 64% des entreprises n'ont pas encore initié leurs travaux en matière d'analyses d'impacts relatives à la protection des données (PIA/AIPD). Cette situation est assez préoccupante en ce qui concerne les PIA dans la mesure où il s'agit de l'une des pierres angulaires du RGPD. Au-delà des 64% n'ayant pas encore initialisé cette démarche, seules 7,4% des entreprises en ont déjà réalisé et 21% environ sont en cours. Il est à noter que 4% précisent qu'elles n'en feront pas et 4% ne savent même pas de quoi il s'agit.
Nous rappelons à cette occasion qu'une AIPD sera en principe obligatoire pour tout traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques (article 35 du RGPD [1]).

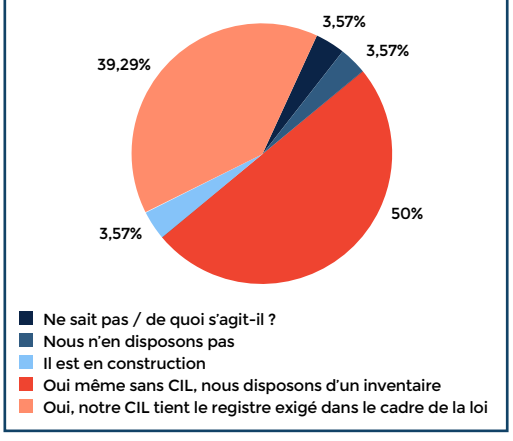
• PRÈS DE 93% DES ENTREPRISES ONT UN REGISTRE OU SONT EN TRAIN DE LE CRÉER

Le registre des traitements des données personnelles est déjà constitué pour environ 43% des entreprises et 50% sont en train de le créer. Seulement 3,5% des entreprises interrogées n'ont pas encore franchi le pas.

[1] https://www.gdpr-expert.eu/article.html?id=35&post_type=post#textesofficiels

LE REGISTRE RGPD

DISPOSEZ-VOUS D'UNE LISTE DE VOS TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL ?



Selon notre baromètre, dans plus de 10% des cas, ce registre serait exhaustif, et pour 46% des répondants la liste des traitements serait à peu près complète. Par contre, dans encore près de 36% des cas, celle-ci reste incomplète, voire très incomplète.
Concernant la compréhension du périmètre que ce registre doit couvrir, pour près de 47%, la liste devrait englober la totalité des traitements, y compris ceux dispensés de déclaration à la CNIL et ceux soumis à autorisation. Alors que, dans un peu plus de 32% des cas, elle est focalisée sur les seuls traitements qui doivent faire l'objet d'une déclaration auprès de la CNIL (ndlr : un héritage de la Loi Informatique et Libertés probablement, est- ce suffisant ?).

Il faut noter que, dans 86% des entreprises interrogées, l'inventaire recense les données liées aux traitements (données structurées liées aux applications sous-jacentes aux traitements). Pour 74% d'entre elles, cela concerne aussi les données confiées à des tiers (hébergement, outsourcing), ce qui montre bien une préoccupation claire des entreprises face à cette problématique. Quant aux donnés déposées dans le Cloud, près de 63% abordent d'ores et déjà ce sujet.

QUEL EST LE DEGRÉ D'AVANCEMENT DE VOS TRAVAUX RELATIFS AU RGPD ?

	OUI	NON	AUCUNE INTENTION DE LE FAIRE
Les données liées aux traitements (données structurées liées aux applications sous-jacentes aux traitements)	86%	14%	0%
Les données accessibles sur les espaces de stockage partagés : NAS, répertoires partagés, Sharepoint... (données non-structurées)	48%	44%	7%
Les métadonnées	24%	68%	8%
Les données personnelles figurant sur support papier	48%	44%	7%
Les données confiées à des tiers : hébergement, outsourcing	74%	26%	0%
Les données dans le Cloud	63%	30%	7%
Les données contenues dans les sauvegardes IT	46%	42%	12%
Toutes les données personnelles dans le SI, qu'elles soient liées ou non à des traitements (données structurées & non-structurées) en interne ou dans le Cloud	37%	56%	7%

• LA FEUILLE EXCEL : L'OUTIL PRÉFÉRÉ DES ENTREPRISES POUR GÉRER LE REGISTRE DES TRAITEMENTS

Par contre, ces listes sont gérées sur la « vieille feuille Excel », qui reste comme à l'habitude l'outil ultime avec un score de plus de 53%. Seulement près de 32% des entreprises utilisent un logiciel payant ou open source installé en interne ou en mode SaaS.
C'est selon nous un sujet de préoccupation pour le maintien à long terme, cependant on voit émerger l'adoption d'outils dédiés beaucoup plus évolués en mode « on-premise » ou SaaS. Ces outils rendent le registre beaucoup plus efficace, riche et utilisable comme un des points de contrôle de la conformité. Il est également à noter qu'une infime partie des répondants utilise encore le support papier.

• LES OUTILS DE GESTION DES ACCÈS ONT LE VENT EN POUPE !

Quant aux outils techniques choisis pour assurer un niveau de sécurité adapté aux risques (article 32), nous aurions pu nous attendre à voir les solutions d'anonymisation, de pseudonymisation et de chiffrement des données personnelles pointer en pole position, mais c'est la gestion des accès et des comptes à privilège (PAM) qui arrive en tête (65%). Toutefois, on constate avec beaucoup de satisfaction qu'un intérêt massif semble émerger à terme sur ces 3 domaines pour une bonne moitié des répondants.
Puis viennent les solutions de gestion, de contrôle et de traçabilité des identités et des accès aux applications et aux données avec près de 54%, une bonne résolution pour se mettre à l'abri des risques de violation de la part des « Insiders ».
Est-ce dû à un bon marketing des éditeurs ou encore grâce au phénomène des « ransomwares » qui démontre chaque jour l'intérêt d'avoir un bon outil de gestion des accès à privilèges et des identités ?...
Avec seulement 15%, la découverte automatisée des données à caractère personnel dans le SI ne fait pas recette aujourd'hui, mais présente un intérêt et donc une piste à suivre dans les mois à venir pour 35% des répondants. Cette mesure semble être une précaution quand il est difficile de cartographier finement les traitements.
Enfin, concernant le SIEM, le DLP et la protection des emails, il est intéressant de voir où les entreprises situent leurs efforts et investissements dans ces domaines, avec respectivement 28%, 23% et 36%.

QUELLES-SONT LES SOLUTIONS TECHNIQUES QUE VOUS COMPTEZ METTRE EN ŒUVRE POUR ASSURER UN NIVEAU DE SÉCURITÉ ADAPTÉ AUX RISQUES ?

	OUI, UNE OU +	NON	INTÉRÊT ET RECHERCHE EN COURS	AUCUN INTÉRÊT
Anonymisation des données personnelles	30%	19%	52%	0%
Pseudonymisation des données personnelles	20%	32%	48%	0%
Chiffrement des données personnelles liées aux traitements	29%	14%	54%	4%
Découverte automatique des données personnelles dans le SI	15%	42%	35%	8%
Gestion/contrôle/traçabilité des identités et des accès aux applications et données	54%	11%	36%	0%
Gestion des accès/comptes à privilège (PAM)	65%	0%	35%	0%
Protection des emails	36%	14%	46%	4%
DLP (Data Loss Prevention)	23%	42%	27%	8%
SIEM	28%	28%	32%	12%

En conclusion, ce second baromètre montre que plus on s'approche de la date fatidique du 25 mai 2018, plus les entreprises prennent conscience de l'ampleur de la tâche à accomplir… et laisse à penser que la conformité RGPD dans les temps impartis reste à l'heure actuelle une chimère…