LA SEMAINE JURIDIQUE
édition générale

Le Règlement général sur la protection des données (RGPD)

Un chantier à démystifier !

Fi des discours anxiogènes et mystificateurs ! Le RGPD peut être appliqué de manière rationnelle. On évitera des approches « Tout IT » ou « Tout Juri ». Elles ont pour avantage d'augmenter les bénéfices de ceux qui les vendent, mais évitent l'essentiel, à savoir la nécessité de diffuser les pratiques au cœur de l'organisation.
Le RGPD ne doit pas être géré comme un projet de court ou moyen terme. C'est avant tout une transformation structurelle et organisationnelle qui est attendue et non une collection d'attributs, un inventaire d'opérations de traitements tous azimuts.
Le cœur du règlement réside dans la notion de « finalité(s) ». C'est sur leur analyse que reposent ce texte et sa mise en pratique. L'approche est donc qualitative avant d'être quantitative. Ainsi l'étude et la description d'une « finalité » relèvent des équipes métier, la mise en œuvre des moyens pour y répondre appartient, souvent, à l'IT, le tout sous le contrôle attentif de la direction juridique.
Pour bien appliquer ce texte, trois mots d'ordre : analyser, organiser, outiller.


Matthieu Bourgeois, avocat associé, Simon Associés, spécialiste en droit des nouvelles technologies, de l'informatique et la communication

Franck Régnier-Pécastaing,
expert en gouvernance de la donnée

Qu'est-ce que le RGPD et pourquoi ce texte ?
Le Règlement général sur la protection des données 2016/679 (en français RGPD, ou en anglais « GDPR » pour *General Data Protection Regulation*) a été adopté le 27 avril 2016 par le Parlement européen après quatre ans de débats. Ce texte n'impose pas aux États membres d'abroger leur législation nationale. Ainsi, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (LIL) est toujours en vigueur ; toutefois, en cas de dispositions divergentes avec le RGPD, ce dernier primera.
Ce nouveau texte répond à un double mouvement : protéger les individus contre les nouveaux risques (vie privée, cybersécurité…) tout en favorisant la circulation des données désormais inhérente à l'activité humaine (économique, sociale, …). Le besoin d'un cadre plus moderne et davantage unifié s'avérait nécessaire pour répondre à ce double impératif et bâtir les fondements d'un marché unique numérique.

Le règlement étant en vigueur, quelles sont les sanctions prévues ?
Le RGPD est en vigueur depuis le 25 mai 2016 (*Règl. (UE) 2016/679, art. 99.1*). Mais ses effets (notamment les sanctions) ont été différés au 25 mai 2018 (*Règl. (UE) 2016/679, art. 99.2*). Cette période de deux ans – dont plus de la moitié est désormais écoulée – a été prévue pour laisser aux organisations le temps de se mettre en conformité. Ce n'est pas de trop à la vue des nouvelles obligations posées par ce texte.
La conformité pour 2018 est un enjeu important pour les organisations. À défaut, elles encourent une amende administrative qui pourra atteindre jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial total de l'exercice précédent, pour certains manquements (le plus élevé des deux plafonds étant retenu).

Qui est concerné ?
Toutes les organisations - ne sont pas visés certains traitements régaliens, comme ceux effectués « *à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales* » (*Règl. (UE) 2016/679, art. 2.2, d*) - dès lors qu'elles sont situées au sein de l'Union européenne ou qu'elles ont une activité dirigée vers des personnes situées au sein de la zone. Ce sera, par exemple, le cas des exploitants de moteurs de recherche ou de réseaux sociaux qui s'adressent à des internautes situés dans l'Union.

Quelles sont les principales nouvelles obligations prévues par ce texte ?
Outre des obligations issues de la LIL, que le RGPD renforce (comme le droit à l'information, les modalités de recueil du consentement…), ce texte impose des nouvelles obligations qui sont de deux ordres :
Sur le plan interne, les organisations devront notamment :
- pour certaines d'entre elles, désigner un délégué à la protection des données (en anglais *Data Protection Officer* ou DPO (*Règl. (UE) 2016/679, art. 37 à 39*), chargé de contrôler la conformité de l'organisation à la réglementation en matière de protection des données ;
- lorsqu'elles comptent plus de 250 employés, ou bien qu'elles réalisent des traitements non occasionnels susceptibles de « *comporter un risque pour les droits et libertés des personnes concernées* » ; constituer et tenir à jour un registre des activités de traitement (*Règl. (UE) 2016/679, art. 30*) ;
- en tout état de cause, mettre en place des procédures internes permettant d'assurer la « *protection des données dès la conception* » des traitements (*Privacy by design*) ainsi que mener des analyses d'impacts préalablement à la mise en œuvre de certains traitements ;
Sur le plan externe, les organisations concernées devront notamment prendre des mesures :
- à l'égard des personnes concernées, notamment en mettant en œuvre de nouveaux droits comme la portabilité de leurs données ;

Parution Septembre 2017

LA SEMAINE JURIDIQUE
édition générale

- à l'égard de l'autorité de contrôle (la CNIL), mettre en place un dispositif permettant de lui notifier la survenance d'une violation des données engendrant « *un risque pour les droits et libertes des personnes physiques* », notification qui devra être etendue à l'ensemble de celles-ci si ce risque est « *élevé* » *(Regl (UE) 2016/679, art 33 et 34)*
- à l'égard des autres acteurs du traitement, etablir des contrats écrits, non seulement avec les sous-traitants, mais également avec les responsables conjoints de traitement, repartissant clairement les rôles et responsabilités de chacun

Désigner un DPO, est-ce un moyen de se libérer de la contrainte réglementaire, en confiant la responsabilité, de fait, à un expert ?

Clairement, Non ! La fonction de DPO est d'abord une fonction de conseil, et potentiellement une fonction de capitalisation, mais en aucune manière elle n'est le réceptacle des responsabilites de l'organisation qui l'a désigné
Au contraire, le DPO est protégé par une immunité qui l'empêche d'être « *relevé de ses fonctions ou pénalisé* » par l'organisation l'ayant designé, du fait de « *l'exercice de ses fonctions* » *(Règl (UE) 2016/679, art 38 3)* Ainsi, l'organisation ne pourra pas sanctionner son DPO pour les prises de position adoptées dans le cadre de ses missions (V Lignes directrices adoptees par le G29, 13 dec 2016, a propos des DPO, *p 15*) Nommer un DPO (interne ou externe) ne permet pas de se libérer de la contrainte juridique

La liste des nouvelles obligations étant particulièrement dense, que faut-il faire en premier ?

La notion de « finalite » est la pierre angulaire de ce texte Tout traitement doit répondre a une finalité determinée et legitime, et porte sur un objet proportionné (c'est-à-dire uniquement sur des données et des moyens strictement nécessaires à la mise en œuvre de la finalité). Par « finalité », il faut entendre « *la raison spécifique pour laquelle les données sont traitees le but ou l'intention de leur traitement* » (V *G29, avis 06/2014, 9 avr 2014, p 26*) L'analyse necessite aussi de définir les acteurs du traitement ceux qui décident des finalités (les responsables de traitement), ceux qui mettent en œuvre les moyens de traitement (les sous-traitants) et ceux qui reçoivent les données (les destinataires) Ce sont toutes ces parties-prenantes qu'il faut qualifier La finalité est donc le « pourquoi » du traitement, tandis que les données sont le « quoi », que les moyens de traitement sont le « comment » et que les parties-prenantes sont le « qui »
La finalite conditionne toute l'analyse de licéité du traitement Il est donc essentiel de commencer par bien identifier et formuler la finalité de chaque opération de traitement C'est une démarche finaliste qu'il faut adopter !

Sur le terrain, quelles difficultés constatez-vous et quelles en sont les causes ?

Sur le terrain, le spectre des organisations va des insouciants aux abattus Les premiers ne se decident pas à traiter le RGPD, soit qu'ils pensent que ce texte est destiné aux entreprises du numerique, soit qu'ils sous-estiment les enjeux Ce profil va diminuant, du fait de la médiatisation du RGPD
Les seconds sont saisis de désarroi devant l'apparente ampleur de la tâche, face a la faiblesse de leurs ressources, ou de leur expertise juridique Pour compenser, ces organisations ont tendance à « se jeter » sur le sujet, par des actions « tous azimuts », sans tenir compte de la necessaire approche finaliste a adopter
Cela se traduit souvent par une approche « Tout IT », guidée par des principes quantitatifs privilégiant l'inventaire de données ou de traitements Ce travail ne permet pas d'atteindre la conformité puisque celle-ci vise l'identification des finalités, non des traitements De même, l'approche « Tout Juri », guidée par le principe de précaution dont l'exageration immobilise l'activité et l'innovation, doit être evitee
Une autre approche, centrée sur l'analyse des operations métiers – desquelles se degagent les finalités – est possible C'est la seule qui soit valable et pérenne Ainsi une approche systémique est préférable à une approche symptomatique pour se mettre en conformité avec le RGPD

Qu'est-ce qui différencie l'approche symptomatique de l'approche systémique ?

Métaphoriquement, le reglement vous oblige a porter une lourde charge, mais vous avez mal au dos Pensez-vous qu'il vaut mieux prendre un antidouleur ou reprendre l'activité physique dont l'insuffisance est la reelle origine du mal ?
Avec l'approche symptomatique l'organisation se focalise sur les obligations imposees par le RGPD, en les considérant isolément, sans démarche d'ensemble, et en privilégiant le traitement des seules non-conformités apparentes qui, bien souvent, révelent des mauvaises pratiques structurelles qu'il faut réformer
Dans les faits et en simplifiant un peu, nous proposons une approche en deux temps et en trois dimensions
- Temps 1 gestion de l'existant (traitements et finalités en cours) ,
- Temps 2 le reste de la vie de votre organisation (nouveaux traitements et finalités) ,
- Dimension 1 l'analyse, soit l'aspect intellectuel ,
- Dimension 2 l'organisation, soit l'aspect rituel ,
- Dimension 3 l'outillage, soit l'aspect formel

Dans le temps 1, deux options
- l'extravagante approche symptomatique ou vous allez diligenter un inventaire global , cette option conduit a devoir absorber toutes les données présentes dans les serveurs de votre organisation pour identifier d'éventuelles données personnelles, pour ensuite identifier les traitements qui consomment ces enregistrements, pour finalement inventorier tout cela dans une base de données qui constituera le socle de votre registre, puis faire de même avec tous les dossiers « papier » et procédures manipulant humainement ces dossiers ,
- l'approche systémique qui privilégie le principe de parcimonie (Ockham) , cette option conduit à considérer que votre organisation connaît les principales opérations métiers qui produisent ou consomment des données personnelles et, donc, a naturellement commencer par l'analyse des finalités pouvant ressortir d'une série d'interview des principaux acteurs métiers Cela aura aussi l'avantage d'acculturer les rouages de votre organisation pour les transformer en acteurs de cette culture de protection des donnees privées
Il nous semble assez évident que seule la seconde approche permet d'identifier les traitements les plus à risques, ceux prioritaires dans la mise en conformité
Dans le temps 2, chaque procédure ou projet ou évolution de ceux-ci devra être soumis à un cadre regroupant les trois dimensions (GDPR *framework*) Le passage du temps 1 au temps 2 induit une transformation, l'incorporation des pratiques et instances nécessaires La donnée, parce que pervasive, requiert une approche organique, pluridisciplinaire, permettant de répondre aux différentes dimensions dans leur intégralité, afin d'éviter l'abandon du DPO, seul et depourvu de leviers d'actions dans l'organisation
Ainsi les organisations doivent se doter d'un cadre analytique et formel ainsi que de rôles et d'instances assurant la tenue des obligations réglementaires du RGPD La dimension organisationnelle et la dimension outillage sont definies et formalisees au sein du cadre L'approche analytique pourra être partiellement capitalisee dans les deux autres dimensions, mais recouvrira principalement un ensemble de compétences, d'usages et de bonnes pratiques issues de l'expérience et de la veille (métier, IT et juridique)
La formalisation (fiche de presentation de traitement, descriptions des parties-prenantes, fiche d'analyse de la finalite, metamodèle du registre aligné sur ces fiches, etc) sont les soutiens structurants facilitant la dimension analytique Leur simple usage, sans apport intellectuel, ne saurait pour autant garantir la conformité du traitement au regard de sa finalite Cet apport est la conjonction des contributions des parties-prenantes au traitement, qu'elles soient internes ou externes à l'entreprise, à l'organisation L'ensemble etant gere par le DPO et contrôlé par la direction juridique

- M. Bourgeois, Droit de la Donnée : LexisNexis, à paraître
- F. Régnier-Pécastaing, MDM, Enjeux et méthodes de la gestion des données : Dunod, 2008 (meilleur livre informatique de l'année)

Parution Septembre 2017