box

RGPD, le dossier pour tout comprendre

L'entrée en vigueur du RGPD (Règlement général sur la protection des données) au 24 mai 2018 va modifier en profondeur la façon dont les organisations conservent et gèrent leurs données, et celles de leurs clients.

A l'heure de la migration massive des données dans le cloud ce virage est d'autant plus complexe à négocier que le futur règlement induit des changements organisationnels, techniques et juridiques. Un bouleversement qui puise historiquement ses contraintes des accords successifs Safe Harbor et Privacy Shield, aux succès relatifs.

Découvrez en détail les nouvelles obligations qui s'imposent aux entreprises, et les étapes pour mener à bien un projet de mise en conformité au RGPD (GDPR, General Data Protection Regulation) dans votre structure. L'occasion aussi d'inverser le rapport de force avec les prestataires de cloud, si ce virage est bien négocié, voire même d'envisager un avantage concurrentiel.

En partenariat avec ZDNet.fr

Sommaire

Que va changer le RGPD ?

Le futur règlement européen va changer radicalement l'approche des entreprises en matière de traitement des données personnelles. A la place de la déclaration préalable à la Cnil, toute une série de nouvelles obligations s'imposeront à elles. Check-list.

« Avec le RGPD, nous entrons dans une nouvelle ère de la protection de la vie privée ». Pour Benjamin May, avocat associé du cabinet Aramis, le général de l'Union européenne sur la protection des données tournera définitivement la page de la directive de 1995 (95/46/CE). « Cette directive européenne est frappée d'obsolescence, la collecte et le traitement des données personnelles ayant fortement évolué depuis. » Le big data est passé par là.

S'agissant d'une directive, sa transposition a créé des disparités entre les Etats-membres. Par ailleurs, les sanctions ne sont guère dissuasives. Les 150 000 euros infligés à Google par la Cnil – le record de la Commission - ne représentent pas grand-chose pour ce dernier. Enfin, la directive de 1995 ne fait pas peser de responsabilité sur le sous-traitant.

Le RGPD (GDPR, General Data Protection Regulation) dont la rédaction a duré plusieurs années, entravée par les actions des lobbies, n'est plus une directive mais un règlement. Pas de transposition nationale, il sera applicable tel quel dès son entrée en vigueur le 25 mai 2018. Laissant deux ans aux entreprises pour se préparer. La Cnil a publié un FAQ à leur attention.

Des amendes allant jusqu'à 4 % du chiffre d'affaires

Si le RGPD reprend la définition des données personnelles de la directive de 1995 - toutes les informations qui identifient une personne physique (et non morale comme en Suisse) – il vise à contraindre les entreprises à prendre leurs traitements « enfin » au sérieux.

« En termes de sanction financière, l'enjeu de la privacy se hisse à la même hauteur que les délits de corruption et de cartel », rappelle Benjamin May. Pour les manquements les plus graves, le montant pourra atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial.

Pour le juriste, « le RGPD prévoit des obligations très précises et d'autres plus sujettes à interprétation ». Le règlement établit tout d'abord des obligations génériques. A commencer par le principe d'« accountability » qui responsabilise l'entreprise. Elle devient garante du respect de la vie privée. La déclaration préalable à la Cnil est supprimée, remplacée par l'obligation de tenir un registre.

Dans ce registre, on y consigne les mêmes informations que dans la déclaration mais en inversant la charge de la preuve. Avant, la Cnil devait démontrer les manquements et le responsable du traitement avait du temps pour régulariser. Demain, cela sera à l'entreprise de démontrer qu'elle est en conformité. « Les entreprises ayant généralement au moins une dizaine de traitements, elles doivent se préparer dès maintenant à la tenue de ce registre », conseille Benjamin May.

Le RGDP introduit aussi une obligation de notification par les responsables de traitement en cas de violations de données à caractère personnel (data breach). Ils doivent alerter la Cnil dans les meilleurs délais, si possible dans les 72 heures après en avoir pris connaissance.

Consentement express et spécifique de l'utilisateur

Autre obligation, le « privacy by design ». Il s'agit de prendre en compte la notion du respect de la vie privée dès la conception d'un système d'information, d'une base de données, d'une application. Une application insuffisamment sécurisée ne serait donc pas conforme. « Cette obligation de « privacy by design » laisse donc une large marge d'interprétation », estime Benjamin May. Avec le « privacy by defaut », l'entreprise doit placer le curseur sur le niveau le plus élevé en termes de protection de la vie privée. Chaque fois qu'elle initie un traitement, elle doit obtenir le consentement express (opt-in) et spécifique de l'utilisateur.

Prenons l'exemple d'une application mobile pour VTC. Lors de son installation, elle va chercher des données personnelles dans votre smartphone et demander à accéder à vos contacts et à votre agenda via un pop-up. Si vous n'acceptez pas, vous n'accédez pas au service. Pourtant, ces informations ne sont pas nécessaires à la fourniture du service en question. Demain, ce cas de figure ne sera plus possible, la collecte de données devant servir la finalité du service. Il faudra, par ailleurs, un formulaire de consentement différent pour chaque type de données. Au risque de pousser 25 pop-up lors de l'installation.

Dernière obligation, celle de nommer un DPO (data protection officer). Cette obligation s'applique aux établissements publics et aux entreprises qui effectuent des traitements sur des données sensibles ou des traitements à grande échelle. Une clinique ou une société de vidéosurveillance dont le respect de la vie privée est au cœur de leur activité sont concernés. « Mais, pour une entreprise lambda, les données de ses salariés ne rentrent pas dans le spectre », tempère Benjamin May. Et par traitement de masse, il faut entendre les clients d'une banque ou les données de géolocalisation.

Comment se préparer au RGPD ?

Les entreprises n'ont pas trop des deux ans laissés par l'Union européenne tant le futur règlement induit des changements organisationnels, techniques et juridiques. Une préparation qui passera par un certain nombre d'étapes.

Le compte à rebours est enclenché. Il reste environ 400 jours aux entreprises pour se préparer à l'entrée en vigueur du RGPD (GDPR, General Data Protection Regulation), le 25 mai 2018. Une période qui ne sera pas de trop tant la mise en place du futur règlement européen introduit des changements organisationnels, techniques et juridiques. Sur son site, la Cnil a résumé ce parcours du combattant en six étapes. Comme tout projet, il comprend des parties « build » et « run ».

Tout commence, pour les entreprises concernées, par la nomination d'un DPO (Data protection officer) ou DPD (Délégué à la protection des données) en bon français. Ce DPO sera une sorte de super Correspondant informatique & Libertés (CIL). Pour les entreprises qui ont un CIL, ce dernier est légitime à occuper cette fonction.

Véritable homme-orchestre, le DPO a toutefois un périmètre plus large. « Le CIL arrête la liste des traitements et s'assure de leur conformité. Le DPO va devoir, lui, savoir évaluer les risques », compare Florence Bonnet, directrice du cabinet TNP CIL Consulting. Ce qui suppose d'avoir une double culture de la gestion des risques et de la conformité mais aussi des compétences en IT et en sécurité.

Fonction transverse, le DPO a l'oreille attentive de la direction générale tout en étant indépendant. A la fois juge et partie, un chief data officer ou un RSSI ne peut occuper ce rôle. Qui alors pour incarner la fonction ? En décembre dernier, le G 29 – le groupe des « Cnil » européennes - a publié des « guidelines » qui précisent son profil et ses missions. Un groupe composé de filiales peut avoir un DPO. Il peut s'agir d'un salarié – il est alors salarié protégé - ou d'une personne extérieure (un juriste, par exemple).

Cartographier l'ensemble des traitements

Une fois le DPO nommé, place à l'état des lieux. L'ensemble des traitements de données personnelles doit être documenté. Cette documentation servira de base au futur registre. Quels sont les objectifs poursuivis ? Quels sont les acteurs internes et externes qui y ont accès ? Quelles sont l'origine et la destination des données ? Sont-elles transférées hors de l'Union européenne ? Pour dresser cette cartographie, les métiers sont mis à contribution. Pour Benjamin May, avocat associé du cabinet Aramis, l'équipe projet doit avoir « l'appui de la direction générale qui va lui ouvrir toutes les portes ».

Une fois ces traitements identifiés, il s'agira d'expliciter les règles à appliquer qui différent selon le degré de criticité des données. Les traitements présentant des risques élevés pour les droits et libertés font l'objet d'une étude d'impact (Privacy Impact Assessment en anglais ou PIA). Quelles sont les mesures organisationnelles (personnes habilitées) et sécuritaires (anonymisation, chiffrement…) à mettre en place ? Dépendant de la finalité du traitement, la durée de la conservation des données doit être également établie. Les données seront-elles ensuite archivées ou supprimées ?

Etablir la chaîne de responsabilité

Sur la partie « run », l'équipe projet doit dérouler son plan d'actions pour se mettre en conformité. Cela passe notamment par la révision de la politique de confidentialité ou des modalités d'exercice des droits (droit d'accès, de rectification, droit à la portabilité, retrait du consentement…). Il s'agit aussi de passer en revue les contrats des sous-traitants afin d'insérer des clauses précisant leurs nouvelles obligations et responsabilités.

Enfin, il faut poser le cadre de gouvernance. A savoir dresser l'ensemble des processus internes qui vont garantir l'intégrité et la protection des données tout au long de la vie d'un traitement. Comment prendre en compte cette protection dès la conception d'un traitement ? Comment seront traitées les demandes des personnes faisant valoir l'exercice de leurs droits ? En cas de violation, quelle est la chaîne de responsabilité ? Durant tout le projet, l'équipe dédiée, et en particulier le DPO, doit évangéliser en interne et sensibiliser les collaborateurs aux enjeux du RGPD. Benjamin May observe une grande disparité dans l'état d'avancement. « Les grands comptes ont déjà lancé leur projet de compliance qui mobilise de 20 à 30 personnes aux compétences variées. Faute de ressources en interne, les ETI font appel à des intervenants extérieurs. Les PME, elles, ne sont tout simplement pas informées du sujet. » Pour sa part, Florence Bonnet observe une prise de conscience qui va crescendo depuis le début de l'année. « On assiste déjà à une pénurie de compétences. Certaines entreprises attendent la rentrée pour se lancer, c'est un mauvais pari. »

Safe Harbor, pourquoi cela n'a pas marché ?

En octobre 2015, la Cour de justice de l'Union européenne invalidait l'accord Safe Harbor encadrant le transfert des données personnelles vers les Etats-Unis. Dans le prolongement de l'affaire Prism, elle mettait fin à un système n'offrant pas de garanties suffisantes. Flash-back.

C'est donc un autrichien de 27 ans qui a fait tomber le Safe Harbor, le cadre juridique qui a régenté des années durant le transfert des données personnelles vers les Etats-Unis. Après avoir découvert l'ampleur de la collecte de données effectuée par Facebook, Maximilian Schrems avait saisi la Cour de justice de l'Union Européenne (CJUE) qui lui a donné raison.

Dans son arrêt du 6 octobre 2015, la CJUE a estimé que les autorités publiques américaines pouvaient accéder de manière massive et indifférenciée aux données transférées, sans assurer de protection juridique efficace aux personnes concernées.

Onze mois plus tôt, la Cnil et ses homologues européennes du G29, avait attiré l'attention, dans un épais document, sur le caractère disproportionné de cette collecte massive et indifférenciée de données permise par la législation américaine. En 2013, Edward Snowden avait préparé le terrain en révélant aux yeux du monde le programme américain de surveillance électronique Prism.

Des prestataires auto-certifiés

Négociés entre les autorités américaines et la Commission européenne en 2000, les principes régissant Safe Harbor ou « sphère de sécurité » étaient assez sommaires. Dans l'esprit de la directive européenne de 1995, le texte accordait la possibilité à un citoyen européen de s'opposer à un transfert ou à une utilisation des données pour des finalités différentes.

Le responsable du traitement de données sensibles devait recueillir le consentement explicite de l'intéressé, lui accorder un droit d'accès et de rectification, et assurer un niveau de protection des données suffisant. Directrice du cabinet TNP CIL Consulting, Florence Bonnet ne regrette pas la fin du Safe Harbor. « C'était un système d'auto-déclaration. Selon leur bon vouloir, les entreprises pouvaient se certifier et appliquer ou non les règles. » Les mesures de contrôles relevant de la Federal Trade Commission étaient notoirement insuffisantes. « De leur côté, les citoyens n'avaient pas véritablement les moyens d'obtenir réparation. »

Coup dur pour les acteurs du cloud américain

L'arrêt de Safe Harbor a toutefois été un coup dur pour les quelque 5 000 entreprises certifiées dont Microsoft Azure, Amazon Web Services, Google ou Facebook. Elles perdaient du jour au lendemain le cadre juridique régissant leurs activités européennes. Pendant la période transitoire, la Cnil recommandait alors de recourir aux clauses contractuelles types de l'Union européenne ou aux Règles internes d'entreprises (BCR).

L'affaire des écoutes de la NSA avait déjà mis à mal l'industrie du cloud américain Une étude conduite par l'Information Technology and Innovation Foundation (Itif) chiffrait à 31 milliards de dollars les pertes pour les prestataires de cloud outre-Atlantique suite à l'affaire Prism. Dans une autre étude de 2014 menée cette fois par le cabinet Vanson Bourne, 97 % des DSI français disaient préférer contracter avec un prestataire européen.

Et pour cause, par effet dominos, une entreprise européenne ayant utilisé un service américain pour héberger les données personnelles de ses clients ou de ses salariés pouvait être la cible de poursuites. La localisation de données sur le vieux Continent par l'implantation de datacenters en Europe par ces fournisseurs ne résolvait qu'une partie du problème.

Privacy Shield, où en est-on ?

Successeur du Safe Harbor, le Privacy Shield encadre le transfert des données personnelles vers les Etats-Unis. Controversé dès son entrée en vigueur en août dernier, il pourrait être amendé dans quelques mois.

Depuis 1er août 2016, le Privacy Shield encadre les transferts des données personnelles vers les États-Unis. Une entreprise française souhaitant recourir à un prestataire établi outre-Atlantique peut vérifier sur le site dédié s'il remplit les conditions établies par l'Administration américaine.

Le Privacy Shield remplace un autre texte, le Safe Harbour, invalidé par la Cour de justice de l'Union européenne en octobre 2015. Sans toutefois régler tous les problèmes que soulevait le précédent accord. Pour Florence Bonnet directrice du cabinet TNP CIL Consulting, « le Privacy Shield a apporté des avancées majeures en proposant plus de contrôles, une révision annuelle, mais reste insuffisant. Comme pour le Safe Harbor, l'accord repose sur de l'auto-déclaration. Pour être certifié, un fournisseur n'a qu'à remplir un questionnaire. »

Les limites de l'auto-certification

Les prestataires auto-certifiés s'engagent à respecter sept grands principes. Ils sont d'abord tenus à informer les personnes du traitement de données les concernant et à publier leur politique de confidentialité. Ils doivent garantir que les données sont fiables, à jour, exactes et en accord avec la finalité prévue lors de leur collecte.

Un citoyen européen peut s'opposer au traitement si cette finalité vient à changer. Il a le droit de corriger ou de supprimer les données inexactes ou traitées en violation du Privacy Shield. Le principe de sécurité impose, lui, aux entreprises adhérentes de prendre « les mesures raisonnables et appropriées » pour assurer la protection des données personnelles.

En cas de litige, un résident européen a plusieurs possibilités. Il peut porter plainte auprès de la société concernée qui devra répondre dans les 45 jours. L'accord prévoit des mécanismes de résolution des litiges sans frais pour le plaignant. Ce dernier peut aussi s'adresser à la Cnil qui adressera sa plainte à la Federal Trade Commission (FTC), l'agence en charge de la supervision du Privacy Shield.

Pour ce qui relève de la sécurité nationale, le Privacy Shield prévoit l'intervention d'un médiateur. Cet « ombudsperson » est indépendant des services de renseignement mais sous l'autorité du Secrétaire d'Etat américain. « Ce qui ne garantit pas son indépendance, soulève Florence Bonnet. Il se contentera, par ailleurs, de confirmer ou d'infirmer la violation mais sans se prononcer sur une éventuelle existence d'activité de surveillance. »

La révision annuelle, l'heure de vérité

Comme on le voit, le texte soulève un certain nombre d'interrogations. En juillet, avant même son entrée en vigueur, le G29, le groupement des « Cnil » européennes avait, dans un communiqué, listé ses lacunes. Depuis, les attaques contre le « bouclier » n'ont cessé. Les défenseurs irlandais des droits numériques de « Digital Rights Ireland » et l'association française La Quadrature du Net ont attaqué le texte en justice.

En février, un groupe d'ONG - dont à nouveau La Quadrature du Net - appelait dans une lettre ouverte à suspendre le Privacy Shield, « loi inadaptée pour protéger les données des européens », ne satisfaisant pas au critère d'« équivalence substantielle » tel que l'avait défini la Cour de justice de l'Union européenne lors de l'invalidation du Safe Harbor. Candidat à l'élection présidentielle, Emmanuel Macron s'engage, lui, dans son programme, à renégocier l'accord avec les Etats-Unis d'ici 2018.

Le décret « anti-immigrés » publié par l'administration Trump a laissé planer le doute d'une possible restriction de la protection des données personnelles. A tort, car il ne s'applique pas aux citoyens européens. Non, l'avenir du Privacy Shield se jouera dans quelques mois lors de la révision annuelle de l'accord où le G29 compte faire une évaluation sans concession.

En attendant, la Cnil rappelle qu'une entreprise peut recourir aux autres cadres juridiques pour transférer ses données hors de l'Union européenne comme les clauses contractuelles type de la Commission européenne ou les règles d'entreprises contraignantes (« Binding corporate rules» ou BCR).

Enfin, notons que les prestataires dont l'activité sera soumise au RGPD (GDPR, General Data Protection Regulation) ne pourront se prévaloir de leur adhésion au Privacy Shield pour démontrer leur conformité au règlement européen.

Privacy Shield : un enjeu majeur pour la compliance

Le flou qui entoure aujourd'hui le cadre réglementaire du transfert de données personnelles oblige les entreprises à se positionner. Et dans ce cadre incertain, il est essentiel de s'appuyer sur des solutions pleinement maîtrisées.

Tafta, TTIP, Safe Harbour, Privacy Shield et maintenant la nouvelle Réglementantion générale sur la protection des données personnelles (GDPR), les échanges commerciaux entre l'Europe et les Etats-Unis sont au cœur de l'actualité économique. En jeu : la définition d'un cadre légal et pérenne aux transferts de données entre entreprises européennes et américaines. Cette zone de turbulences est aujourd'hui tellement diffuse qu'il peut paraître complexe de définir l'attitude à adopter. Une chose est sûre : quelle que soit leur nationalité, les acteurs économiques des deux ensembles vont devoir se soumettre à un nouvel arsenal réglementaire. Résumons :

- Depuis 1998, c'est le Safe Harbor qui régulait les échanges de données personnelles. Pour pouvoir transférer de telles données de l'Europe vers les Etats-Unis, les entreprises demandeuses devaient être certifiées par un organisme indépendant.
- En octobre 2015, la Cour de justice de l'Union européenne invalide l'accord Safe Harbor. La Cour considère que les États-Unis n'offrent pas un niveau de protection adéquat aux données personnelles transférées.
- Le successeur de Safe Harbor est le Privacy Shield, qui a été adopté par la plupart des états membres en juillet 2016.
- A tout cela s'ajoute la nouvelle GDPR qui entrera en application le 25 Mai 2018 et qui imposera plusieurs obligations à toutes les entreprises gérant des données personnelles avec des sanctions plutôt lourdes en cas de violation de la loi.

L'intérim BCR

Compliqué ? Ce n'est qu'un début. Car non seulement il reste à vérifier si la validité du Privacy Shield résistera à la revue des Cours européennes, mais dans l'intervalle, ce sont d'autres référentiels, comme les BCR (Binding Corporate Rules, également citées dans le GPDR), qui offrent plus de solidité, qui doivent s'appliquer pour éviter tout vide juridique.

Dans ce contexte flou, les entreprises doivent néanmoins se positionner rapidement. L'implémentation du GDPR est en effet un processus long, et on estime que 91% des entreprises qui n'ont pas déjà entamé le travail ne seront pas conformes lors de la mise en place de l'accord en 2018. Au risque d'être exposées aux sanctions pouvant aller jusqu'à 20 millions d'Euros ou jusqu'à 4% de leur revenus annuels.

Box : le Privacy by Design

Toute entreprise désireuse de se mettre en conformité avec les référentiels actuels et futurs pour ne pas entraver son business doit donc envisager rapidement sa politique globale de sécurité et de gouvernance.

C'est tout l'enjeu de Box, qui a fait le choix du «Privacy by Design » en portant pour le compte de ses clients tous les enjeux de conformité contemporain et RGPD. Déjà certifié BCR, la solution Box vient en effet d'obtenir le Privacy Shield sur l'ensemble de son offre. Pour nos clients, c'est la certitude de demeurer en totale conformité avec les différents référentiels majeurs du marché sans avoir à prendre en charge le lourd processus de certification et de déclaration, et en gardant un contrôle étroit sur leurs données.
En outre, Box se positionne comme un véritable partenaire pour ses clients dans cette étape cruciale : parce que le patrimoine informationnel de nos utilisateurs constitue leur principal actif, nous travaillons avec des cabinets indépendants pour les aider à évaluer leur exposition au risque et identifier les perspectives du déploiement d'une solution cloud dans ce nouveau paysage sécuritaire mondial.

Jérémy Grinbaum, VP France et Europe du sud, Box

Que doit contenir un contrat cloud « idéal » ?

Les prestataires de cloud sortent difficilement de leurs contrats-type. Pour autant la pression concurrentielle et réglementaire offre de nouvelles marges de négociations. Le RGPD peut notamment aider à inverser le rapport de force.

Quelle marge de négociation contractuelle dispose une entreprise qui s'apprête à confier tout ou partie de ses données à un prestataire de cloud ? En principe, aucune. A la base, un contrat cloud est un contrat d'adhésion. Un contrat-type à prendre ou à laisser (« take it or leave it »).

Afin de proposer une offre « scalable » à bas coût, les fournisseurs ont poussé très loin les concepts de standardisation et de mutualisation. Faire du sur-mesure remettrait en cause leur modèle économique.

Toutefois, la situation évolue favorablement ces dernières années. La pression concurrentielle aidant, les offreurs font du respect de normes telles que ISO 27001 et 27018 dédiées à la sécurisation des données un argument commercial. La jurisprudence a aussi rappelé l'entreprise utilisatrice à ses devoirs. L'arrêt du Conseil Etat du 30 décembre 2015 a confirmé l'obligation du responsable de traitement de données à caractères personnelles – en l'occurrence Orange - de prendre des mesures afin de s'assurer que les données confiées à un sous-traitant soient sécurisées.

Mais c'est surtout le RGPD, Règlement européen consacré à la protection des données personnelles, qui va encadrer la relation entre les deux parties. « S'il n'entrera en vigueur qu'en mai 2018, il indique tout ce qui doit se trouver dans un contrat cloud », estime Eric Le Quellenec, avocat, directeur du département informatique conseil du cabinet Alain Bensoussan Lexing. En particulier, l'article 28-3 qui fait obligation au client d'informer son prestataire de la finalité du traitement et de la nature des données. Au sous-traitant de mettre en regard les ressources techniques et organisationnelles ad hoc pour en assurer la protection.

Les 3 grands principes du RGPD

Le RGPD repose sur quelques grands principes. Le premier principe porte sur le « privacy by design ». L'ensemble des infrastructures matérielles et logicielles utilisé par les providers pour fournir leurs services, doivent intégrer nativement des mécanismes de protection des données personnelles. Cette notion à l'œuvre pour certaines professions réglementées - données médicales hébergées chez des prestataires agréés, stockage des données bancaires répondant à la norme PCI-DSS - s'appliquera à tous.

Le deuxième principe, c'est le « security by default ». Non seulement la donnée est protégée nativement, mais le prestataire cloud doit assurer un traitement sélectif des données personnelles afin que ne soit traitée que la donnée nécessaire à la finalité poursuivie, et seulement cette donnée (principe de « minimalisation »). Seuls les employés du sous-traitant habilités à cette gestion des données sont autorisés y accéder.
Troisième principe : l'« accountability » (responsabilité). Le provider cloud doit faire la preuve à tout moment qu'il répond aux exigences de protection des données au regard des demandes de la Cnil. Le devoir de communication en cas de violation de la sécurité et de fuite des données implique qu'il tienne des registres retraçant les principes de sécurisation qui s'appliquent au service cloud tout au long de son cycle de vie.

Coresponsable de la sanction financière

Le RGPD introduit surtout une coresponsabilité entre les parties sur lequel peut jouer le contractant. Car c'est le responsable de traitement et lui seul qui en cas de fuite de données peut se voir infliger une sanction financière pouvant aller jusqu'à 4 % de son chiffre d'affaires mondial.
Pour Thomas Beaugrand, associé du cabinet Staub & Associés, il est possible pour un grand compte de négocier un déplafonnement de la responsabilité de son sous-traitant. « Si la faute de l'incident lui incombe, il sera exposé à des pénalités financières d'autant plus lourdes qu'elles ne seront plus plafonnées dans son contrat. »

Une entreprise en position de force peut aussi inclure une clause audit. Difficile à obtenir, elle peut être limitée à une visite annuelle du datacenter à date fixe. A défaut, Eric Le Quellenec suggère de renforcer les pénalités financières en cas manquement aux engagements qualité (SLA).

De son côté, Thomas Beaugrand conseille de stipuler une clause de « rendez-vous ». Des jalons pour mesurer, d'ici mai 2018, où en sont les deux parties dans l'implémentation des règles technico-juridiques du RGPD. Le prestataire doit notamment communiquer son plan d'action et son un rétro planning. « C'est aussi un levier de négociation. »
En ce qui concerne les entreprises françaises contractant avec des prestataires américains, il ne faut pas, selon lui, s'en tenir au « Privacy Shield » qui comme son prédécesseur « Safe Harbor » repose sur leurs seules déclarations. « On reste dans l'auto-certification. » Il recommande de leur faire signer les clauses contractuelles types de la Commission européenne, et de les compléter par des exigences contractuelles spécifiques issues du RGPD.

Enfin, il faut gérer la fin du contrat, sujet sur lequel le RGPD ne s'étend pas. Il s'agit de prévoir et organiser la réversibilité, s'assurer de la suppression des données chez l'ancien prestataire.

Quelles données mettre dans le cloud ?

Le passage au cloud pose la question de la criticité des données. Comment arbitrer entre les données à conserver en interne et celles éligibles à monter dans le nuage. Les métiers sont mis à contribution pour réaliser cette classification.

Depuis l'essor du cloud, une entreprise doit régulièrement se poser la question. Quelles sont les données à conserver en interne et celles qui peuvent être massivement externalisées dans le nuage ? La mise en œuvre du RGPD rend encore plus incontournable cet arbitrage puisque les règles de gestion qui s'appliquent derrière sont appelées à être automatisées.

Pour Thomas Beaugrand, associé du cabinet Staub & Associés, une analyse préalable d'impacts sera obligatoire dans certains cas. « La question se posera pour un traitement de masse de données personnelles de type big data ou des traitements de données dites sensibles liées, à l'orientation sexuelle et politique d'un individu ou à son origine ethnique.» Le caractère sensible d'une donnée (data sensibility) intervient parfois de façon indirecte, telles données de santé d'un individu pouvant, par exemple avoir un impact sur l'exécution de son contrat d'assurance.
L'analyse d'impacts conditionnera les choix opérés par l'entreprise sur la base des préconisations de son prestataire cloud. Elle doit répondre à un certain nombre de questions. Doit-on ou non collecter ces données compte tenu du risque qu'elles représentent pour les personnes physiques ? Est-ce que ces données sont indispensables aux activités de l'entreprise en matière notamment de prospection ou de ciblage ?

Quelles règles métiers appliquer ?

Pour dresser cet inventaire, les métiers sont mis à contribution. Il s'agit d'évaluer leur « niveau de douleur » en cas de perte de confidentialité sur ce type de données. « Quel serait l'impact financier, juridique et en termes d'image ? », questionne Lionel Prades, consultant senior sécurité gouvernance et gestion des risques chez Orange Cyberdefense. Entre les données des directions financières et commerciales, ou celles émanant de la R&D et de production, le ressenti diffère.

Ensuite, il convient de définir les sphères de diffusion propres à une organisation. Qui partage quoi et sous quelle forme ? « Une fois cette cartographie établie, on peut décider qu'une information ne sera accessible qu'à un service, à un groupe limité (confidentiel) voire à un seul individu (secret). »

La mise en place d'une solution de DLP (Data Loss Protection) qui va tracer en continu les données sensibles peut participer à cette définition des règles métiers. «Une série d'entretiens avec les métiers permettra de savoir, service par service, quels sont les modèles de documents (templates) utilisés et les mots-clés qui caractérisent la confidentialité, avance Yann Cam, consultant sécurité à la société de conseil Synetis. Tel fichier Excel ne pourra être imprimé, envoyé vers une boîte aux lettres inconnue, enregistré sur une clé USB ou partir vers un espace de stockage en ligne. »

Une fois les règles posées, il faut s'assurer qu'elles ne sont pas contournées. Une politique de gouvernance menée conjointement par la gestion des risques, la DSI et – quand il y en a un – le CIL/DPO (Correspondant Informatique & Libertés, Data Protection Officer) va garantir la conformité du traitement des données dans la durée.

Hébergement on-premise versus cloud

Pour Lionel Prades, « le cloud ne change pas radicalement l'exposition aux risques. Tout dépend de la confiance placée dans le prestataire et du niveau de sécurisation souhaité dans le contrôle d'accès, la traçabilité des données, leur chiffrement, leur anonymisation. A chaque menace, il y a un dispositif de protection qui correspond. »

Selon lui, un hébergeur a un savoir-faire dans la sécurisation des données ou le patch management que n'a pas une entreprise privée. Surtout s'il prévaut du respect de normes comme ISO 27018. « Sur des données sociales et RH, il vaut parfois mieux qu'elles soient dehors que dedans. »
Le surcoût lié à la protection peut toutefois rendre le cloud plus cher qu'un hébergement maison. Accepte-t-on d'aller sur un serveur mutualisé ou, à l'inverse, choisit-on un hébergement ultra individualisé où ce sont ses propres serveurs qui sont enfermés dans une cage ? « Peut-on alors encore parler de cloud ? », s'interroge Lionel Prades.

La conformité, un avantage compétitif

Du côté des fournisseurs comme des entreprises, garantir la vie privée des utilisateurs au travers de certifications peut être vu comme un atout concurrentiel. De nouveaux modèles économiques devraient aussi émerger autour de la « privacy ».

Contrainte ou opportunité ? La question se pose pour chaque chantier réglementaire. Le RGPD (GDPR, General Data Protection Regulation) n'échappe à la règle. Au fur et à mesure que les travaux autour de sa rédaction avançaient, des prestataires européens ont crié à la concurrence faussée. Plus contraignant que la directive européenne de 1995, le nouveau règlement européen présenterait, à leurs yeux, un désavantage concurrentiel par rapport à leurs concurrents, principalement américains.

Même son de cloche du côté de leurs clients. Selon une étude menée en 2015 par le cabinet Vanson Bourne, et commandée par Ipswitch, deux tiers des entreprises françaises estimaient que la mise en conformité au RGPD constituait un fardeau financier. Au regard des investissements en technologies à consentir et des nouveaux services à créer.

Le RGPD a pourtant pour principale vertu de rappeler combien la protection des données personnelles est importante. Une fuite de données peut avoir des conséquences qui vont bien au-delà des lourdes sanctions prévues par le règlement. « La négligence de Yahoo ! lui a fait perdre 500 millions de dollars de valorisation de cession, et lui a causé un préjudice d'image difficilement quantifiable », argue Thomas Beaugrand, associé du cabinet Staub & Associés.

Des services cloud « privacy friendly »

Le prestataire, sous-traitant d'un service potentiellement défectueux, ne peut pas se désintéresser du problème. Si des acteurs chinois et américains se moquent éperdument du sujet, « d'autres prestataires constatent que la protection des données devient un argument commercial essentiel, à l'instar de la protection de l'environnement ou du respect de standards sociaux », poursuit le juriste. Ils peuvent avancer que leurs services cloud sont « privacy friendly », et respectent le plus haut standard légal en la matière. Sur les sites, des fournisseurs affichent d'ailleurs leur future compatibilité avec le RGPD.

En attendant d'avoir le label de la Cnil, comme le prévoit le texte. « Il y aura un rehaussement du marché, un écrémage des acteurs qui ne seront pas conformes, une distinction concurrentielle fondée sur l'effectivité de la protection des données personnelles et de la conformité au règlement », estime Thomas Beaugrand.

Ce tampon pourrait devenir indispensable pour les grands comptes mais aussi pour les petites entreprises qui vont aller chercher l'expertise en externe et s'en remettent davantage encore à leurs prestataires cloud, au risque de renforcer leur dépendance.

Beaucoup de prestataires étrangers se conforment déjà aux exigences de la législation européenne, via la signature avec leurs clients européens des Clauses contractuelles types de l'Union européenne quand il y a des flux transfrontaliers de données. En matière de sécurisation des données, les normes qualité ISO 27001 ou ISO 27017 deviennent incontournables.

Moins courue, ISO 27018 :2014 concerne pourtant directement la protection des données personnelles dans le cloud. Le provider s'engage à ne pas utiliser ces données à des fins de marketing ou de publicité, à fournir une transparence sur la manière dont les données sont stockées, à communiquer avec l'utilisateur en cas de faille de sécurité.

L'internaute reprend le contrôle de ses données

Du côté des entreprises, Florence Bonnet, directrice du cabinet TNP CIL Consulting, estime que la protection des données personnelles devient un avantage compétitif pour les sociétés spécialisées dans le profilage, le marketing digital. « L'Europe va leur offrir un cadre stable, c'est une vraie force. »

Elle prédit aussi l'émergence « de nouveaux modèles économiques qui vont se bâtir sur la confiance et la transparence. Des services seront « privacy compliant » comme il y a des produits bancaires éthiques. » Au risque d'arriver à des modèles payants garantissant la vie privée, limités aux personnes qui en ont les moyens.

On peut aussi imaginer des formes d'interactions plus positives dans le sillage du mouvement MyData ou de l'expérimentation MesInfos de la Fondation Internet Nouvelle Génération (Fing). Dans ce mode « self data », l'utilisateur reprend le contrôle de ses données. Libre à lui de les exploiter lui-même ou de les confier aux marques de son choix dans un rapport rééquilibré.

Le DPO en 4 questions

D'ici à un an, le délégué à la protection des données va faire son entrée dans les entreprises. Qui est-il ? Quelles sont ses attributions ? Voici les clés pour l'accueillir au mieux.

Vous avez jusqu'en mai 2018 pour le recruter ou le former. À cette date, le nouveau règlement général sur la protection des données (RGPD) (GDPR, General Data Protection Regulation) entrera en vigueur dans l'Union européenne et imposera à certaines organisations la nomination d'un délégué à la protection des données, ou DPO (Data Protection Officer). Explications.

La désignation d'un DPO est-elle obligatoire ?

Tous les organismes publics doivent obligatoirement avoir nommé un DPO d'ici à mai 2018. Mais c'est également le cas pour toutes les entreprises qui réalisent « un suivi régulier et systématique des personnes à grande échelle » ou qui traitent à grande échelle « des données dites « sensibles » ou relatives à des condamnations pénales et infractions », selon le texte du RGPD. De nombreuses sociétés sont donc potentiellement concernées dans la banque, l'assurance, la santé, les télécommunications, ou encore le marketing. Le G29, qui regroupe les différentes CNIL européennes, détaille les lignes directrices de cette obligation dans un document publié sur le site de la commission européenne. Pour les autres organisations, même si rien ne les y oblige, le G29 les encourage néanmoins à suivre cette même démarche.

Qui peut remplir cette fonction

Avant toute chose, si le RSSI (Responsable de la Sécurité des Systèmes d'Information) peut éventuellement se voir confier la casquette supplémentaire de DPO, ce dernier ne doit pas être vu comme son successeur. Dès lors que l'on évoque la sécurité des données, il est tout naturel de se tourner vers le RSSI. Mais le DPO a un rôle bien spécifique puisqu'il est le garant de la conformité. Alors que le RSSI veille à la mise en place des solutions techniques de sécurité adéquates, le DPO

s'assure du respect des législations et réglementations en vigueur et devient l'interlocuteur privilégié des autorités de contrôle. Il doit donc disposer de solides compétences juridiques. Le DPO peut cumuler cette fonction avec un autre rôle dans l'entreprise, mais ne doit pas être en situation de conflit d'intérêts. Un directeur marketing par exemple, dont la mission repose sur l'exploitation des données clients, pourrait avoir du mal à imposer des règles qui constitueraient des contraintes pour sa propre activité. Les entreprises qui ont déjà un CIL (Correspondant Informatique et Libertés) dans leur équipe pourront légitimement le faire évoluer vers un rôle de DPO.

Quel est son champ d'action

Le délégué à la protection des données aura en premier lieu un rôle de conseil. Familier des réglementations propres à son activité, aux législations nationales et aux directives internationales, il saura aiguiller son entreprise pour faire les bons choix. Dans un établissement de santé, il saura par exemple vérifier la certification HIPAA d'un fournisseur. Mais il devra également être positionné à un échelon hiérarchique suffisant et obtenir les ressources financières et humaines nécessaires pour devenir une autorité de contrôle indépendante. C'est lui qui devra inventorier et évaluer les traitements de données personnelles dans l'entreprise, et mettre en place la politique de protection adaptée.

Comment faciliter son intégration

La mission du DPO fait que, comme le RSSI, il risque d'être confronté à des utilisateurs peu enclins à accepter des contraintes de protection qui affectent leur productivité. Sa mission comportera donc un volet essentiel sur la sensibilisation aux bonnes pratiques, mais également sur la création d'un environnement de travail conjuguant conformité et efficacité. À l'heure du cloud et de la mobilité, la fonction de DPO ne peut se limiter à interdire des usages déjà largement ancrés dans le quotidien des professionnels. Il devra au contraire accompagner l'évolution des méthodes de travail en permettant aux entreprises de profiter des nouvelles opportunités du numérique sans exposer les données à des failles de sécurité et donc à des risques de fuite. C'est pourquoi, en collaboration étroite avec le DSI et le RSSI, il orientera les choix technologiques vers des solutions offrant de solides capacités de gouvernance et respectant par exemple les principes de « Privacy by Design ».

Safe Harbor, Privacy Shield, Brexit… Comment suivre la valse réglementaire

Dans un contexte de négociations tendues sur la protection des données, générateur de normes de plus en plus complexes à appréhender, sur quel référentiel s'appuyer pour ne pas se mettre en défaut vis-à-vis du régulateur et bâtir l'avenir ?

Le couperet est tombé le 6 octobre 2015. Deux ans après les révélations d'Edward Snowden sur les pratiques de surveillance de l'Agence Nationale de Sécurité américaine (NSA), la Cour de Justice européenne met un terme au Safe Harbor. Cet accord entre les États-Unis et l'Union européenne permettait aux entreprises américaines de transférer sur leur sol des données d'entreprises et de citoyens européens, à condition qu'elles respectent un niveau de protection et de confidentialité conforme aux normes européennes.

Pour le remplacer, le Privacy Shield est entré en vigueur en juillet 2016. Le principe général est une fois encore d'inciter les sociétés américaines à respecter les pratiques européennes en termes de « privacy », mêmes lorsque les données traversent l'Atlantique. Ce dernier intègre toutefois de nouvelles dispositions concernant l'accès aux données par l'administration américaine et renforce le pouvoir de contrôle et de sanction de la FTC (Federal Trade Commission, équivalent américain de la DGCCF française).

Cloud de proximité

Cet exemple de revirement réglementaire illustre toute la difficulté pour les entreprises européennes de confier leurs données à des fournisseurs américains. La question du traitement des données à l'extérieur des frontières de l'UE est toujours une préoccupation centrale et un frein majeur à l'adoption de technologies pourtant bénéfiques pour de nombreux professionnels. Et si la présence du fournisseur dans la Privacy Shield List reste pour l'heure une certification de référence pour les entreprises, des incertitudes demeurent quant à sa pérennité. Dès lors, à une époque où les données sont de plus en plus mobiles et hébergées dans le cloud, quelle stratégie adopter ? La réponse tient en un mot : localisation.

C'est en effet un argument de poids pour tout acteur du cloud : la possibilité pour le client de choisir l'emplacement géographique où seront stockées ses données. Outre l'aspect rassurant de savoir ses informations proches de soi, la localisation des données sur le sol européen répond aux obligations de nombreux secteurs (finance, santé, assurance, banque, etc.) dont les données sensibles ne peuvent quitter le territoire de l'UE. La première recommandation lors du déploiement d'une nouvelle solution est donc de vérifier la localisation du datacenter qui hébergera les données. Pour prendre le moins de risque possible vis-à-vis des régulateurs, celui-ci doit être situé chez un voisin européen.

Conforme aujourd'hui et demain

La plupart des fournisseurs ont bien compris cet enjeu aujourd'hui et proposent différentes localisations pour leurs services. C'est le cas par exemple de Box, spécialiste de la gestion de contenus dans le cloud. Avec ses « box zones », l'entreprise américaine offre à ses clients français la liberté d'opter pour un hébergement en Allemagne (Francfort), en Irlande (Dublin) ou en Angleterre (Londres). Ces derniers ont ainsi la garantie que leurs données ne traversent pas l'Atlantique, et ce y compris dans la mise en place d'un plan de reprise d'activité. Le scénario de sauvegarde peut inclure un stockage primaire à Francfort et un site secondaire à Dublin. Les organisations qui travaillent sur des marchés plus éloignés peuvent aussi accéder à des infrastructures au Japon, à Singapour, en Australie ou au Canada. Une possibilité qui, en plus d'offrir aux utilisateurs de faibles temps de latence pour accéder à leurs documents, permet également de prendre en compte les différentes réglementations locales.

Enfin, un autre point important à vérifier est la réversibilité. Pour être prêt à réagir rapidement à une évolution plus ou moins soudaine des réglementations, il convient de préciser avec son fournisseur les conditions de réversibilité dans le contrat de service. Car ce qui était conforme hier peut ne plus l'être demain. Le Brexit, par exemple, pourrait remettre en cause le Privacy Shield dans le Royaume-Uni. Dans un tel cas de figure, votre prestataire doit pouvoir vous accompagner dans la migration de vos données. Faire appel à un partenaire disposant d'infrastructures dans différents pays permettra de faciliter le transfert des informations vers une destination qui correspondra davantage à vos exigences.

Fiche Technique Box

Le moyen le plus facile pour travailler ensemble, partout !
Avec Box, tous les fichiers de vos équipes sont dans le cloud. Un moyen simple pour leur permettre d'accéder, éditer, commenter et partager tout type de fichier en temps réel, depuis n'importe quel terminal et en toute sécurité.

Une approche intégrée répondant aux préoccupations sur la confidentialité et la protection des données des clients internationaux.

1- Box est "GDPR ready"

Box a obtenu les BCR, la valeur de référence pour la protection des données
En Août 2016 Box a reçu les BCR (Binding Corporate Rules) en tant que contrôleur et processeur et peut légalement transférer les données depuis l'Europe et la zone Europe vers les Etats-Unis.

Le GDPR reconnait les BCR.
Grâce aux BCR, Box se positionne extrêmement bien pour adresser les GDPR (effectif en Mai 2018). Les BCR sont le seul instrument reconnu pour le transfert des données personnelles.

Les BCR reconnus dans de nombreux pays du monde.
Les BCR de Box ont été approuvés par: l'ICO du Royaume-Uni, la DPA espagnole, la DPA polonaise. Le PPC japonais reconnaît la valeur des BCR.

2 - L'approche de Box en matière de conformité globale

Conformité Externe

- Certifications étendues : internationales, spécifiques au pays, et axées sur des types de données spécifiques

Conformité Interne

- Audits internes indépendants des exigences en matière de protection des données
- Examen régulier des processus de protection des données : PIA, inventaire des données personnelles, avis, consentement
- Tests de pénétration et cycle de vie du développement logiciel sécurisé

Caractéristiques / Fonctionnalités

- Box Zones : Possibilité de stocker les données en région
- Box Governance : eDiscovery opposable, destruction contrôlée et conservation juridique
- Box KeySafe : possibilité donnée à l'entreprise de gérer ses propres clés de chiffrement, en plus du chiffrement des échanges et du stockage fourni par défaut

3 - Relations DPA (Data Protection Authority – Autorité de protection des données)

Relations proactives sur la confidentialité dans le cloud et la conformité aux DPA, avec:
- La CNIL (Commission Nationale de l'Informatique et des Libertés)
- ICO au Royaume Uni
- Autorité monétaire de Singapour
- DPA Bavarois
- PPC du Japon

Certifications et rapports complets en fonction des types de données et géographies.

ISO 27001
Norme mondiale pour la sécurité de l'information et le contrôle des systèmes

ISO 27018
Norme du fournisseur de services Cloud pour la gestion des informations personnelles identifiables (PII- Personally Identifiable Information)

SOC-1 et SOC-2 Type II
Rapports de tiers couvrant les principes de sécurité, de disponibilité et de confidentialité

TÜV Rheinland Certified Cloud Service
Certification pour la sécurité des données et la confidentialité

PCI Data Security Standard
La norme de sécurité de l'industrie des cartes de paiement. Conforme aux exigences du DSS (Data Security Standard) pour stocker l'information du titulaire de la carte en tant que fournisseur de services

HIPAA et HITECH
Plateforme de confiance pour PHI (**personal health information – Informations personnelles de santé**), PHR (Personal Health Records – Dossier personnel de santé) et recherche médicale

G-Cloud Framework
G-Cloud Framework - approuvé pour le partage des données officielles

FedRAMP
Programme fédéral des États-Unis pour l'évaluation de la sécurité, l'autorisation et le suivi des services Cloud

BCR (Binding Corporate Rules)
Règles d'entreprise contraignante approuvées en tant que processeur et contrôleur

FINRA / SEC 17a-4
Règle 17a-4 de la SEC sur la conservation des données financières

APEC CBPR
Certification répondant aux exigences de confidentialité transfrontalières régies par l'APEC (Asia Pacific Economic Cooperation – Coopération Economique Asie Pacifique)

C5
Catalogue des contrôles de conformité en matière de Cloud Computing

TCDP
Trusted Cloud Data Protection – Protection sécurisée des données dans le Cloud

À propos de Box

Box (NYSE: BOX) est l'entreprise de Gestion de Contenu d'Entreprise permettant aux organisations de révolutionner leur façon travailler en connectant de manière sécurisée les employés, les informations et les applications. Fondée en 2005, Box accompagne plus de 71000 entreprises à travers le monde telles que, Schneider Electric, GE, Eurostar et ICADE. Le siège de Box est situé à Redwood City en Californie et l'entreprise possède des bureaux aux Etats-Unis, en Europe et en Asie.

Pour en savoir plus : www.box.com