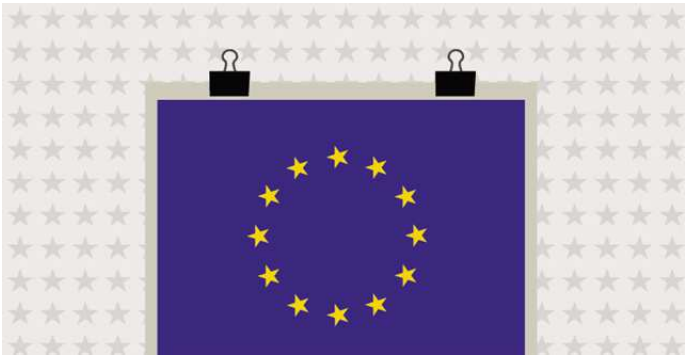
Information & technologies

RGPD, la conformité de dernière minute

À 15 jours de l'entrée en application du RGPD, les entreprises sont loin d'être conformes. Quelques mesures pour prouver sa bonne foi, à défaut de sa conformité effective



Dans deux semaines, tous les organismes, publics comme privés, traitant des données personnelles des citoyens européens devront être conformes au Règlement général sur la protection des données (RGPD). Si la situation est déjà bien avancée pour certaines structures, d'autres voient arriver l'échéance avec angoisse car leur mise en conformité est loin d'être acquise. Recommandations de dernière minute pour être conforme a minima, avant le début d'une nouvelle ère en matière d'utilisation et de protection des données personnelles.

Par Sophie Sébirot

C'est un fait : en dépit de la multitude de conférences, webinars et autres publications destinées à aider les organisations à être conformes le jour J, ces dernières ne seront pas toutes ni totalement conformes au RGPD le 25 mai prochain. Loin s'en faut. Selon une étude Forrester, début 2018, seulement 26 % des entreprises européennes étaient conformes au RGPD. "Pour certaines entreprises, les dernières recommandations à mettre en œuvre sont plutôt les premières", note Me Gérard Haas, avocat et fondateur du cabinet Haas et avocats. "Nous avons assisté à une période d'attentisme de la part de certaines sociétés qui n'ont pas pris la mesure de l'ampleur du chantier de la mise en conformité", confirme Patrick Tisser, consultant manager chez NTT Security.

Un autre point tout aussi avéré est qu'il est impossible pour une société d'être à 100 % conforme au RGPD en quelques semaines. Des mesures de dernière minute s'imposent donc pour démontrer la bonne foi et la volonté des organisations d'y être conforme. "Pour les retardataires, il convient de prioriser les actions et d'éviter d'agir dans l'urgence au risque de mal faire", insiste Raphaël Brun, manager en charge du projet RGPD chez Wavestone. Me Haas dédramatise : "Il ne faut pas que le RGPD soit source d'angoisse : il n'est jamais trop tard pour se mettre en conformité, car il s'agit d'un chantier colossal".

La check-list de dernière minute

Si la CNIL n'attend pas une conformité à 100 % des entreprises, il importe néanmoins d'être conforme sur les points majeurs du texte, au risque de sanctions graves. "La première question qu'une entreprise doit se poser est dans quelle mesure elle est concernée par le RGPD. À partir de là, il convient de mettre en place des mesures adéquates", fait remarquer Paul-Oliver Gibert, expert pour les Assises de la sécurité et président de l'AFCDP (Association française des correspondants à la protection des données personnelles).

"La première question qu'une entreprise doit se poser est dans quelle mesure elle est concernée par le RGPD. À partir de là, il convient de mettre en place des mesures adéquates"

La check-list de dernière minute devrait comporter les points suivants : "désigner un pilote, même si la structure n'est pas dans un contexte où elle en aurait l'obligation ; effectuer le recensement des traitements de données personnelles et s'interroger sur des grands thèmes tels que la minimisation des données collectées, les modalités d'informations de recueil du consentement, l'identification des cas de recours aux sous-traitants ; mettre en œuvre de mesures visant à assurer la sécurité de données et documenter l'ensemble des actions menées, dans l'optique de démontrer la conformité à tout moment", fait valoir Dominique Soulier, membre du conseil d'administration du Clusif (Club de la sécurité de l'information français).

Désigner un DPO ou un chef de projet

La désignation d'un DPO (Délégué à la protection des données) fait partie des mesures à même de démontrer la volonté d'une entreprise d'être conforme au RGPD. "La nomination d'un DPO est conseillée car elle constitue une marque de respect du RGPD. Il s'agit donc d'un acte important pour bien commencer sa mise en conformité", souligne Paul-Olivier Gibert. Pour les grands groupes, NTT Security préconise la nomination de DPO relais pour chaque filiale.

"La nomination d'un DPO est conseillée car elle constitue une marque de respect du RGPD. Il s'agit donc d'un acte important pour bien commencer sa mise en conformité"

"La mise en place d'un chef de projet est idéale, mais toutes les structures ne peuvent se le permettre pour des raisons de ressources humaines ou financières", note Marco Pasqualotto, directeur juridique et affaires réglementaires de Hub One. Pour les PME, Raphaël Brun recommande de désigner un DPO externe : "il décryptera le RGPD en leur indiquant ce qui est vraiment important, les accompagnera et leur évitera d'engager des dépenses qui ne sont pas indispensables".

Disposer d’un registre de traitement des données

CNIL comme experts le répètent à l’envi : disposer d’un registre de traitement des données est primordial. “À compter du 25 mai, la charge de la preuve concernant la protection des données personnelles pèsera sur les entreprises. Les organisations doivent documenter tout ce qu’elles vont mettre en place pour protéger les données personnelles comme sensibles”, explique Marco Pasqualotto.

“Il est important de savoir quelles données sont collectées, pourquoi, pour combien de temps et d’appliquer le principe de minimisation des données”

“L’une des premières choses à faire est de cartographier les données, puis de définir un plan d’action et mettre en œuvre une démarche qualité”, précise Me Haas. “Il est important de savoir quelles données sont collectées, pourquoi, pour combien de temps et d’appliquer le principe de minimisation des données”, explique Darine Fayed, responsable juridique de la société d’emailing Mailjet.

Le consentement des clients

La protection des données personnelles imposée par le RGPD nécessite de recueillir le consentement des clients pour les utiliser. “Lorsque l’on dispose du consentement des personnes, il est important d’en conserver la trace. De nombreuses sociétés n’avaient pas prévu d’assurer la traçabilité des données”, déclare Patrick Tissier. “Le droit à la portabilité des données est un droit que les citoyens doivent pouvoir exercer dès le 25 mai”, affirme Paul-Olivier Gibert. “Mailjet a passé en revue tous ses processus informatiques afin de s’assurer que les droits de ses clients étaient respectés, notamment en anonymisant les données. La communication avec nos clients est désormais plus claire et plus transparente”, souligne Darine Fayed.

“Lorsque l’on dispose du consentement des personnes, il est important d’en conserver la trace. De nombreuses sociétés n’avaient pas prévu d’assurer la traçabilité des données”

Les sous-traitants ne doivent pas être oubliés, car ils peuvent servir de point d’entrée pour une cyberattaque. “Revoir les contrats avec les sous-traitants, du moins les plus importants ou ceux qui contiennent des données sensibles, est crucial”, indique Patrick Tissier. “Les rapports avec les sous-traitants sont également importants. Il convient de définir la notion de responsabilité de traitement, ce qui est loin d’être facile”, confirme Marco Pasqualotto. “Il nous a fallu plus de 6 mois pour revoir les contrats avec les quelque 75 sous-traitants de Mailjet”, indique Darine Fayed.

Tout dépend du niveau de maturité

L’application de ces diverses mesures dépend bien sûr du degré de conformité des entreprises au RGPD. “Certaines entreprises ne sont pas complètement conformes, d’autres le sont moyennement et d’autres ne le sont pas du tout. Dès lors, les priorités ne sont pas les mêmes”, fait remarquer Raphaël Brun, qui poursuit : “Celles qui ne sont pas du tout conformes ont intérêt à mettre très rapidement en place un registre de traitement des données utilisées. La seconde priorité est de constituer un plan d’action comprenant une analyse d’impact et de structurer les projets les plus complexes et les plus onéreux. Cela permettra aux entreprises d’avoir une feuille de route et de savoir où elles en sont dans leur mise en conformité en cas de contrôle. La troisième priorité est de mobiliser l’ensemble des directions concernées par le RGPD pour qu’elles puissent travailler de conserve”.

“Celles qui ne sont pas du tout conformes ont intérêt à mettre très rapidement en place un registre de traitement des données utilisées”

“Les entreprises les plus avancées doivent se souvenir que la notion de transparence est au cœur du RGPD. Il convient donc de bien communiquer sur les droits des clients à protéger leurs données personnelles, et que cela soit bien compris en interne”, explique Raphaël Brun. “La notification des fuites de données est également primordiale dans le cadre du RGPD. Il est essentiel de mettre à jour les processus de gestion de crise, voire de procéder à des exercices de gestion de crise”, insiste le manager de Wavestone. Les dernières recommandations à mettre en œuvre dépendront également de la taille des organisations, de leur recours aux données personnelles et de leur secteur d’activité.

Le big bang du 25 mai

Être au moins en partie conforme au RGPD au 25 mai est essentiel, car cette date marque le début d’une nouvelle ère dans l’utilisation des données personnelles. “Nous allons changer d’ère ; le RGPD ne signifie pas qu’il ne sera plus possible de ne rien faire avec les données, mais que l’on ne pourra plus procéder comme avant”, souligne Marco Pasqualotto. “Auparavant, les entreprises faisaient du quantitatif, désormais elles devront faire du qualitatif, à savoir la collecte du mieux et non du tout”, précise Me Haas, qui poursuit : “les entreprises qui jouent le jeu continueront de se développer, les autres se mettront d’elles-mêmes à l’écart. Les organisations n’ont pas le choix : le marché souhaite de la confiance”.

“Le 25 mai ne constitue qu’une première étape dans la mise en conformité au RGPD, car la plupart des programmes courront jusqu’en 2019, voire 2020”

Paul-Olivier Gibert va plus loin : “la mise en application du RGPD n’est pas une date butoir, c’est un big bang”. Raphaël Brun temporise : “le 25 mai ne constitue qu’une première étape dans la mise en conformité au RGPD, car la plupart des programmes courront jusqu’en 2019, voire 2020”. “Le travail qui reste à faire pour être conforme au RGPD, est conséquent, il nécessite du temps, des moyens et limitera le business de certaines organisations”, ajoute Marco Pasqualotto. Et Paul-Olivier Gibert de conclure : “Le RGPD est un garde-fou majeur face à une dérive orwellienne. Il est important de s’engager sur la manière dont on veut vivre”. Les citoyens, las des scandales et fuites de données à répétition, semblent l’avoir compris. Ils n’aiment plus Big Brother.

A lire égalementLes guides de la CNIL pour une mise en conformité bien ordonnée

La Commission nationale informatique et libertés (CNIL) a publié de nombreux ouvrages didactiques pour aider les entreprises, quelle que soit leur taille, à se mettre en conformité. En janvier dernier, l'autorité de régulation a publié un guide sur la sécurité des données personnelles listant les précautions élémentaires à mettre en œuvre de façon systématique. Ce document rappelle que dans le cadre d'une gestion des risques, même minimale, quatre étapes doivent être suivies : recenser les traitements, apprécier les risques, mettre en œuvre et vérifier les mesures prévues, et réaliser des audits de sécurité périodiques. Ce guide comprend également 17 fiches thématiques, ainsi qu'une évaluation à la fin de l'ouvrage pour savoir si l'entreprise est en conformité ou pas. Les guides PIA de la CNIL permettent de mener une analyse d'impact relative à la protection des données.

Par ailleurs, la CNIL, en coopération avec Bpifrance, a publié un guide pratique adapté aux TPE/PME. Ce document comprend des fiches thématiques rappelant les grands principes du RGPD, un plan d'actions en quatre étapes, à savoir constituer un registre de traitement des données, trier les données, respecter les droits des personnes et sécuriser les données, des fiches pratiques et les 6 bons réflexes de la protection des données personnelles. Un autre guide conçu par la confédération des PME (CPME), avec le concours de la CNIL également, est paru récemment. Il recense les neuf étapes clés à suivre pour être en conformité avec la nouvelle réglementation européenne. Cette publication est illustrée par des exemples et des conseils.

Les sanctions en cas de non-respect du RGPD

Contrairement aux sanctions prévues dans le cadre de la loi Informatique et libertés, qui ne pouvaient excéder 150 000 euros pour un premier manquement, les sanctions prévues par le RGPD sont pour le moins dissuasives : "jusqu'à 10 millions d'euros ou, dans le cas d'une entreprise, 2 % du chiffre d'affaires annuel mondial pour des manquements notamment au privacy by design, privacy by default, en matière de PIA, etc. et jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, 4 % du chiffre d'affaires annuel mondial pour manquement notamment aux droits des personnes (droits d'accès, de rectification, d'opposition, de suppression, droit à l'oubli, etc.)", indique le cabinet Haas Avocats. Dans chacun des cas, c'est le montant le plus élevé qui est pris en compte. Des sanctions pécuniaires qui peuvent largement mettre en péril l'activité des entreprises contrevenantes.

On en parle moins, mais des sanctions pénales s'appliquent également, pouvant aller jusqu'à 300 000 euros d'amendes et cinq ans d'emprisonnement pour les violations les plus graves, telles que le non-respect des formalités préalables ou encore le détournement de la finalité des données personnelles. À cela s'ajoutent bien évidemment des répercussions en termes d'image et de réputation. La perte de confiance en Facebook depuis l'affaire Cambridge Analytica en est un exemple flagrant. Selon un récent sondage réalisé par le Ponemon Institute, seuls 29 % des personnes interrogées estiment que Facebook s'engage réellement en faveur de la protection des données personnelles. Ils étaient 79 % à le penser en 2017 ! Last but not least, les entreprises craignent des actions de groupe de la part d'associations de protection des droits et libertés des citoyens sur Internet en cas de manquements. On ne plaisante plus avec les données personnelles.

La CNIL a reçu 8 360 plaintes en 2017, contre 7 703 en 2016.
27 % des plaintes concernent la diffusion de données personnelles sur Internet.
Source : CNIL