DONNÉES PERSONNELLES

Moins de 13 mois pour se mettre en conformité

Entré en vigueur en mai 2016, le RGPD modifie les règles de gestion des données à caractère personnel dans les entreprises. Fin mai 2018, toutes les organisations devront être en conformité. Et passer d'une obligation de déclaration à une obligation de preuve permanente.

Le 25 mai 2018, l'ensemble des entreprises ayant des activités en Europe devront être en conformité avec le Règlement général sur la protection des données (RGPD). Une révolution dans la gestion des données personnelles au sein des entreprises que le Daf doit enclencher au plus tôt.

QUI EST CONCERNÉ ?

Le RGPD s'applique "au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier." Ce règlement s'applique à toute structure (responsable de traitement des données ou sous-traitant) ayant un établissement dans l'Union européenne ou bien proposant une offre de biens ou de services qui vise les personnes présentes sur le territoire de l'Union européenne. Les actions de profilage visant cette cible sont également concernées.

Nota bene **Alors que la loi Informatique et libertés se basait sur des critères d'établissement et de moyens de traitement, le règlement européen introduit la notion de ciblage : le critère principal d'application est désormais le traitement des données d'une personne se trouvant au sein de l'UE.**

QU'EST-CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL ?

L'une des difficultés posées par le RGPD va consister à définir ce que sont ces données personnelles. Le règlement précise qu'il s'agit de "toute information concernant une personne physique identifiée ou identifiable", directement ou indirectement. Des données indirectement identifiantes, telles qu'un numéro de téléphone ou un identifiant, en font donc partie. De même, les données comportementales collectées sur Internet – notamment dans le cadre d'actions marketing de profilage –, si elles sont corrélées à une identité, revêtent un caractère personnel. Selon le traitement appliqué aux données, des informations non identifiantes peuvent ainsi devenir identifiantes, par croisement des informations collectées.

Nota bene **Le RGPD prévoit des exceptions selon les cas, notamment au niveau des traitements de données RH (recrutement, contrat de travail…), pour lesquels les États membres peuvent prévoir "des règles plus spécifiques pour assurer la protection des droits et libertés" (article 88).**

QUELLES OBLIGATIONS POUR LES ENTREPRISES ?

La loi Informatique et libertés se basait sur le déclaratif initial et des contrôles ponctuels. Le règlement européen remplace cette obligation de déclaration par celle de prouver à chaque moment que l'entreprise protège les données. Dès lors, la structuration même des outils de collecte des données (CRM, DMP, solutions de tracking ou de géolocalisation…), mais aussi les contrats passés avec les

sous-traitants et clients sont impactés. *« Le règlement couple des notions techniques et juridiques »*, souligne Me Thomas Beaugrand, avocat associé au sein du cabinet Staub & Associés. Il introduit de nouveaux principes et concepts qui renvoient désormais vers plus de précautions techniques.

Par ailleurs, les entreprises ont, entre autres obligations, celle de donner la finalité précise de la collecte des données (il s'agit de la minimisation, l'un des grands principes de la dataprotection, qui impose que seules les données nécessaires au but poursuivi pourront être collectées).

Le RGPD impose également le principe de conservation limitée des données, ainsi que celui de coresponsabilité des sous-traitants et des entreprises en matière de protection de la data, qui distribue les responsabilités en fonction de la mainmise de chacun sur les données.

TROIS PRINCIPES DIRECTEURS

Avec la démarche de privacy by design, les données personnelles devront être identifiées directement en tant que telles dans le système afin de limiter leur accès. C'est donc dès la conception intellectuelle et technique des traitements que cette notion doit être intégrée. *« Le privacy by design doit être traduit en dur dans le code source des outils utilisés par l'entreprise »*, insiste Me Beaugrand.

Dans le cadre de la démarche de security by default, les données doivent être discriminées par défaut pour n'utiliser que celles qui sont strictement nécessaires à la finalité poursuivie. Ainsi, les outils doivent discriminer les données selon les traitements et les habilitations.

Enfin, avec la démarche d'accountability, le responsable du traitement doit disposer de registres décrivant tous les traitements appliqués aux données, afin de pouvoir démontrer à tout moment que la protection des données personnelles au sein de sa structure est optimale.

QUELLES SONT LES ACTIONS ET MODIFICATIONS À METTRE EN ŒUVRE?

Face au bouleversement engendré par l'entrée en vigueur du RGPD en mai dernier, il reste aux entreprises moins de 13 mois pour se mettre en conformité: à compter du 25 mai 2018, toutes les organisations devront respecter le nouveau règlement, et des sanctions lourdes, jusqu'à 4 % du CA annuel mondial de l'entreprise prise en défaut, pourront être appliquées.

La première étape, pour le Daf, consiste donc à réaliser un mapping afin d'identifier les traitements des données existants au sein de sa structure. Pour les services juridiques, *« il sera nécessaire de se mêler à toutes les fonctions support pour assurer la mise en place de ce règlement »*, recommande Clémence Scottez, chef de service des affaires économiques de la Cnil, afin de déterminer les interlocuteurs-clés.

Deuxième étape: réaliser des études de risques et d'impact selon les traitements adoptés et la nature des données, et si besoin se faire accompagner par des experts pour définir ▶▶▶

À SAVOIR

DANS QUELS CAS NOMMER UN DPO?

La désignation d'un délégué à la protection des données, qui sera le garant de la conformité au règlement, est obligatoire:

- lorsque le traitement des données est effectué par une institution publique;
- si les activités de base de l'organisme consistent en des traitements qui imposent un suivi régulier et systématique à grande échelle des personnes concernées (par exemple pour les ciblages marketing ou la lutte contre la fraude);
- si les activités de base de l'organisme consistent en des traitements à grande échelle de données sensibles ou de données relatives aux condamnations et infractions spéciales (par exemple, des infractions pénales dans le cadre de la lutte contre les incivilités en banque).

Le DPO doit avoir une certaine neutralité et être en contact direct avec le Comex pour remonter les problématiques rapidement. À noter, le RGPD autorise la mutualisation du DPO pour des groupes d'entreprises. Les petites structures pourront ainsi faire appel à un prestataire externe, à condition que ce délégué soit "facilement joignable à partir de chaque lieu d'établissement" (article 37.5 du RGPD).

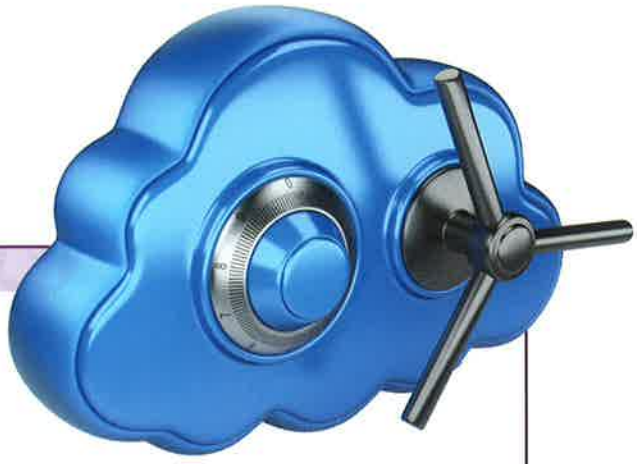
Pour rappel, même si une entreprise n'est pas concernée par l'obligation de désigner un DPO, elle devra tout de même pouvoir justifier à tout moment du strict respect du RGPD dans sa gestion des données.

« Le privacy by design doit être traduit en dur dans le code source des outils utilisés par l'entreprise. »

Me THOMAS BEAUGRAND, CABINET STAUB & ASSOCIÉS

AVIS D'EXPERT

Me SYLVAIN STAUB, associé au sein du cabinet Staub & Associés



« C'est une démarche de recâblage complet de l'entreprise »

Comment le Daf peut-il coordonner les différents services afin d'être en conformité avec le RGPD d'ici mai 2018?
La mise en conformité de l'entreprise, a fortiori du groupe d'entreprises, constitue un véritable projet auquel doivent participer la plupart des services, car ils manipulent tous, à des degrés divers, des données personnelles. Le service marketing, qui prospecte, le service client, qui gère l'ensemble des contrats et donc des contacts chez les clients, le service achats, en relation avec les fournisseurs, la DSI, qui conçoit les systèmes ou implémente la sécurité, la DRH, qui traite les données des salariés, doivent tous être sensibilisés, ainsi que le département R&D, pour les entreprises qui éditent ou intègrent des technologies numériques, car le RGPD doit être intégré à l'ADN de ces produits dès leur conception. Il s'agit d'une démarche de "recâblage" complet de l'entreprise, qui doit se doter de processus, de réflexes et de modalités de contrôle pour que la conformité au RGPD soit effective et de chaque instant. Mai 2018 arrivera très vite et il n'y aura pas de délai supplémentaire; il semble donc impératif de se lancer dans ce projet sans attendre.

Quelles démarches le Daf doit-il entreprendre auprès de ses éditeurs de logiciels?
L'entreprise doit dès à présent interroger ses fournisseurs, qu'il s'agisse des éditeurs logiciels, des éditeurs de SaaS et autres services cloud, et des ESN qui interviennent en son sein pour déployer qui un ERP, qui un CRM, qui un système de communications unifiées, afin de connaître leur niveau d'expertise et de conformité au RGPD. Mais on ne doit pas s'illusionner: ces ESN ne sont pas encore toutes conformes, et elles-mêmes doivent investir un temps et une énergie considérables pour actualiser leur organisation et leurs produits. Et l'entreprise cliente ne peut se contenter de s'en remettre aux travaux de son fournisseur, car elle-même doit adopter des processus et des règles internes de protection des données personnelles, indépendamment des produits acquis. Ce recâblage va impacter les modes d'utilisation par le personnel des outils qui leur sont confiés, et modifier les règles de confidentialité des données au sein de l'entreprise. À l'instar de la coresponsabilité voulue par le RGPD entre "responsables de traitements" et "prestataires sous-traitants", une "coresponsabilité" doit advenir et implique donc une réflexion conjointe des parties dans les contrats, et une démarche de mise en conformité progressive.

Qu'en est-il des données personnelles collectées avant l'entrée en vigueur du RGPD?
Elles devront clairement être traitées, à l'avenir, conformément aux nouvelles exigences du RGPD. C'est notamment pour cela que le règlement a accordé un délai de deux ans pour se mettre en conformité: demain, toutes les données personnelles traitées dans l'entreprise devront bénéficier des règles du privacy by design, du security by default, et toutes les personnes physiques concernées devront bénéficier des nouveaux droits mis en place. Il faudra donc prévoir des vagues de régularisations à déployer auprès des populations concernées, afin de préciser l'information qui leur est due, et de collecter des consentements complémentaires, notamment dans le cadre des traitements big data et onboarding qui se déploient en big bang actuellement sur le marché, y compris au sein des industries les plus sensibles à la sécurité de la data (banques, santé, telcos...).

une politique de gestion des données. L'EDPB (European data protection board), émanation du G29 qui regroupera l'ensemble des Cnil européennes, va fournir des listes de traitements soumis à des études d'impact.

Nota bene **Le Daf, main dans la main avec les différentes directions de l'entreprise, au premier rang desquelles la DSI, devra mettre en place les réorganisations internes nécessaires (désignation du délégué à la protection des données – DPO –, mais aussi déploiement des différentes démarches de privacy by design, security by default et accountability) et contractualiser les mesures de sécurité avec les clients et fournisseurs.** ●

BÉNÉDICTE GOUTTEBROZE