RGPD : 6 mois d'existence et déjà des sanctions

Mises en demeure pour atteinte à la sécurité des données clients, pour absence de consentement au traitement de données, pour vidéosurveillance excessive… Les entreprises qui ne sont pas en conformité avec le RGPD se voient peu à peu épingler par la Cnil. Quels sont les risques qu'elles encourent ? Le point avec des professionnels des cabinets d'audit RSM et Fideliance et leurs conseils pour se mettre en conformité.

Depuis l'entrée en application le 25 mai 2018 du RGPD, le Règlement général sur la protection des données personnelles, les mises en demeure s'enchaînent. Même si pour le moment, ce sont plutôt les grandes entreprises qui sont épinglées, de petites structures sont elles aussi parfois sur la sellette. C'est le cas par exemple d'une jeune start-up de ciblage publicitaire fondée en 2015, mise en demeure le 23 octobre 2018 pour *« absence de consentement au traitement de données de géolocalisation à des fins de ciblage publicitaire »*. Si elle ne se conforme pas aux injonctions de la Cnil dans les trois mois, l'autorité administrative se réserve le droit de prononcer une sanction (lire encadré page suivante.

Sécurité de l'information. *« Jusqu'à maintenant, les sanctions prononcées par la Cnil sont en grande partie dues à des violations de données pour mesures de sécurité informatique insuffisantes. Les entreprises se font pirater et les données se retrouvent sur la place publique »* indique Jean-Éloi Pénicaut, senior manager IT et Risk advisor chez RSM, un cabinet international d'audit, d'expertise comptable et de conseil. Outre les aspects juridiques et organisationnels qui relèvent du RGPD, la sécurité de l'information est donc une thématique importante du règlement européen. *« Le référentiel incontournable en matière de sécurité de l'information est la norme ISO 27001,* complète Jean-Philippe Isemann, associé de RSM. *Elle est d'une grande aide pour la mise en conformité au RGPD en apportant à l'entreprise une vision globale et des orientations pratiques en matière de gestion des risques liés à la sécurité de l'information. »*

Ce que risquent les entreprises. La procédure de mise en demeure n'est pas une sanction. Elle intervient après une plainte reçue par la Cnil ou après un contrôle que la Commission a effectué dans une entreprise ou une organisation. Il s'agit d'une demande de mise en conformité par rapport aux manquements constatés. Pour y répondre, l'entreprise dispose d'un délai de 10 jours à 6 mois, renouvelable une fois, voire de 24 heures en cas d'urgence. Ce délai est notifié dans la mise en demeure. Celle-ci est parfois rendue publique ce qui peut constituer pour l'entreprise une première forme de sanction.

Si l'entreprise ne répond pas aux exigences de la mise en demeure, des sanctions peuvent alors être prononcées par la Cnil. La procédure de sanction est progressive. *« Le premier niveau est un rappel à l'ordre. La Cnil peut ensuite, selon les cas, obliger à mettre un traitement de données en conformité, interrompre un traitement de données, ordonner de satisfaire aux demandes des personnes. En dernier lieu, elle peut prononcer une sanction pécuniaire pouvant aller jusqu'à 4 % du chiffre d'affaires annuel mondial ou 20 M€ »,* détaille Jean-Éloi Pénicaut. Selon lui, ce plafond a, pour le moment, peu de chance d'être atteint ou appliqué : *« Au regard des sanctions prononcées depuis quelques mois, pour l'instant, la Cnil insiste davantage sur l'aspect pédagogique de la sanction. »*

« La Cnil peut également décider de rendre publique la sanction, ajoute Jean-Philippe Isemann. *En termes d'image, la communication de la sanction a généralement un fort impact négatif pour l'entreprise, situation particulièrement redoutée. »*

Responsabilité du chef d'entreprise. En dehors de ces sanctions administratives, une sanction civile ou pénale peut être prononcée à l'endroit du chef d'entreprise. *« Les personnes ayant subi un préjudice peuvent attaquer l'entreprise en responsabilité civile »,* note Jean-Éloi Pénicaut.

« D'après l'article 84 du RGPD, les États

Plusieurs organisations ont été mises en demeure de redimensionner leur système de vidéosurveillance qui filmait en permanence le personnel.

7 par jour

C'est le nombre de notifications de violations de données que reçoit la Cnil en moyenne depuis le 25 mai 2018.

Jean-Éloi Pénicaut, senior manager IT & Risk advisory de RSM.

Jean-Philippe Isemann, associé de RSM, responsable du département IT & Risk advisory.

Xavier Larbalette, directeur des systèmes d'information de Fideliance.

Arnaud Audo, expert-comptable associé de Fideliance.

membres peuvent également mettre en place des sanctions supplémentaires en cas de violation du RGPD, cela pouvant aller pour la France à une sanction de 5 ans d'emprisonnement et de 300 000 € d'amende pour le chef d'entreprise » complète Xavier Larbalette, directeur des systèmes d'information chez Fideliance Digital, société de conseil en systèmes d'information, filiale de la société d'expertise comptable Fideliance.

Les autorités équivalentes à la Cnil en Europe. Il existe dans chaque pays de l'Union européenne une autorité équivalente à la Cnil. *« C'était déjà le cas avant le RGPD mais elles se sont structurées depuis pour travailler dans un cadre commun »*, observe Jean-Éloi Pénicaut. Ainsi, la France a modifié sa loi Informatique et Libertés par un décret d'août 2018, paru 4 mois après l'application du règlement et qui l'adapte au contexte français. Mais il subsiste des différences, que les entreprises internationales doivent prendre en compte : *« Il existe parfois des divergences locales d'interprétation qui peuvent être une problématique pour structurer et homogénéiser les processus,* avance Jean-Philippe Isemann. *Il faut alors ajuster les versions locales des contrats. »*

La mise en conformité. Les entreprises, et notamment les PME et TPE, sont aujourd'hui encore loin d'être toutes en conformité avec le RGPD. Afin de s'y mettre rapidement, Jean-Éloi Pénicaut conseille d'abord d'identifier les fichiers de données personnelles (salariés, clients, prospects, fournisseurs…) et de se poser les questions suivantes : *« L'entreprise traite-t-elle de nombreuses données personnelles ? Traite-t-elle des données sensibles c'est-à-dire, pour simplifier, des données médicales, politiques, religieuses, judiciaires, d'orientation sexuelle ? Y a-t-il des échanges avec des prestataires externes, des échanges hors Union européenne ? »* Il s'agit de mettre en place un registre des traitements. Des modèles de registres sont disponibles sur le site de la Cnil. Nombre de sociétés font également appel à des sociétés de conseil pour les aider dans leurs démarches.
« Si l'entreprise compte plus de 250 salariés ou si elle exploite des données à caractère personnel sensibles, elle a l'obligation de désigner un délégué à la protection des données ou DPO (Data ▶

Les dernières mises en demeure de la Cnil

(Source : site internet de la Cnil)

19 juillet 2018, Fidzup et Teemo. Ces deux entreprises collectent des données personnelles et de géolocalisation via les smartphones et réalisent des campagnes publicitaires sur les mobiles. Cependant, la Cnil a relevé que le consentement des personnes concernées n'est pas recueilli comme l'exige le RGPD. Par ailleurs Teemo conserve les données de localisation pendant 13 mois, ce qui est contraire à l'obligation de définir et de respecter une durée de conservation des données proportionnée à la finalité du traitement. Les deux entreprises ont 3 mois pour recueillir le consentement des utilisateurs et pour définir une durée de conservation adéquate, pour que leur activité soit pleinement conforme aux textes.

24 juillet 2018, Institut des techniques informatiques et commerciales. L'école privée d'enseignement supérieur a été mise en demeure de redimensionner dans les deux mois son système de vidéosurveillance en cessant de filmer en permanence le personnel, les enseignants et les élèves, dans leurs salles de cours et dans leurs lieux de vie. Elle doit également supprimer les images enregistrées et informer toute personne susceptible d'être filmée par le dispositif.

18 octobre 2018, sociétés des groupes Humanis et Malakoff-Médéric. La Cnil a constaté que ces sociétés utilisent les données personnelles qu'elles détiennent concernant les régimes de retraite complémentaire pour effectuer de la prospection commerciale pour des produits et services de leurs groupes. Elle les a mises en demeure de cesser ce détournement de finalité dans un délai d'un mois.

23 octobre 2018, Singlespot. Cette société a recours à des outils techniques (SKF) pour collecter les données personnelles et de géolocalisation des utilisateurs via leurs smartphones. Ces données sont ensuite croisées afin d'afficher de la publicité ciblée sur les smartphones à partir des lieux que les personnes ont visités. Cependant, la Cnil a constaté que le consentement des personnes concernées n'était pas valablement recueilli et qu'elles ne sont pas systématiquement informées, lors du téléchargement des applications mobiles, qu'une collecte de leurs données de localisation est effectuée. L'entreprise dispose de trois mois pour se mettre en conformité.

30 octobre 2018, École 42. La Cnil a mis en demeure l'association de formation en informatique de redimensionner son système de vidéosurveillance en cessant de filmer en permanence salles de cours et lieux de vie. Elle rappelle aussi que tout système de vidéosurveillance plaçant des salariés ou des étudiants sous surveillance constante est excessif.

9 novembre 2018, Vectaury. Tout comme la société Singlespot, cette entreprise a recours aux technologies SDK pour collecter des données personnelles via les mobiles et réaliser des campagnes publicitaires sur ceux-ci. Cependant elle n'a pas recueilli de façon valable le consentement des personnes concernées. Elle est également mise en demeure de supprimer les données qu'elle avait indûment collectées.

Les dernières sanctions de la Cnil

(Source : site internet de la Cnil)

Le 28 juin 2018, Adef, amende de 75 000 €. La Cnil a relevé que de nombreuses données personnelles des demandeurs de logement inscrits sur le site internet de l'Adef (Association pour le développement des foyers) étaient accessibles : noms, dates de naissance, adresses postales, nombre d'enfants, références bancaires, salaires, revenus fiscaux de référence, allocations adultes handicapés… Compte tenu de la gravité de la violation et du caractère intime et complet des données concernées, la Cnil a décidé, en plus de l'amende, de rendre publique sa décision.

Le 31 juillet 2018, Archipel Habitat, amende de 30 000 €. L'office public de l'habitat de Rennes Métropole Archipel Habitat a été sanctionné pour avoir utilisé le fichier de ses locataires à d'autres fins que la gestion de l'habitat social. La Cnil a rendu publique sa décision estimant notamment indispensable de rappeler à l'ensemble des acteurs du secteur social, l'interdiction d'utiliser des fichiers d'usagers pour des finalités autres et incompatibles avec les finalités initiales.

Le 2 août 2018, DailyMotion, amende de 50 000 €. La plateforme a fait l'objet d'une attaque informatique qui avait notamment concerné 82,5 millions d'adresses emails. Tout en soulignant que l'attaque subie par la société était sophistiquée, la Cnil a relevé qu'elle n'aurait pas pu aboutir si certaines mesures de sécurité élémentaires avaient été mises en place.

Le 20 septembre 2018, Assistance Centre d'Appels, amende de 10 000 €. La société spécialisée dans la télésurveillance d'ascenseurs et de parkings a été sanctionnée pour avoir mis en œuvre illégalement un système biométrique à des fins de contrôle des horaires des salariés. La Cnil a également constaté qu'un dispositif d'enregistrement des appels téléphoniques fonctionnait sans que les salariés et les interlocuteurs n'en soient informés. De plus, les postes de travail n'étaient pas suffisamment sécurisés par des mots de passe robustes ou un verrouillage automatique.

Le 27 septembre 2018, Alliance Française Paris Île-de-France, amende de 30 000 €. Les données des personnes suivant des cours de français étaient librement accessibles. Un contrôle en ligne a permis de constater qu'en modifiant un numéro d'identifiant contenu dans une URL de l'espace utilisateur, il était possible de télécharger factures, certificats d'inscription ou récapitulatifs des cours suivis. La Cnil a souhaité rappeler qu'une violation de données commise par un sous-traitant, comme ici, ne dispense pas le responsable de traitement d'assurer un suivi rigoureux des actions menées par le sous-traitant.

Protection Officer), note Arnaud Audo, associé de Fideliance. *C'est lui qui va être responsable de la cartographie des traitements. Il va ensuite prioriser les actions à traiter en fonction des failles repérées et gérer les risques tout au long de la vie de l'entreprise.* »

La fonction de DPO peut être assurée par un salarié nommé par le chef d'entreprise. Il doit être indépendant et ne doit pas être en situation de conflit d'intérêt. « *Le dirigeant peut aussi préférer avoir recours à un consultant externe qui fait office de DPO. Le cabinet RSM intervient en qualité de DPO externalisé pour plusieurs sociétés* » souligne Jean-Philippe Isemann. Dans tous les cas, s'il y a fuites de données, c'est le chef d'entreprise qui est responsable.

Les contrats avec les sous-traitants. Les fournisseurs qui traitent de données clients d'une entreprise (envois de mailing, hébergement cloud…) doivent eux aussi être en conformité avec le règlement européen. L'article 28 du règlement spécifie que les fournisseurs ou prestataires ayant accès à des données concernées par le RGPD doivent présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, de manière à ce que le traitement réponde aux exigences du RGPD.

L'exemple d'une TPE. L'entreprise Gazdetect, créée en 2008, compte douze salariés. Elle fait partie de ces entreprises qui se concentrent sur leur cœur de métier, à savoir la distribution et la maintenance de détecteurs de gaz et d'équipements de protection respiratoire. Pour se mettre en conformité avec le RGPD pour l'ensemble de ses activités, y compris celles qui se développent en dehors de l'Europe, elle s'est appuyée sur les conseils de Fideliance. « *L'entreprise étant basée en France, elle doit gérer l'ensemble des données à caractère personnel de façon identique dans tous les pays* », explique Xavier Larbalette. Une fois les risques identifiés, ils ont été priorisés, classifiés et les plus critiques ont été traités en priorité. La plupart de ces risques relève de bonnes pratiques ou de principes de base poursuit le DSI : « *Par exemple, pour sécuriser au maximum le système d'information, il faut appliquer des mots de passe complexes.* » Les conditions générales de ventes et tous les contrats ont également été vérifiés. La notion de transparence a été notifiée aux clients. « *Chez Gazdetect, les données clients n'ont pas lieu d'être utilisées pour autre chose que les achats de matériel spécifiques ou pour effectuer des mailings* », affirme Xavier Larbalette. L'information de l'utilisation de leurs données est donc clairement spécifiée aux clients et consolidées dans les conditions générales de vente.

La notion de consentement est également un élément fort du RGPD. En outre, il faut prouver que ce consentement a bien été effectué et en garder la preuve. Gazdetect a donc demandé à ses clients leur consentement pour recevoir des mailings et a stocké cette information. Depuis, elle leur donne la possibilité de se rétracter.

Il est important à présent de signifier toutes nouvelles informations qui pourraient avoir un impact sur le RGPD.

Les atouts du RGPD pour les entreprises. Le règlement unifie la réglementation au niveau européen et redonne aux citoyens le contrôle de leurs données personnelles. Il se révèle être une opportunité pour les entreprises qui mettent en place de bonnes pratiques de sécurité ce qui permet d'augmenter leur capital confiance auprès de leurs clients, de leurs partenaires et également de leurs propres salariés. « *Il faut prendre conscience que le patrimoine digital est vital à la survie des entreprises* », observe Xavier Larbalette.

« *Si jusqu'à présent la Cnil a été relativement clémente, en 2019 le risque va s'amplifier pour les sociétés, y compris pour les petites entreprises. On ne peut que les encourager à se mettre en conformité avec le RGPD* », souligne Arnaud Audo.

Martine Porez

13 000

C'est le nombre de DPO désignés (personnes physiques ou morales) à fin octobre 2018 pour 24 500 organismes (contre 5 000 correspondants informatique et libertés avant le RGPD).