GRAND FORMAT

MISE EN CONFORMITÉ AU GDPR : LES PME NE DOIVENT PLUS TARDER

Le 25 mai prochain, le Règlement Général sur la Protection des Données (RGPD ou GDPR en anglais) entrera en application dans l'ensemble de l'Union européenne. Les PME, qui disposent de moins de moyens humains et financiers, seront également impactées par ce texte européen. À moins de 3 mois de l'échéance, les PME doivent dès maintenant débuter leur mise en conformité. En priorisant certaines mesures, elles pourraient encore parvenir à temps à offrir à leurs clients et employés de meilleures garanties quant à la protection de leurs données personnelles.

TEXTE: QUENTIN DEUXANT

L'annonce n'est pas neuve. Et le contenu du règlement pas si révolutionnaire qu'il n'y paraît. Mais le GDPR (Règlement sur la Protection des Données) est sur toutes les lèvres et fait couler beaucoup d'encre. La raison en est simple: après des années de flottement durant lesquelles les données personnelles étaient protégées par une directive européenne transposée de façon variable dans les législations des différents états membres, ce nouveau règlement introduit deux éléments potentiellement anxiogènes pour les entrepreneurs, à savoir d'une part leur propre responsabilisation par rapport à la problématique et, d'autre part, la possibilité de lourdes sanctions en cas d'infraction. «La protection des données personnelles en Europe n'est pas une nouveauté en soi, rappelle Tine A. Larsen, présidente de la Commission Nationale pour la Protection des Données (CNDP). Mais ce qui change fondamentalement avec ce règlement, c'est que les entreprises ne devront plus introduire une notification ou demander une autorisation préalable pour traiter des données personnelles. Elles devront le faire d'elles-mêmes et l'effectivité des mesures prises sera contrôlée a posteriori, avec une possibilité de sanction à la clé. C'est une manière de responsabiliser les entreprises: si on utilise des données personnelles, il y a une contrepartie, à savoir garantir leur protection.»

Alors que la demande d'autorisation était auparavant très cadrée, et souvent remplie par les professionnels qui fournissaient les services ou le matériel de collecte de données, il revient aujourd'hui aux entreprises elles-mêmes de s'intéresser à la réglementation et de se mettre en conformité. De quoi poser problème aux structures plus réduites, qui ne peuvent pas compter sur une armada de consultants.

LES MÊMES EXIGENCES POUR LES PME, PAS LES MÊMES MOYENS

Le GDPR prend-il cet aspect en compte en réservant un traitement différent aux PME? Pas vraiment. «Le texte s'applique à tout le monde, le petit artisan comme les grandes entreprises, indique Tine A. Larsen. Avec la digitalisation, qui imprègne tous les secteurs d'activité, même un petit coiffeur de quartier peut collecter des données personnelles sur ses clients, par exemple grâce à des cartes clients.» Ainsi, les principes généraux du GDPR sont invariables. «Les PME et les autres entreprises doivent se poser les mêmes questions, affirme Christophe Buschmann, membre effectif du Collège de la CNPD. La collecte de données que je réalise est-elle légale? Ai-je informé les personnes dont je collecte les données? Puis-je collecter ces données de manière moins intrusive ou massive? Est-ce que je sais ce qui est fait des données collectées? Les données sont-elles correctes et à jour? Les données collectées sont-elles sécurisées et supprimées lorsqu'elles ne sont plus utilisées? Pour une entreprise, quelle que soit sa taille, il faut pouvoir répondre à toutes ces questions et leur donner la réponse appropriée.»

L'investissement à consentir pour se mettre en conformité varie en fonction de

«C'EST UNE MANIÈRE DE RESPONSABILISER LES ENTREPRISES: SI ON UTILISE DES DONNÉES PERSONNELLES, IL Y A UNE CONTREPARTIE, À SAVOIR GARANTIR LEUR PROTECTION.»

plusieurs facteurs, notamment le contexte de l'activité de la PME, le type et la quantité de données personnelles traitées. Chez MGSI, une société luxembourgeoise spécialisée dans la protection des données, on la chiffre, dans certains cas, à plusieurs milliers d'euros. «Une PME qui n'emploie que 25 personnes, mais qui est active dans plusieurs pays pourrait être logée à la même enseigne que des multinationales comptant des centaines d'employés, explique Mélanie Gagnon, CEO de MGSI. Certaines PME pourraient donc devoir investir plusieurs milliers d'euros pour mettre en place des mesures et des outils permettant de se mettre en conformité avec le GDPR. Or, leurs ressources ne sont évidemment pas comparables à celles des plus grandes structures.»

UN REGISTRE RÉPERTORIANT LES TRAITEMENTS DE DONNÉES PERSONNELLES

Mais quelles sont exactement ces données personnelles que le règlement européen cherche à protéger? Il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable. Parmi celles-ci, sont considérées comme plus sensibles les données sur l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques ou biométriques destinées à identifier une personne physique de manière unique, les données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique, ainsi que celles concernant les condamnations pénales. Parmi les mesures à mettre en place pour garantir la protection des données de ses clients et ses employés (lire encadré), la plus prioritaire est donc de procéder à un inventaire répertoriant l'ensemble des traitements de données en cours dans l'entreprise. «L'exercice est salutaire, car il permet d'identifier quelles sont les données que traite l'entreprise, poursuit Mélanie Gagnon. De cette manière, elle peut donc savoir quelles données personnelles sont traitées, et prendre les mesures qui s'imposent en fonction, notamment, de la sensibilité des données.» La tenue d'un registre des traitements de données est, dans tous les cas, une obligation prévue par le GDPR. «Sauf pour les entreprises comptant moins de 250 personnes», précise Thierry Lallemang, membre effectif du Collège du CNPD. Cela veut-il dire que la plupart des PME n'ont pas à s'y soumettre? «Le texte parle en effet de cette limite de 250 employés, mais il comprend aussi une série d'exceptions» répond Mélanie Gagnon. Mieux vaut donc vérifier, en fonction des données que traite l'entreprise, si l'une des exceptions s'applique.

250

Est le nombre d'employés maximum pour qu'une entreprise ne soit pas soumise à la tenue d'un registre des traitements des données.

NE PAS FAIRE L'AUTRUCHE

L'un des principaux risques auquel s'expose la PME par rapport au GDPR est de croire qu'elle ne traite aucune donnée personnelle. À titre d'exemple, dès lors que la PME a un salarié, elle traite for-

LE GUIDE DES BONNES ET MAUVAISES PRATIQUES

Pour commencer votre mise en conformité au GDPR et mettre votre PME sur les bons rails, voici, selon Mélanie Gagnon, les actions à prioriser:

1. Consulter le site web de la CNPD, vous y trouverez de nombreuses informations, notamment un «guide de préparation au nouveau règlement général sur la protection des données».

2. Procéder à un inventaire des traitements de données personnelles effectués au sein de chaque service/département de votre entreprise: cette démarche vous permettra d'avoir une vue d'ensemble pour mettre en place les mesures qui s'imposent.

3. Analyser l'obligation de nommer ou non un DPO (Data Protection Officer). Son rôle et ses responsabilités au sein de l'entreprise doivent être définies conformément au GDPR. À noter que ce DPO peut être interne ou externe.

4. Mettre en place des procédures permettant aux individus d'exercer leurs droits. Si un ancien client vous demande le droit à l'effacement, comment allez-vous vous y prendre? Où sont ses données? Qui en a la possession et/ou les a copiées?

5. Revoir tous vos contrats de sous-traitance pour respecter les exigences du GDPR.

6. Se former sur le sujet, notamment en assistant aux séances de la CNPD ou aux séminaires GDPR de prestataires comme MGSI, conçus pour les PME.

cément des données personnelles. Elle peut même traiter des données dites «sensibles» si elle collecte l'extrait du casier judiciaire lors du recrutement ou encore, en cours d'emploi, les certificats médicaux en cas de maladie du salarié. «Il y a une certaine méconnaissance de la part de nombreuses PME, analyse Mélanie Gagnon. Certaines pensent qu'elles passeront entre les mailles du filet parce qu'elles sont de trop petite taille, d'autres adoptent la politique de l'autruche: elles attendent de voir ce qui va se passer, quelles seront les premières sanctions, avant de se décider à agir. Or, il ne faut pas croire que la mise en conformité ne prendra que peu de temps. Il est donc préférable de s'y prendre à l'avance pour répondre aux nouvelles exigences en toute sérénité.»

«CERTAINES PME PENSENT QU'ELLES PASSERONT ENTRE LES MAILLES DU FILET PARCE QU'ELLES SONT DE TROP PETITE TAILLE, D'AUTRES ADOPTENT LA POLITIQUE DE L'AUTRUCHE: ELLES ATTENDENT DE VOIR CE QUI VA SE PASSER, QUELLES SERONT LES PREMIÈRES SANCTIONS, AVANT DE SE DÉCIDER À AGIR.»

DES SANCTIONS PROPORTIONNELLES POUR FAIRE MAL

Si la démarche peut paraître fastidieuse, le jeu en vaut toutefois la chandelle. En effet, le GDPR introduit des sanctions assez lourdes pour que la protection des données soit, enfin, prise au sérieux par les entreprises. Les premiers chiffres annoncés ont d'ailleurs eu le don de réveiller l'intérêt par rapport au sujet: une amende s'élevant à 2% du chiffre d'affaires et allant jusque 10 000 000 d'euros pour des manquements relatifs à la sécurité des données collectées; et une sanction financière égale à 4% du chiffre d'affaires (jusqu'à 20 000 000 d'euros) pour les manquements au droit des personnes (droit d'accès, droit à l'oubli, etc.). Cela dit, ces chiffres ont été volontairement gonflés pour constituer un moyen de pression suffisant pour de grands acteurs comme les GAFA (Google, Apple, Facebook, Amazon). Guidés par une autre culture de la protection des données, ces géants mondiaux n'auraient absolument pas été impactés par des amendes moins élevées. «Le texte européen laisse toutefois une certaine latitude aux organes de contrôle nationaux comme le nôtre», précise Tine A. Larsen. La CNPD compte donc sanctionner chaque infraction au cas par cas, en évaluant la gravité des faits, l'ampleur de la violation, des dommages, du nombre de personnes touchées, etc. Par ailleurs, il est clair que nous serons moins tolérants avec de grandes entreprises disposant de toutes les ressources humaines et financières nécessaires qu'avec de petites PME, plus démunies à ce niveau. Le but, avec ces sanctions, est de faire mal. Mais pas de tuer l'entreprise non plus.»

Pour Mélanie Gagnon, certaines PME pourraient être sérieusement ébranlées en cas de sanction. «Si une start-up aux moyens limités se voit infliger une amende s'élevant à 4% de son chiffre d'affaires, cela peut mettre son activité en péril, explique-t-elle. En outre, certains secteurs d'activité bénéficient de marges plus faibles, notamment dans le domaine de l'alimentation. Une ponction de cette importance sur le chiffre d'affaires – pas sur le bénéfice donc – peut s'avérer très dangereuse» De quoi rappeler la nécessité de mettre en place les bonnes procédures au sein des PME, particulièrement fragiles en cas de sanction.

La CNPD joue sans doute le rôle le moins plaisant dans cette procédure, puisque c'est elle qui devra contrôler et infliger les sanctions aux entreprises, sous le contrôle du tribunal administratif et du Comité européen de protection des données. «Nous

ConnectedOffice

L'offre TOUT-EN-UN qui inclut :

- Internet
- Téléphonie fixe sur IP
- Mobile

et bien d'autres
services utiles pour
vous accompagner
dans votre business !

Prenez rendez-vous dans
l'un de nos Business Corners

Cloche d'Or : 2462 4001 • **Ettelbruck** : 2462 4002 • **Kirchberg** : 2462 4003

cisco
Meraki

POST
LUXEMBOURG

25 MAI 2018

Date de lancement de la nouvelle réglementation sur la protection des données

À ÉVITER

1. Faire l'autruche: ignorer le GDPR et ses conséquences potentielles pour votre entreprise est une mauvaise idée. Beaucoup d'entreprises pensent qu'elles ne traitent pas de données personnelles ou que leur société est trop petite pour être contrôlée. Mais cette attitude revient à jouer avec le feu.

2. Attendre: certaines PME sont paralysées par les exigences du GDPR. Toutefois, il est recommandé de ne plus attendre, car il reste moins de 3 mois avant son entrée en vigueur. En fonction des données que vous traitez et de ce que vous en faites, la mise en conformité de votre société pourrait prendre un certain temps. Anticipez donc pour éviter de vous retrouver au pied du mur.

effectuerons des contrôles proactifs, mais aussi réactifs, c'est-à-dire sur base de plaintes, indique Christophe Buschmann. Mais il ne faut pas voir ceux-ci comme une répression pure et simple. Notre volonté, c'est d'abord de sensibiliser les entreprises pour qu'elles se conforment. En outre, les contrôles nous permettront d'identifier les éléments qui n'auraient pas été bien compris, et donc de mieux cibler notre communication par la suite.»

DES OUTILS ET DES INFORMATIONS POUR AIDER LES PME

Pour bien comprendre les devoirs de votre entreprise en matière de protection des données, la CNPD et d'autres institutions luxembourgeoises ont déjà multiplié les communications, conférences et autres formations permettant d'informer au mieux les entreprises grand-ducales. «Les PME sont particulièrement vulnérables aux informations pas toujours exactes qui circulent, explique Thierry Lallemang. En effet, elles ne disposent pas des ressources humaines qui, en interne, pourraient leur permettre de démêler le vrai du faux. Je pense par exemple au droit à l'oubli dont la violation, en théorie, entraîne l'application d'une sanction s'élevant à 4% du chiffre d'affaires de l'entreprise. Beaucoup pensent qu'il s'agit d'un droit absolu. Or, c'est faux: il existe un bon nombre d'exceptions et les PME ne vont pas devoir gérer, du jour au lendemain, des dizaines de demandes de clients leur demandant de supprimer toutes les données les concernant. Il est donc particulièrement important que les PME s'intéressent à la question pour savoir exactement jusqu'où vont leurs devoirs concernant la protection des données. Notre site web rassemble les principales informations sur le sujet, et nous invitons les patrons de PME à aller y jeter un œil.»

On ne peut que vous recommander de suivre ce conseil si vous souhaitez entrer sereinement, dès le 25 mai prochain, dans cette nouvelle ère concernant la protection des données.