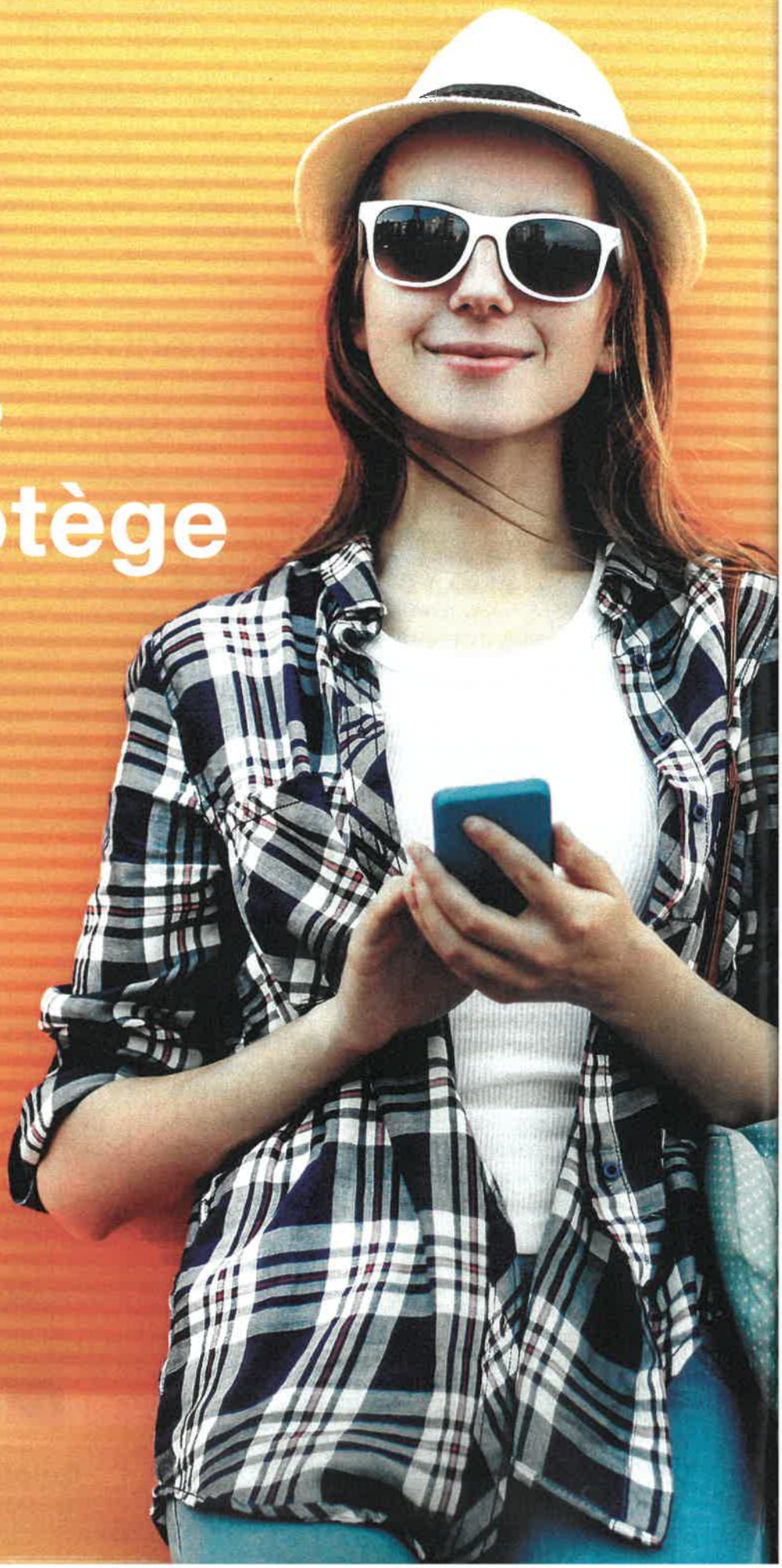
RGPD
L'Europe vous protège



RGPD

quelques points chauds

Le principe de responsabilité nécessite des procédures et des politiques de protection des données personnelles qui révolutionnent l'organisation de l'entreprise et sa culture.

Définition et anonymisation

La définition des données personnelles selon le RGPD est très large : *«Toute information se rapportant à une personne physique identifiée ou identifiable»*, soit des données de localisation, des identifiants en ligne... *«Le règlement est lourd et les transpositions en droit français sont plus sévères que dans les autres pays. Et il y a encore beaucoup d'incertitudes. L'anonymisation n'est pas une solution miracle, c'est une nécessité dans certains cas. Il s'agit non seulement de soustraire le nom mais de ne pas pouvoir retrouver la personne. Or, dès lors que vous avez des données qui sont découpées finement et peu de catégories, ce n'est pas suffisant, il est toujours possible de l'identifier»*, souligne Michel Piermay, président de Fixage, membre du Syndicat des actuaires conseils et actuaires experts indépendants et du Haut-conseil de l'Institut des actuaires et actuaire agrégé IA.

Le rôle du DPO

La nomination d'un DPO témoigne de la conduite d'une politique de responsabilité. Cependant, au sein des entreprises, il peut rapidement être débordé par l'ampleur de la tâche. *«Le DPO se retrouve avec un nombre incalculable de sollicitations : "Est-ce que je peux afficher tel élément sur un contrat? Je lance une étude sur un marché cible dans le cadre de la DDA ou de MIFID, qu'ai-je le droit de faire sur cet échantillon dans ce cadre?"»*, explique Dan Chelly, Senior Partner Risk Management chez Optimind.

La traçabilité

L'obligation de tenir un registre de traitement des données et de faire des analyses d'impact fait de la traçabilité des données une question centrale du RGPD. La sensibilisation des salariés est essentielle à la mise en conformité et les notions à maîtriser sont nombreuses : connaissance des procédures de collecte, de traitement, d'archivage et de destruction des données. *«Par ailleurs, les personnes doivent explicitement autoriser l'accès à leurs données pour un usage précis défini à l'avance : même l'utilisation ultérieure pour de simples statistiques est interdite s'il n'y a pas cette autorisation explicite préalable. Une fois traitées, les données doivent être détruites ou sécurisées de manière à n'être accessibles par exemple qu'à un nombre restreint d'interlocuteurs : contrôleurs, autorités antiblanchiment, fisc... Les actuaires doivent concilier traçabilité et protection des données»*, estime Michel Piermay.

Le consentement au cœur du débat

La définition du consentement est revue par le RGPD. Il doit être informé, libre et spécifique, c'est-à-dire qu'il ne peut pas être lié à l'acceptation d'un contrat. *«Les entreprises doivent également fournir une information sur le profiling avec le droit d'opposition au profiling. Cela s'applique particulièrement à l'analyse des risques ou au ciblage à des fins de marketing et implique de modifier les mentions d'information dans les contrats avec les assurés mais aussi dans tous les formulaires»*, précise Ariane Mole, avocate associée chez Bird & Bird et *co-head* de la pratique internationale en protection des données personnelles. Mais c'est surtout la question du retrait du consentement qui fait l'objet de discussions. *«Le groupe des Cnil européennes a récemment sorti des* guidelines *sur l'information des personnes concernant la transparence, qui indiquent que le retrait de consentement devrait avoir des conséquences y compris sur les traitements réalisés après qu'il a pris effet. Je pense qu'il est légitime que les assureurs en discutent avec la Cnil car il n'y a pas de raison de considérer que, lorsque la personne retire son consentement, cela annihile tous les traitements précédents, ce serait abusif et pourrait encourager la fraude»*, explique l'avocate.

NPA5 : les règles d'or pour les actuaires

Avant même l'entrée en vigueur du RGPD, l'Institut des actuaires s'est saisi de la question des données personnelles. Il est le premier institut au niveau international à avoir élaboré une norme professionnelle pour encadrer non seulement l'utilisation mais aussi la protection des données massives, des données personnelles et des données de santé à caractère personnel. La norme est entrée en vigueur le 1er janvier 2018.

- **Privilégier l'anonymisation.** La norme incite les actuaires à préférer l'usage de données personnelles anonymisées ou, à défaut, à rendre impossible la réidentification des individus.
- **Une durée de conservation limitée.** Les données personnelles doivent être conservées pour une durée déterminée. Un allongement de celle-ci doit faire l'objet d'une démarche spécifique, avec l'accord explicite du DPO.
- **Maîtriser les outils.** Les possibilités offertes sont énormes, tant en termes logiciels que de bases de données, mais elles ne doivent pas faire oublier la responsabilité de l'actuaire. En utilisant ces outils, il devra documenter son contrôle, utiliser des méthodes alternatives et faire état de ses doutes.
- **Éviter la discrimination.** L'actuaire doit vérifier que des variables discriminantes au regard des réglementations ne sont pas utilisées. Il doit également s'assurer de ne pas réaliser de discrimination tarifaire de façon indirecte du fait de variables externes.