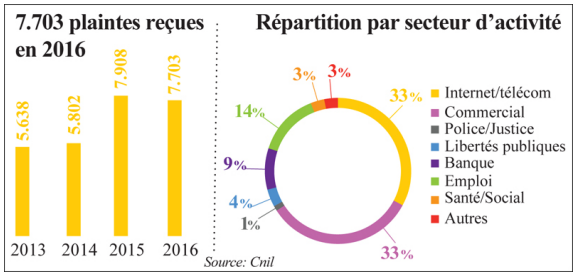
Protection des données personnelles : Ce qui change en 2018 avec le règlement RGPD

Protection des données personnelles : Ce qui change en 2018 avec le règlement RGPD

Le nouveau règlement européen sur la protection des données personnelles entrera en vigueur le 25 mai 2018. «Ce texte rénove la régulation européenne des données et offre à l'Europe la possibilité de récupérer sa souveraineté numérique…», indique Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (Cnil).

Le règlement renforce les droits des personnes à l'ère numérique
Les entreprises doivent se préparer au nouveau cadre juridique
Entrée en vigueur en mai 2018



En 2016, la Cnil a enregistré 7.703 plaintes (un peu moins que le record de 2015, 7.900 cas). Elles ont concerné principalement les secteurs Internet/télécom et le commerce
«La complexité du règlement avec ses 99 articles et ses 200 considérants ne doit pas masquer pour autant l'essence du texte qui consiste à renforcer la place centrale de l'individu dans l'univers des données», dit-elle. Pour le cas de la France, un projet de loi devra être déposé au Parlement au plus tard en juin 2017 pour garantir une meilleure application du règlement.
■ **Nouveau cadre juridique:** Le règlement européen constitue une évolution du cadre juridique de la protection des données et permet de construire une régulation commune sur l'ensemble du territoire de l'Union. Globalement, le texte renforce l'obligation des organismes publics et privés de protéger les données personnelles de leurs utilisateurs et clients. En pratique, le droit européen s'appliquera chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet. La territorialité du droit européen se construit donc désormais autour de la personne. Cela se traduit par l'apparition de nouveaux droits (portabilité des données, limitation du traitement, réparation d'un dommage matériel ou moral…). Les obligations en matière d'information sont également renforcées notamment en cas de faille de sécurité.
■ **L'expression du consentement renforcée:** Les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambiguë. Le but de cette évolution est d'améliorer l'information qui doit être claire et accessible aux personnes concernées par les traitements de données.
■ **Portabilité des données:** Ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme facilement réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit de redonner aux personnes la maîtrise de leurs données et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.
■ **Protection des enfants:** L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les Etats membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.
■ **Biométrie:** Les données biométriques doivent faire l'objet d'une vigilance particulière. Le règlement européen a consacré le caractère particulier de ces données en les qualifiant de données «sensibles», au même titre que les données concernant la santé, les opinions politiques ou les convictions religieuses, dont le traitement est par principe interdit sauf dans certains cas limitativement énumérés.
■ **Open data:** Si elle ne concerne pas initialement la protection des données à caractère personnel, le nouveau contexte numérique implique de mieux la prendre en compte. Et ce notamment au niveau de la mise à disposition des données comme de leur réutilisation, la protection de la vie privée. Le nouveau cadre juridique permet cette conciliation.
Les sanctions s'alourdissent
Les autorités de protection pourront imposer des amendes administratives (jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial d'une entreprise). Ces sanctions pécuniaires pourront être prises en complément ou à la place de nombreuses mesures correctrices (ordonner de communiquer à la personne concernée une violation de données, la rectification ou encore la suspension de flux de données vers un pays tiers). Effacer des données ou limiter le traitement ou encore retirer une certification sont sur la liste des dispositions… Ces mesures et sanctions ne seront plus limitées au responsable de traitement mais pourront également être prises à l'égard d'un sous-traitant. Dans l'hypothèse de traitements transfrontaliers, la Cnil travaillera avec d'autres autorités de protection afin qu'une seule décision de sanction soit adoptée par l'autorité chef de file.
[Article original de Fatim-Zahra TOHRY]

Réagissez à cet article

Source : *Protection des données personnelles: Ce qui change | L’Economiste*