LE RGPD ET LES SOCIÉTÉS DE MAINTENANCE INFORMATIQUE

En 2019, 7 000 actes d'investigation ont été conduits par la CNIL. Une attention particulière a été portée aux conditions dans lesquelles un prestataire traite des données personnelles, pour le compte d'un responsable de traitement. Des contrôles ont donc été effectués, sur cette thématique, auprès de 15 fournisseurs de services et solutions informatiques. Il en est ressorti que certains acteurs pensaient à tort ne pas être soumis au RGPD, considérant que, ne réalisant qu'une prestation de maintenance, leur accès aux données personnelles n'étaient que ponctuel. Or, l'accès est par lui-même un traitement et donc l'entreprise soumise aux dispositions du RGPD.

En effet, sont des sous-traitants et notamment concernés par le RGPD les prestataires de services informatiques (hébergement, maintenance, ...), les intégrateurs de logiciels, les sociétés de sécurité informatique, les entreprises de service du numérique ou anciennement SSII qui ont accès aux données.

Or, le RGPD impose des obligations spécifiques aux sous-traitants qui doivent aider les responsables de traitement dans leur démarche permanente de mise en conformité, il en est ainsi – notamment – de l'obligation d'assistance. À cet égard, il est opportun pour les sous-traitants de détailler dans leur contrat le contenu exact de leur obligation d'assistance et d'indiquer que toute prestation allant au-delà donnera lieu à facturation.

En effet, il est désormais impératif qu'un contrat soit rédigé entre ce sous-traitant et le responsable du traitement, lequel doit indiquer les obligations incombant au sous-traitant pour protéger la sécurité et la confidentialité des données.

Le sous-traitant doit offrir « *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 présent règlement et garantisse la protection des droits de la personne concernée* » (art. 28 du RGPD).

Ainsi, le sous-traitant doit mettre en œuvre des mesures de sécurité dont, par exemple – parmi celles s'adressant

Christelle REYNO

plus spécifiquement aux prestataires de maintenance :

• les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services
• les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique

On pourra notamment citer les mesures suivantes :

- La signature d'un engagement de confidentialité ou prévoir dans les contrats de travail une clause de confidentialité spécifique concernant les données à caractère personnel ;
- La mise en place d'une gestion des habilitations permettant de limiter les accès aux seules données dont un utilisateur a besoin ;
- L'authentification des utilisateurs ;
- Le traçage / la journalisation des accès, notamment enregistrer les interventions de maintenance dans une main courante ;
- La mise en place de sauvegardes régulières hors site pour limiter l'impact d'une disparition non désirée de données (avec test régulier de restauration des sauvegardes) ;
- L'archivage des données qui ne sont plus utilisées au quotidien mais qui n'ont pas encore atteint leur durée limite de conservation, par exemple parce qu'elles sont conservées afin d'être utilisées en cas de contentieux.

Le sous-traitant doit également mettre à la disposition de son client toutes les informations nécessaires pour démontrer le respect de ses obligations (à cet égard, le responsable de traitement peut solliciter un audit du sous-traitant) et tenir un registre qui recense ses clients et décrit les traitements qu'il effectue pour leur compte.

Le sous-traitant doit notamment veiller à ce que dès leur conception, ses outils, produits, applications ou services, intègrent de façon effective les principes relatifs à la protection des données et à ce que ceux-ci garantissent par défaut, que seules sont traitées les données nécessaires à la finalité du traitement.

Aux termes de l'article 84 du RGPD, les violations des obligations du sous-traitant font l'objet d'amendes administratives pouvant s'élever jusqu'à 10 000 000 € ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Il doit être rappelé que lorsqu'un responsable du traitement et un sous-traitant participent au même traitement et, lorsqu'ils sont responsables d'un dommage causé par le traitement, chacun est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective. Il est donc impératif que le sous-traitant connaisse précisément ses obligations et participe activement à la rédaction du contrat, notamment sur les aspects de responsabilité.

En outre, le sous-traitant a intérêt à ce que les instructions du responsable du traitement pour le compte duquel il intervient soient précisément définies dans le contrat le liant ; à défaut, ils pourraient engager leur responsabilité de manière solidaire aux côtés du responsable du traitement.

Maître Christelle REYNO (du cabinet LEGALPROTECH AVOCATS), DPO certifié et anciennement juriste en SSII (ESN), assiste notamment ses clients, responsables de traitement, comme sous-traitants, en ce sens.