N° 15
JANVIER 2019

Matmut
PROTECTION JURIDIQUE

La lettre *d'information* des professionnels

© palau83 - Fotolia

PROTECTION DES DONNÉES PERSONNELLES

La loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 a été modifiée afin de la rendre compatible avec la réglementation européenne, notamment le Règlement général sur la protection des données. Applicable à compter du 25 mai 2018, le RGPD a renforcé les droits des personnes physiques sur leurs données personnelles et créé de nouvelles obligations à la charge des acteurs traitant ces données.

QUEL EST LE CHAMP D'APPLICATION DU RGPD ?

Le RGPD concerne les entreprises, les organismes publics, les collectivités territoriales et les associations, indépendamment de leur taille ou de leur activité, qui traitent des données personnelles de personnes (prospect, client, fournisseur, salarié…) se trouvant sur le territoire de l'Union européenne.

Sont concernés par le RGPD les responsables de traitement (personne physique ou morale, autorité publique… qui détermine les finalités et les moyens du traitement) et les sous-traitants (personne physique ou morale, autorité publique… qui traite des données pour le compte du responsable de traitement).

QU'EST-CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL ?

Il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable, par exemple :
- nom, prénom, date de naissance,
- adresse personnelle,
- numéro de téléphone personnel ou professionnel,
- numéro client,
- adresse mail personnelle ou professionnelle (comportant des éléments pouvant identifier une personne physique, le patronyme par exemple),
- numéro de carte d'identité, de sécurité sociale,
- donnée biométrique (donnée génétique, empreinte digitale)
- adresse de protocole internet (IP), cookie.

QU'EST-CE QU'UN TRAITEMENT DE DONNÉES PERSONNELLES ?

Il s'agit de toute opération ou ensemble d'opérations sur des données à caractère personnel de personnes physiques, effectuée informatiquement ou manuellement, quel que soit le procédé utilisé, par exemple :
- la collecte de données via un formulaire, un questionnaire, un fichier,
- l'enregistrement d'images de vidéo surveillance,
- la conservation,
- la modification,
- la consultation,
- l'extraction,
- la communication par transmission, diffusion.

COMMENT SE METTRE EN CONFORMITÉ AVEC LA RÉGLEMENTATION SUR LA PROTECTION DES DONNÉES PERSONNELLES ?

Les responsables de traitement et leurs sous-traitants doivent s'assurer et pouvoir démontrer que le traitement est effectué conformément au RGPD. Les formalités préalables auprès de la CNIL (déclarations de fichiers et autorisations préalables) sont, sauf exception, supprimées.

Parmi les actions à mettre en œuvre :

1. Le responsable du traitement et le sous-traitant doivent désigner un Délégué à la Protection des Données (DPD) :
- si leur activité fait partie du secteur public,
- si leur activité principale les amène à réaliser un suivi régulier et systématique de personnes à grande échelle,
- si leur activité principale amène le traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et infractions.

Le délégué a notamment pour mission :
- d'informer et de conseiller le responsable du traitement ou le sous-traitant et de sensibiliser leurs employés,
- de contrôler le respect du règlement européen et du droit français en matière de protection des données,
- de coopérer avec la CNIL.

2. Le responsable du traitement doit tenir un registre des traitements des données sous une forme écrite, papier ou électronique. Ce registre permet de préciser notamment :
- son nom et ses coordonnées,
- la finalité du traitement (à quoi le fichier va-t-il servir ?),
- les catégories de données traitées (elles doivent être nécessaires à la finalité),

- les personnes qui ont accès aux données (seules les personnes habilitées doivent avoir accès aux données),
- les délais de conservation des différentes catégories de données (ils doivent être justifiés).

Cette obligation de tenue d'un registre des traitements ne s'applique pas aux entreprises ou organisations comptant moins de 250 employés sauf si les traitements qu'elles effectuent :

- sont susceptibles de comporter un risque pour les droits et libertés des personnes concernées (vidéosurveillance, géolocalisation par exemple),
- ne sont pas occasionnels : gestion de la paie, fichiers clients ou fournisseurs,
- portent sur des catégories particulières de données (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données de santé et biométriques…) ou des données relatives à des condamnations et infractions pénales.

Le sous-traitant doit tenir, dans les mêmes conditions, un registre des activités de traitement qu'il effectue pour le compte de son client.

La CNIL propose sur son site un modèle de registre de traitements.

3. Le responsable du traitement et le sous-traitant doivent sécuriser les données et notifier, dans certains cas, la violation de données à caractère personnel à la Commission Nationale de l'Informatique et des Libertés (CNIL) :

Toutes les mesures techniques et organisationnelles appropriées pour assurer la sécurité du traitement doivent être prises : pseudonymisation et chiffrement des données, mise à jour des antivirus, mots de passe complexes et changement régulier de ces derniers, sécurisation des locaux, habilitations…

La CNIL doit être informée, si possible dans les 72 heures au plus tard, de toute destruction, perte, altération, divulgation ou accès non autorisé à des données personnelles susceptible de présenter un risque pour les droits et libertés des personnes concernées (téléservice disponible sur son site).

Les personnes concernées par cette violation doivent également en être informées dans les meilleurs délais, par tout moyen permettant d'en apporter la preuve (lettre recommandée avec AR, courrier électronique…), si cette dernière est susceptible d'engendrer un risque élevé pour leurs droits et libertés (usurpation d'identité par exemple).

Le sous-traitant doit notifier au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

4. Le responsable du traitement doit respecter les droits des personnes et leur permettre d'exercer ceux-ci.

La personne concernée par la collecte de données personnelles (souscription d'un contrat, achat en ligne, ouverture d'un compte bancaire…) doit recevoir, au moment de cette collecte ou en différé si cette collecte est indirecte, plusieurs informations dont :

- l'identité et les coordonnées du responsable du traitement et, le cas échéant, du DPD,
- les finalités du traitement (gestion du recrutement, gestion de la clientèle, enquête de satisfaction…),
- le fondement juridique de ce traitement : consentement de la personne concernée au traitement de ses données personnelles, exécution d'un contrat auquel elle est partie ou sauvegarde de ses intérêts vitaux, respect d'une obligation légale à laquelle le responsable du traitement est soumis…,
- les destinataires des données,
- la durée de conservation des données,
- les droits sur ses données personnelles qu'elle peut exercer auprès du responsable du traitement :
  - accès à ses données faisant l'objet d'un traitement,
  - rectification de ses données incorrectes, inexactes ou incomplètes,
  - effacement de ses données dans des cas précis,
  - limitation du traitement de ses données dans des cas précis,
  - opposition au traitement de ses données,
  - récupération de ses données pour un usage personnel ou pour les transférer à un autre organisme (droit à la portabilité),
  - retrait de son consentement au traitement de ses données, à tout moment, lorsque celui-ci a été recueilli, s'il s'agit du fondement juridique du traitement,
- le droit d'introduire une réclamation auprès de la CNIL ou une action de groupe via une association agréée de défense des consommateurs si la personne considère qu'il y a manquement à la réglementation,
- les modalités d'exercice de ses droits : formulaire de contact sur le site internet de l'entreprise, espace personnel client, service dédié…

QUELS SONT LES RISQUES ENCOURUS EN CAS DE NON-RESPECT DU RGPD ?

- Atteinte à l'image et à la réputation de la personne morale,
- amende administrative prononcée par la CNIL selon la gravité du manquement :
  - jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent pour une entreprise ou jusqu'à 10 000 000 d'€,
  - et, pour les manquements les plus graves, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent pour une entreprise ou jusqu'à 20 000 000 d'€.
- sanctions pénales : en fonction de la gravité de l'infraction, jusqu'à 5 ans d'emprisonnement et 300 000 € d'amende pour les personnes physiques et 1 500 000 € d'amende pour les personnes morales,
- mise en jeu de la responsabilité civile de la personne morale par toute personne ayant subi un dommage matériel ou moral du fait d'une atteinte à ses données personnelles et condamnation éventuelle à des dommages et intérêts.