

LE POINT SUR...

Règlement européen sur la protection des données : ce qui change pour les professionnels

Le nouveau règlement européen sur la protection des données personnelles entrera en application le 25 mai 2018. L'adoption de ce texte doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique.

LA RÉFORME DE LA PROTECTION DES DONNÉES POURSUIT TROIS OBJECTIFS :

1. **Renforcer les droits des personnes**, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures.
2. **Responsabiliser les acteurs traitant des données** (responsables de traitement et sous-traitants).
3. **Crédibiliser la régulation** grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.

UN CADRE JURIDIQUE UNIFIÉ POUR L'ENSEMBLE DE L'UE

Le texte adopté est un règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres. Le même texte s'appliquera donc dans toute l'Union.

Le règlement est applicable à partir du 25 mai 2018. Dès lors, les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du règlement.

UN CHAMP D'APPLICATION ÉTENDU

► *Le critère du ciblage*

Le règlement s'applique, dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler ».

En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet.

► *La responsabilité des sous-traitants*

Par ailleurs, alors que le droit de la protection des données actuel concerne essentiellement les « responsables de traitements », c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement. Toutes les entreprises sont donc potentiellement concernées.

LE POINT SUR...

Règlement européen sur la protection des données : ce qui change pour les professionnels

UN RENFORCEMENT DES DROITS DES PERSONNES

Le règlement européen renforce les droits des personnes et facilite l'exercice de ceux-ci.

► **Consentement renforcé et transparence**

Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.

L'expression du consentement est définie : 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.

► **De nouveaux droits**

Le droit à la portabilité des données : ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers.

Des conditions particulières pour le traitement des données des enfants : pour la première fois, la législation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans.

Introduction du principe des actions collectives : tout comme pour la législation relative à la protection des consommateurs, les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données auront la possibilité d'introduire des recours collectifs en matière de protection des données personnelles.

Un droit à réparation des dommages matériel ou moral : toute personne ayant subi un dommage matériel ou moral, du fait d'une violation du présent règlement, a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

De nouveaux outils de conformité à mettre en oeuvre :

- La tenue d'un registre des traitements mis en œuvre,
- La notification de failles de sécurité (aux autorités et personnes concernées),
- La certification de traitements,
- L'adhésion à des codes de conduites,
- Le DPO (Délégué à la protection des données),
- Les études d'impact sur la vie privée (EIVP).

De nouvelles sanctions possibles en cas de non-conformité.

Les autorités de protection peuvent notamment :

- Prononcer un avertissement,
- Mettre en demeure l'entreprise,
- Limiter temporairement ou définitivement un traitement,
- Suspendre les flux de données,
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes,
- Ordonner la rectification, la limitation ou l'effacement des données.

S'agissant des amendes administratives, elles peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 M€, ou, dans le cas d'une entreprise, **de 2 % jusqu'à 4 % du chiffre d'affaires annuel mondial**, le montant le plus élevé étant retenu.

**Pour être à jour de vos obligations,
contactez dès à présent
votre expert-comptable !**