Document sur les changements clés du RGPD

Le document suivant a été créé à partir du site Web : https://eugdpr.org/the-regulation/.
Tous les textes ont été extraits de ce site Web, non créés par le partenariat DIGIT.

Le but du RGPD est de protéger tous les citoyens de l'Union européenne contre les atteintes à la vie privée et les fuites de données dans un monde axé sur l'échange de données. Le but du RGPD est de protéger tous les citoyens de l'Union européenne contre les atteintes à la vie privée et les fuites de données dans un monde axé sur l'échange de données.

Portée territoriale accrue (applicabilité extraterritoriale)

- Le changement le plus important dans le paysage réglementaire de la confidentialité des données est certainement lié à la **compétence élargie du RGPD**, dans la mesure où il s'applique à toutes les sociétés qui traitent les données à caractère personnel de personnes concernées résidant dans l'Union, quel que soit le siège de l'entreprise.
- Auparavant, l'applicabilité territoriale de la directive était ambiguë.
- Le RGPD s'applique également au traitement des données à caractère personnel des personnes concernées dans l'UE par un responsable du traitement ou un sous-traitant non établi dans l'UE, lorsque les activités consistent à : offrir des biens ou des services aux citoyens de l'UE (que le paiement soit exigé ou non) et la surveillance des comportements au sein de l'UE.

Pénalités

- Les organisations en infraction avec le RGPD peuvent recevoir une amende pouvant **atteindre 4 % du chiffre d'affaires global annuel** ou **20 millions d'euros** (le montant le plus élevé). Il s'agit de l'amende maximale pouvant être infligée pour les infractions les plus graves, par exemple ne pas disposer du consentement suffisant du client pour traiter les données ou violer les concepts de Privacy by Design.

Consentement

- Les **conditions du consentement ont été renforcées** et les entreprises ne peuvent plus utiliser de longues conditions générales de ventes qui sont pleines de jargon juridique.
- La demande de consentement doit être présentée sous une forme intelligible et facilement accessible, l'objet du traitement des données doit être explicité avec ce consentement.
- Le consentement doit être clair, distinct des autres questions et présenté sous une forme intelligible et facilement accessible, dans un langage clair et simple.
- Il doit être aussi facile de retirer son consentement que de le donner.

Notification de violation de données

- En vertu du RGPD, les notifications de violation de données sont désormais obligatoires dans tous les États membres où une violation de données risque « d'entraîner un risque pour les droits et libertés des personnes ».

- Cela doit être fait dans les 72 heures après avoir pris connaissance de la violation de données. Les responsables du traitement de données sont également tenus d'informer leurs clients, les contrôleurs, « sans retard injustifié » après avoir pris connaissance d'une violation de données.

Droit d'accès aux données

- Une partie des droits étendus des personnes concernées définis par le RGPD est le droit des personnes concernées d'obtenir du responsable du traitement de l'information de confirmer si les données à caractère personnel les concernant sont traitées, où et dans quel but.
- En outre, le responsable du traitement fournit gratuitement une copie des données à caractère personnel sous forme électronique. Ces nouveautés constituent un changement radical vers la **transparence des données** et la responsabilisation des personnes concernées.

Droit à l'oubli numérique

- Également appelé effacement des données, le droit à l'oubli donne à la personne concernée le droit de demander au responsable du traitement d'effacer ses données personnelles, de cesser toute diffusion des données et, éventuellement, de faire en sorte que des tiers en interrompent le traitement.

Portabilité des données

- Le RGPD introduit la portabilité des données — le droit pour une personne concernée de recevoir les données personnelles qui la concernent.

AGENTS DE PROTECTION DES DONNÉES

- En vertu du RGPD, il n'est pas nécessaire de soumettre des notifications/enregistrements à chaque APD locale pour les activités de traitement de données, il n'est pas non plus obligatoire de notifier/obtenir l'approbation des transferts sur la base des clauses du contrat type (MCC).
- Comme expliqué ci-dessous, il **existe des exigences internes** en matière de conservation des enregistrements, et la nomination de DPO (agent de protection des données) n'est obligatoire que pour ceux dont les activités principales consistent en des opérations de traitement qui nécessitent **un contrôle régulier et systématique des personnes concernées à grande échelle ou des catégories de données ou des données relatives à des condamnations pénales et à des infractions.**
- Fait important, l'agent de protection des données :
  - Doit être nommé en fonction de ses qualités professionnelles et, en particulier, des connaissances spécialisées dans le domaine de la protection des données.
  - Il peut être un membre du personnel ou un prestataire externe.
  - Ses coordonnées doivent être fournies à l'autorité de protection des données compétente.
  - Il doit être doté des ressources appropriées pour mener à bien ses tâches et maintenir ses connaissances spécialisées.
  - Il doit rendre compte directement au plus haut niveau de la direction.

- Il ne doit pas effectuer d'autres tâches qui pourraient faire naître un conflit d'intérêts.

Veuillez répondre aux questions suivantes :

1. Que pensez-vous de ces recommandations ? Qu'avez-vous le plus retenu ?

2. Avez-vous été concerné par cela dans votre vie personnelle ou professionnelle ? Si oui, comment ?

3. Y a-t-il autre chose que vous voudriez ajouter ou changer au règlement RGPD ?