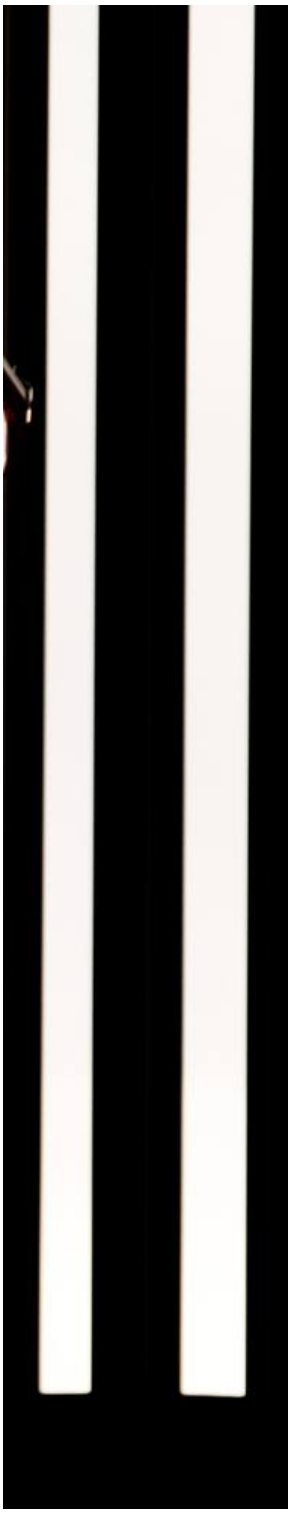


ARTICLE

M-12 : APERÇU DE L'ENSEMBLE DES 12 CHANGEMENTS CLÉS LIÉS À L'APPLICATION DU RGPD

IT et données personnelles Droit de la concurrence, consommation et distribution Contrats commerciaux et internationaux | 24/05/17 | Florence Chafiol

TECH & DIGITAL

Le **Règlement européen 2016/679** sur la protection des données personnelles (« RGPD ») du 27 avril 2016 sera dans **UN AN**, le 25 mai 2018, le socle de la règlementation applicable en matière de données à caractère personnel au sein de l'Union Européenne. Vous trouverez ci-dessous, les changements les plus significatifs du RGPD :

1 L'EXTRA TERRITORIALITÉ DU RGPD

Il sera difficile d'y échapper puisque le RGPD s'applique aux traitements :

- ✓ Effectués par tous les responsables du traitement (RT) ou **sous-traitants (ST)** établis sur le territoire de l'UE que le traitement ait lieu ou non dans l'Union (critère de l'établissement) ;
- ✓ Effectués par les **RT** ou **les ST, établis hors de l'UE**, qui proposent des biens ou des services sur le territoire de l'UE ou qui suivent le comportement des personnes (profilage) au sein de l'UE (critère du ciblage).

2 LES BASES LÉGALES DE TRAITEMENT ET CONSENTEMENT

- ✓ La base légale du traitement (notamment consentement, exécution d'un contrat ou intérêt légitime) doit être indiquée aux personnes concernées lors de la collecte des données ;
- ✓ Consécration de la doctrine de la CNIL dans la définition et l'appréciation d'un consentement valide. Les exigences pour baser un traitement sur le consentement sont renforcées par le RGPD (par exemple, il n'est plus possible de considérer que l'acceptation de la « *privacy policy* » est une base légale valide pour traiter les données, de même que l'acceptation des CGV ou des CGU) ;
- ✓ Lorsque le traitement est basé sur l'intérêt légitime du RT, celui-ci devra être en mesure de justifier qu'il a effectué une « balance des intérêts » entre ses intérêts et la préservation des droits et libertés fondamentaux des personnes concernées.

6 L'ANALYSE D'IMPACT RELATIVE À LA VIE PRIVÉE (DPIA)

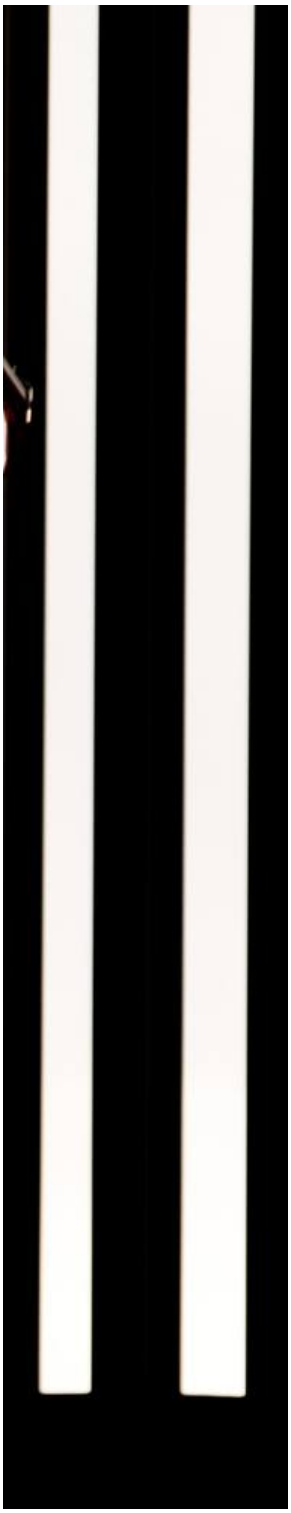
- ✓ DPIA obligatoires dans certains cas : pour tous les traitements à risque, le RT devra réaliser une analyse d'impact ;
- ✓ En cas de risque élevé avéré, il devra consulter l'autorité de contrôle avant la mise en œuvre du traitement.

7 SÉCURITÉ ET NOTIFICATION DES VIOLATIONS DE SÉCURITÉ

- ✓ Principe général de notification des violations de données à caractère personnel ;
- ✓ Notification par le RT (plus seulement les opérateurs téléphoniques) de la violation à l'autorité de contrôle dans les 72h ;
- ✓ Obligation d'information des personnes concernées par le traitement en cas de risques élevés pour leurs droits et libertés ;
- ✓ Le ST doit notifier toute violation au RT.

8 LES CERTIFICATIONS ET CODES DE CONDUITES

- ✓ Possibilité renforcée de recourir à ces mécanismes pour prouver la conformité des traitements ;
- ✓ Les codes seront élaborés par les acteurs représentatifs d'un secteur d'activité puis soumis à l'autorité de contrôle pour avis et publication.



3 LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES PERSONNELLES (DPO)

- ✓ Obligation de désigner un DPO dans certains cas : (i) le traitement est effectué par une autorité ou un organisme public ; (ii) les activités de base du RT ou du ST consistent en des **traitements de données à grande échelle** soit dans le cadre du suivi régulier et systématique de personnes (profilage), soit de données sensibles ou de données relatives à des infractions ou condamnations pénales ;
- ✓ Possibilité de recourir à un DPO externe sans limitation ;
- ✓ Mission d'information et de conseil du RT ou du ST, de contrôle du respect de la législation, point de contact pour l'autorité de contrôle, etc. ;
- ✓ Doit disposer de formation et de moyens pour exercer sa mission.

4 AUTORITÉ CHEF DE FILE ET CEPD

- ✓ Chaque autorité est compétente pour exercer ses missions et pouvoirs dans son pays ;
- ✓ Pour traitements transfrontaliers (ex : une entreprise ayant des filiales dans plusieurs États membres de l'UE), l'autorité chef de file du RT sera celle du lieu de son établissement principal. Toutefois, des exceptions existent dans le cadre desquelles d'autres autorités de contrôle nationales pourront coopérer ;
- ✓ Le Comité Européen de Protection des Données (CEPD) remplace le G29 et tranche, le cas échéant, les différends entre les autorités de contrôle.

5 L'"*ACCOUNTABILITY*" ET LA GOUVERNANCE DES DONNÉES

- ✓ Abandon de la logique de « formalités préalables » (même si certaines pourraient subsister, notamment l'autorisation préalable), obligation de tenue d'un registre ;
- ✓ Principe de conformité et de responsabilisation des acteurs (*accountability*) se traduisant par l'obligation d'être en mesure de démonter à tout moment la mise en place de mesures de protection appropriées et de conformité au RGPD (mécanismes, procédures, DPIA, etc.).

9 LE RÉGIME ET LES NOUVELLES OBLIGATIONS DES SOUS-TRAITANTS

- ✓ Application directe de certaines obligations aux ST ;
- ✓ Responsabilité directe du ST pour certains manquements et responsabilité conjointe et solidaire avec le RT pour les demandes d'indemnisation des personnes concernées ;
- ✓ Obligation de tenue d'un registre des activités de traitement ;
- ✓ Peut être amené à désigner un DPO ;
- ✓ Obligation d'assistance au RT pour assurer la conformité au RGPD; (sécurité, DPIA, destruction…).

10 INFORMATION DES PERSONNES ET TRANSPARENCE

- ✓ Accroissement du nombre d'informations à fournir aux personnes lors de la collecte des données personnelles ;
- ✓ Obligation de transparence lors de la communication (format lisible, clair et intelligible des informations).

11 DROITS DES PERSONNES

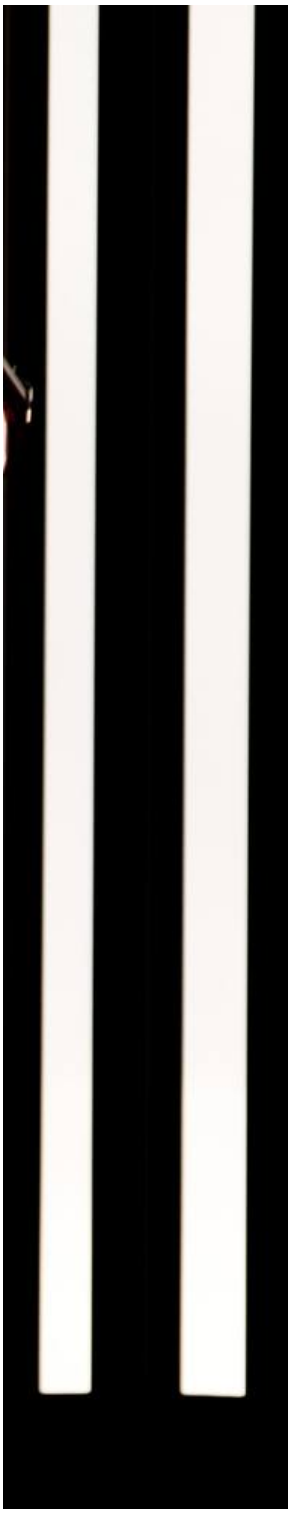
- ✓ Les droits déjà existants persistent ;
- ✓ Droit à la portabilité (obtenir ses données dans un format lisible) ;
- ✓ Droit à l'oubli ;
- ✓ Droit à la limitation du traitement ;
- ✓ Droit d'introduire une réclamation auprès de l'autorité de contrôle (déjà existant en pratique, mais non mentionné en tant que tel) ;
- ✓ Droit à un recours juridictionnel contre le RT **ou le ST** ;
- ✓ Droit à réparation du dommage matériel ou moral du fait d'une violation du RGPD (responsabilité conjointe et solidaire du RT et du ST).

12 SANCTIONS

- ✓ Augmentation du montant des sanctions ;
- ✓ 2 paliers de sanction distincts en fonction du manquement ;
- ✓ Jusqu'à 10 millions et 2% du chiffre d'affaires mondial annuel de l'exercice précédent (le montant le plus élevé étant retenu) : ex : non désignation de DPO, absence de registre, notification des failles de sécurité, etc. ;
- ✓ Jusqu'à 20 millions et 4% du chiffre d'affaires mondial annuel de l'exercice précédent (le montant le plus élevé étant retenu) : ex : non-respect des obligations sur les transferts, mauvaise information des personnes, etc.

L'ensemble de ces **changements clés sera abordé en détails dans nos prochaines newsletters,** ainsi que dans le cadre de nos formations.

En lien avec les changements ci-dessus, vous trouverez ci-dessous un calendrier de mise en conformité constituant une suggestion de plan d'action des différentes mesures à mettre en place jusqu'à la date d'entrée en application du règlement (25 mai 2018). Ces actions s'inscrivent dans la durée et devront être adaptées, à la fois à votre structure



interne et aux évolutions et prises de positions des autorités compétentes.