IP, IT & Media News from Luxembourg

Octobre 2016

Réforme Europeenne de la protection des données

Après 4 années de négociations, le Paquet « Protection des données à caractère personnel », établissant de nouvelles règles européennes sur la vie privée à l'ère du numérique, a été officiellement adopté par le Parlement européen et le Conseil en avril 2016. Vous trouverez ci-après quelques précisions sur le contexte et les points essentiels de la réforme, ainsi qu'une checklist pour vous aider à respecter ces nouvelles règles.

Contexte de la réforme

La Commission européenne a lancé, en 2012, une réforme des règles régissant la protection des données à caractère personnel dans l'Union européenne (« *UE* »). Après 4 années de négociations, le Parlement européen, le Conseil et la Commission européenne ont trouvé, au mois d'avril 2016, un accord final sur la réforme de la protection des données, qui comprend deux instruments juridiques :

- **Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale. Les Etats membres disposent d'un délai expirant le **6 mai 2018** pour la transposer dans leur droit national.
- **Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016**, dit Règlement Général sur la Protection des Données, ou « *RGPD* ». Ce règlement réforme et abroge les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel telles que prévues par la directive 95/46/EC. Le RGPD est entré en vigueur le 24 mai 2016 et sera **directement applicable dans tous les Etats membres à partir du 25 mai 2018.**

La directive vie privée et communications électroniques[1], qui précise les modalités d'application de certains principes de la directive 95/46/CE sur la protection des données au secteur des communications électroniques, sera aussi révisée dans les années à venir.

[1] Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

Objectifs du RGPD

Le RGPD vise à renforcer les droits fondamentaux des citoyens et à créer un cadre juridique harmonisé pour la protection des données personnelles adapté à l'économie numérique, tout en allégeant les formalités administratives pour les responsables du traitement.

La réforme conserve les grands principes de la protection des données (à savoir loyauté, licéité, transparence, intégrité, confidentialité, exactitude), tout en introduisant de nouvelles règles consolidant les libertés individuelles et relevant les défis des opérations de traitement à haut risque, telles que le « *big data* ».

A quoi s'attendre ?

Une réforme générale

Un ensemble de règles harmonisées au sein de l'UE, communes à tous les Etats membres, apportant clarté, cohérence et sécurité juridique quant aux règles applicables. Le RGPD offre toutefois aux Etats membres la faculté d'adapter leur législation à des problèmes spécifiques (notamment le régime des sanctions pénales).

Un champ d'application territorial plus large: le nouveau règlement sera applicable aux responsables du traitement et sous-traitants établis dans l'UE, mais également à ceux établis dans un Etat tiers, lorsque les activités de traitement concernent (i) l'offre de biens ou de services à des résidents de l'UE ou (ii) le suivi de leur comportement au sein de l'UE.

Un cadre consolidé

- **Droits étendus pour les personnes concernées**

Droit à l'oubli: le RGPD précise les conditions d'exercice du droit à l'oubli[2].

Droit à la portabilité des données d'un responsable du traitement à un autre.

Voies de recours: les possibilités de réparation judiciaire pour les personnes concernées ont été élargies. En cas de violation des règles du RGPD, elles auront droit à un recours juridictionnel effectif et à une réparation non seulement de la part du responsable du traitement (comme cela est le cas actuellement), mais aussi de la part du sous-traitant.

Protection spécifique des enfants, obligeant les parents à fournir leur consentement préalable.

- **Obligations accrues pour les responsables du traitement et les sous-traitants**

Standards plus élevés concernant le consentement des personnes physiques au traitement de leurs données.

Informations extensives sur le traitement devant être fournies par le responsable du traitement (durée de conservation des données, détail des transferts hors UE, et base juridique du traitement).

Suppression des notifications/autorisations préalables des traitements de données auprès des autorités nationales de protection des données.

Ajustement des obligations des responsables du traitement/sous-traitants en fonction du risque de leurs activités pour la protection des données personnelles :

✓ Réalisation d'une **Analyse d'Impact relative à la Protection des Données** *(« AIPD »)* préalablement aux activités de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

✓ Tenue de **registres pour les activités de traitement,** devant contenir, *inter alia*, une description des données traitées, les motifs qui sous-tendent le traitement et une description des mesures de sécurité techniques et organisationnelles adoptées.

✓ Adoption de **mesures techniques et organisationnelles** (politiques internes, pseudonymisation, etc.) pour répondre aux exigences du RGPD.

[2] Tel qu'énoncé précédemment par la Cour de justice de l'UE dans l'arrêt Google Espagne (C-131/12)

✓ Désignation d'un **délégué à la protection des données** *(« DPD »)* pour les responsables du traitement et les sous-traitants qui (i) sont des autorités publiques, (ii) effectuent un suivi régulier et systématique à grande échelle des personnes concernées, ou (iii) traitent des données sensibles ou liées à des condamnations pénales.

Procédures spécifiques en cas de **violation de données à caractère personnel** devant être suivies tant par le responsable du traitement que le sous-traitant.

Des sanctions plus sévères

Les autorités de contrôle pourront imposer, au cas par cas, des sanctions administratives dissuasives aux responsables du traitement et aux sous-traitants en cas de violation du RGPD. Certaines violations seront punies d'une amende pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Le RGPD permet aussi aux Etats membres de réglementer les sanctions pénales.

Moins de deux ans pour se conformer!

Le RGPD sera applicable à partir du mois de **mai 2018**, mais les responsables du traitement et les sous-traitants sont encouragés à assurer la conformité de leurs procédures au regard du RGPD le plus tôt possible. Les mesures suivantes sont notamment recommandées :

☑ Vérifiez si vous avez l'obligation de **désigner un DPD**

☑ Vérifiez si vous avez l'obligation d'**effectuer une AIPD**

☑ Révisez votre mécanisme de conformité actuel afin de pouvoir respecter l'obligation de **tenir des registres pour les activités de traitement** et d'identifier les **violations de données à caractère personnel** dès que possible

☑ **Vérifiez vos activités de traitement basées sur le consentement** pour vous assurer que celui-ci est conforme aux exigences du RGPD

☑ **Actualisez vos procédures en vigueur** afin de permettre aux personnes concernées d'exercer leurs nouveaux droits (droit à l'oubli, droit à la portabilité des données, etc.)

☑ **Révisez et complétez, le cas échéant, vos polices et documents internes** afin d'inclure les informations supplémentaires exigées par le RGPD (e.g. base juridique du traitement, durée de conservation des données).

A noter qu'un projet de loi[3] facilitant la transition vers le nouveau régime instauré par le RGPD vient d'être déposé à la Chambre des Députés. Ce projet prévoit notamment l'allégement des formalités d'autorisation préalable en matière de traitements à des fins de surveillance et de transferts de données personnelles vers des pays tiers.

Pour plus d'information veuillez contacter:

Claire DENOUAL

Senior Associate, Avocat à la Cour, Member of the Luxembourg

claire.denoual@molitorlegal.lu

Virginie LIEBERMANN

Senior Associate, Avocat à la Cour, Member of the Luxembourg

virginie.liebermann@molitorlegal.lu

[3] Projet de loi n°7049 portant modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel