MOLITOR

Avocats à la Cour

CHECK-LIST AVANT L'ENTREE EN VIGUEUR DU RGPD

Posted on Wednesday 21st of February 2018 in Media, Data, Technologies & IP

A moins de 4 mois avant la date butoir du 25 mai 2018 sonnant l'entrée en vigueur du nouveau règlement européen sur la protection des données personnelles (Règlement 2016/679, dit « RGPD »), la question se pose de l'état de conformité de votre entreprise en matière de traitement de données personnelles.

Vous procédez à un traitement de données personnelles dès lors que vous :

- Collectez, enregistrez, structurez, conservez, adaptez, modifiez ou utilisez, ou encore,
- Effacez ou détruisez

des données personnelles.

Les données personnelles consistent en *« toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement ».*

Où en êtes-vous avec le GDPR ?

Téléchargez notre **check list** des questions à se poser pour évaluer le niveau de votre conformité aux nouvelles exigences du RGPD.

VOTRE MISE EN CONFORMITE

Nous vous proposons ci-après une **check list** des questions à se poser pour évaluer le niveau de votre conformité aux nouvelles exigences du RGPD :

Etape 1: Elaboration d'un plan d'action

- Un **plan d'action** et de mise en conformité au RGPD a-t-il été élaboré ?
- Mon entreprise est-elle soumise à la nomination d'un **délégué à la protection des données personnelles (DPO)** ?
    - Dans l'affirmative, un DPO a-t-il été nommé ?
- Quelles sont les entités / départements concernés par le plan de mise en conformité (état des lieux des activités / procédures de l'entreprise traitant des données personnelles) ?

Etape 2 : Audit des traitements existants

- Les **finalités des traitements**, les **sujets des traitements** et les **catégories de données** personnelles traitées ont-ils été identifiés ?

8, rue Sainte-Zithe PO Box 690 L-2016 Luxembourg - T (+352) 297 298 1 - F (+352) 297 299 www.molitorlegal.lu

- Mon entreprise peut-elle justifier de **la base légale** de chacun des traitements de données personnelles engagés ?
- Des **durées de conservation** des données personnelles sont-elles définies (et communiquées aux personnes concernées) ?
- L'ensemble des données personnelles collectées est-il nécessaire à la poursuite de la finalité du traitement (proportionnalité) ?

Etape 3: Identification des traitements à risque et catégories particulières de données

- Mon entreprise effectue-t-elle des traitements pouvant potentiellement impacter la vie privée des personnes concernées ? :
  - Des critères de décision pour déterminer la nécessité d'une étude **d'impact sur la vie privée** ont-ils été définis ?
  - Une méthode d'étude d'impact sur la vie privée (DPIA) a-t-elle été définie ?
- Mon entreprise effectue-t-elle des traitements impliquant le **croisement** entre plusieurs catégories de données ou la **réutilisation** de données collectées lors d'un autre traitement ?
- Mon entreprise effectue-t-elle des traitements entrant dans le cadre du **profilage** ?
- Les données traitées font-elles l'objet de **transferts** en dehors de l'Union Européenne ?
- Est-ce que mon entreprise a recours à **des sous-traitants** qui traitent des données personnelles pour le compte de mon entreprise (revue des contrats avec les sous-traitants et contrôle du respect des exigences du RGPD par les sous-traitants) ?

Etape 4 : Mise en place de procédures

- Des éléments de conformité au RGPD ont-ils été intégrés dans les procédures de mon entreprise ?
- Mon entreprise a-t-elle mis en place des **mécanismes de gestion** (recueil, enregistrement, modification, révocation…) du consentement des personnes concernées par le traitement de données personnelles (lorsque la base légale est le consentement) ?
- Mon entreprise a-t-elle mis en place une procédure pour répondre aux demandes **d'exercice des droits prévus par le RGPD** (droits d'accès, de rectification, de suppression des données, droit à l'oubli, droit à la portabilité, à la limitation du traitement) ? Les personnes concernées bénéficient-elles d'une information claire et compréhensible lors de la collecte des données ?
- Mon entreprise a-t-elle mis en place des mécanismes **d'archivage** et de **suppression** des données personnelles ?
- Le RGPD a-t-il été intégré au **programme de formation** RH de mon entreprise ?
- Le **service informatique** de mon entreprise a-t-il été associé à la mise en conformité ?
  - Des mesures de **sécurisation** des données (accès protégés, pseudonymisation, chiffrement, stockage et transfert sécurisés, règles de purge et d'archivage…) on-elles été décidées ?
  - Un processus de **détection**, de traitement et de notification des violations de données personnelles est-il arrêté ?
- L'**assurance** de mon entreprise couvre-t-elle les risques (sanctions, dommages et intérêts, incidents…) liés au traitement de données personnelles ?

Etape 5 : Documentation

- Mon entreprise a-t-elle documenté sa conformité au RGPD ?

- Existe-t-il une cartographie exhaustive des données personnelles traitées dans le système d'information de mon entreprise ?
- Une analyse d'impact des traitements pouvant potentiellement impacter la vie privée des personnes concernées a-t-elle été réalisée ?
- Un registre des traitements a-t-il été établi ?
- Un registre des incidents sur les traitements des données a-t-il été mis en place ?

ATTENTION AUX SANCTIONS !

En cas de traitement illicite ou de non conformité les sanctions peuvent atteindre un montant maximal de 20 millions d'euros ou jusqu'à 4% du chiffre d'affaires annuel mondial. A cela s'ajoute d'éventuels dommages et intérêts pour la personne concernée.

Nous sommes à votre disposition pour vous accompagner dans le processus de mise en conformité au RGPD : date butoir le 25 mai 2018.

Contactez nous.

Your contact(s)

Virginie LIEBERMANN
Counsel
Avocat à la Cour, Member of Luxembourg Bar, 2008
virginie.liebermann@molitorlegal.lu