Futur Règlement européen sur la protection des données, qui est concerné ?

Futur Règlement européen sur la protection des données, qui est concerné ?

Le 25 février dernier, Arendt & Medernach organisait une conférence sur le futur Règlement européen sur la protection des données (ci-après « le Règlement »[1]afin de permettre aux entreprises de mieux comprendre les nouvelles obligations auxquelles elles seront prochainement soumises et leur procurer l'essentiel de ce qu'il faut retenir de ce nouveau texte.

Contexte

Après deux années riches en actualités en matière de données personnelles (droit à l'oubli consacré par la Cour de Justice de l'Union européenne (CJUE)[2], et invalidation du Safe Harbor[3] notamment), le nouveau Règlement arrive à point nommé pour remplacer le cadre juridique actuel adopté il y a plus de 20 ans[4].

4 ans de discussions et 4000 amendements ont été nécessaires pour parvenir à un accord autour de ce nouveau texte qui sera adopté en mai/juin prochain. Il sera applicable dans deux ans à compter de sa date d'entrée en vigueur, soit pour l'été 2018.
Si l'échéance semble lointaine, il est toutefois nécessaire d'envisager dès à présent les changements apportés par ce nouveau texte.

De nouvelles obligations pour les entreprises

Il résulte de ce Règlement diverses obligations pour les entreprises et notamment :

• De mettre en œuvre les principes de « privacy by design / privacy by default» afin d'assurer une protection des données dès leur conception et par défaut ;
• De tenir des registres des traitements de données personnelles sauf cas exceptionnels ;
• De notifier toute violation de données dans les 72h auprès de l'autorité de contrôle voire de la personne concernée le cas échéant ;
• De détailler/préciser l'information des personnes concernées ;
• D'adapter leurs contrats de sous-traitances ;
• D'assurer la portabilité des données ;
• De nommer un Délégué à la Protection des Données le cas échéant.
• Les entreprises doivent envisager ces obligations avec le plus grand sérieux puisque de nouvelles sanctions financières pourront désormais être prononcées par les autorités nationales de protection des données. En effet, selon le manquement, ces sanctions pourront atteindre de 2 à 4% du chiffre d'affaires mondial d'une entreprise ou de 10 à 20 millions d'euros, le montant le plus important devant être retenu.

Qu'est-ce qu'une donnée personnelle ?

"Les données à caractère personnel sont définies par le futur Règlement comme « toute information concernant une personne physique identifiée ou identifiable ; est réputée identifiable une personne qui peut être identifiée directement ou indirectement , notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, économique, culturelle ou sociale ».
Cette définition est identique à celle prévue actuellement dans la loi luxembourgeoise[7] mais elle ajoute quelques exemples. Il est notamment précisé qu'un identifiant en ligne, tel qu'une adresse IP, peut être qualifié de données à caractère personnel," explique Héloïse Bock, Partner Arendt & Medernach.

Est-ce qu'on peut dire que toutes les entreprises seront concernées par ce nouveau Règlement ?

"Le champ d'application du règlement est élargi puisque celui-ci aura vocation à s'appliquer à toutes les entreprises traitant des données personnelles dès lors qu'elles sont établies sur le territoire de l'Union européenne ou, lorsqu'elles sont établies hors de l'Union européenne si ces traitements ciblent des citoyens européens.
Un grand nombre d'entreprises seront ainsi concernées en pratique," poursuit-elle.

Des droits nouveaux et renforcés

Pour les personnes concernées, ce nouveau Règlement introduit le célèbre droit à l'oubli ou droit à l'effacement, déjà consacré par la CJUE en 2014[5] mais également, le droit à la portabilité des données qui permet de transférer les données d'un prestataire vers un autre. Les droits d'accès, d'opposition et de rectification des données ainsi que le droit à l'information, existants dans le cadre juridique actuel, sont maintenus et renforcés.

Les transferts de données hors de l'Union européenne

Concernant les transferts de données en dehors de l'Union européenne, le Règlement ajoute de nouvelles bases de légitimité ponctuelles/limitées sur lesquelles un responsable de traitement pourra se fonder en cas de transfert vers un pays n'assurant pas un niveau de protection adéquat.
Le sort des transferts de données réalisés vers les Etats-Unis n'est pas réglé par le Règlement, toutefois, une nouvelle décision d'adéquation est attendue très prochainement[6]. La Commission européenne et les États-Unis se sont en effet accordés sur un nouveau cadre pour les transferts transatlantiques de données le mois derniers : le «bouclier vie privée UE-États-Unis» ou « EU-US Privacy Shield ».

To do list avant 2018

Pour conclure, les avocats d'Arendt & Medernach ont dressé une « to do list » générale reprenant les points suivants :

• Recenser les traitements de données réalisés en pratique et leurs finalités;
• Faire un audit pour évaluer le niveau de conformité actuel et identifier les lacunes;
• Réaliser un « mapping » de tous les transferts de données en considérant les catégories de données, les destinataires des transferts, les bases de légitimité etc.;
• Effectuer des études d'impact lorsqu'un traitement à risque est envisagé;
• Nommer un délégué à la protection des données si nécessaire;
• Mettre en place ou adapter la documentation existante (registres, policies, contrats de sous-traitance, etc.)

[1] Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (2012/0011 COD)
[2] CJUE, 13 mai 2014, affaire C-131/12
[3] CJUE, 6 octobre 2015, affaire C-362/14
[4] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
[5] CJUE, 13 mai 2014, affaire C-131/12
[6] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf
[7] Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel
… [Lire la suite]

Réagissez à cet article

Source : *Futur Règlement européen sur la protection des données, qui est concerné ?*