Nouveau règlement européen sur la protection des données personnelles : Les changements pour les entreprises | Le Net Expert Informatique

Nouveau règlement européen sur la protection des données personnelles : Les changements pour les entreprises

Fin juillet, le Contrôleur Européen de la Protection des Données a publié ses recommandations sur le futur règlement européen portant à quatre le nombre de versions du document. L'occasion de faire le bilan sur les trois évolutions du règlement qui auront le plus d'impact pour les entreprises.

QUEL CHANGEMENT POUR LES ENTREPRISES ?

Mise en place du Privacy by Design (Articles 23, 30, 32a, 33a et 33)

Première nouveauté, les entreprises devront définir et mettre en œuvre des procédures permettant d'intégrer les problématiques liées à la manipulation des données personnelles dès la conception de nouveaux services.

Cette démarche s'accompagne de l'obligation de réaliser des analyses de risques relatives à la vie privée des personnes (discrimination, diffusion de données confidentielles, etc.) préalablement à la mise en place des traitements les plus sensibles et à chaque modification du traitement.

Face aux risques sur la vie privée des personnes induits par ces traitements, il sera imposé aux entreprises d'adopter des mesures de sécurité adéquates en vue de les maitriser.

Concrètement que retenir du Privacy by Design ?

Une mise à jour de la méthodologie projet afin d'identifier au plus tôt les traitements sensibles et une méthode d'analyse de risques à définir et outiller.

Il sera pour cela possible de s'inspirer des guides pratiques de la CNIL intitulés « Etude d'impact sur la vie privée », qui seront à simplifier et contextualiser aux besoins spécifiques de l'entreprise.

Responsabilisation ou « Accountability » (Articles 22 et 28)

Toute entreprise devra désormais être capable de prouver sa conformité vis-à-vis du règlement.

Cette exigence se traduit par :

• l'adoption d'une politique cadre de gestion des données à caractère personnel ;

• une organisation associée ;

• des procédures opérationnelles déclinant les thèmes du règlement (information, respect des droits des personnes, transfert à des sous-contractants, etc.).

L'entreprise devra également être en capacité de prouver l'application de ces politiques et donc, de mettre en place des processus de contrôle.

L'occasion de parler de la personne qui illustrera ce principe d' « Accountability » : le DPO (pour Data Protection Officer). Il devient quasiment obligatoire et remplace le CIL actuel.

Concernant ce DPO, le texte entérine l'obligation de lui fournir le personnel, les locaux, les équipements et toutes les autres ressources nécessaires pour mener à bien ses missions. Encore une fois le parlement souhaite aller au-delà de cette exigence : il propose de nommer au sein de la direction une personne responsable du respect du règlement.

Comment appliquer ce principe ? Il sera nécessaire de définir a minima une politique avec des règles de protection des données ainsi qu''un plan de contrôle et de formation. Cette politique pourra par exemple s'inspirer du modèle des BCR « Binding Corporate Rules », dont le principe a été entériné dans le futur texte, pour lesquelles des modèles types et des premiers retours d'expérience existent déjà.

Obligation de notification des fuites (articles 31 et 32)

L'ensemble des parties s'accordent sur l'obligation de notification des fuites aux autorités. Le Parlement propose même que les entreprises mettent en ligne un registre listant les types de brèches de sécurité rencontrées. Il sera intéressant de constater comment cette exigence cohabitera avec les législations nationales en matière de sécurité et la protection des intérêts de la nation qui tendent à limiter la diffusion de ce type d'information.

La notification de fuites aux personnes concernées, quant à elle, n'est obligatoire que si l'entreprise n'est pas en mesure de démontrer qu'elle a mis en œuvre des mesures afin de rendre cette fuite sans conséquence. D'où l'intérêt d'effectuer correctement l'analyse de risques, de définir et d'implémenter des mesures appropriées.

Au final, deux recommandations afin d'anticiper le futur règlement sur ce point :

• un processus de gestion des fuites de données à définir en l'orchestrant avec les dispositifs de gestion de crise existants et les processus de relation client,

• la réalisation d'exercices réguliers afin de tester son efficacité avec tous les acteurs concernés.

UNE MISE EN CONFORMITÉ À ANTICIPER

Au-delà de ces trois nouveautés majeures, d'autres modifications plus limitées en termes d'impacts organisationnels sont également à prendre en compte, comme la création du droit à la portabilité ou l'extension de la liste des données sensibles. On peut par ailleurs noter le renforcement d'obligations existantes comme le droit à l'information et le recueil du consentement. Le diable se nichera dans les détails.

Pour conclure, les deux années de mise en application du règlement ne seront pas de trop (soit une mise en conformité d'ici début 2018) et nous ne pouvons que conseiller d'initier la mise en conformité dès 2016, avec le cadrage et le lancement des premiers chantiers majeurs. D'autant plus que le sujet devient de plus en plus visible médiatiquement (condamnation récente de Boulanger, Google et l'application du droit à l'oubli, etc.) et que les sanctions financières deviennent réellement significatives (entre 2 et 5% du chiffre d'affaire mondial). L'occasion pour toutes les entreprises de communiquer largement sur les principes de respect de la vie privée effectivement appliqués.

Source : http://www.solucominsight.fr/2015/09/nouveau-reglement-europeen-sur-la-protection-des-donnees-personnelles-anticiper-les-3-impacts-majeurs/