INTERTITRE

Passer à la deuxième étape de la mise en conformité RGPD

La mise en œuvre du Règlement Général sur la Protection des Données, entré en vigueur le 25 mai 2018, n'a pas lieu sans son lot de difficultés. Si la première année a été marquée par la mise en place de la documentation (registre, politiques et notices), par des débats sur le positionnement entre responsable de traitement et éventuel sous-traitant ou sur la nécessité de nommer ou non un Data Protection Officer (DPO), «il faut désormais se focaliser sur le déploiement opérationnel». Bénédicte d'Allard, Manager chez Arendt Regulatory & Consulting (ARC), nous aide à comprendre les grands chantiers qui s'annoncent. Interview.

Bénédicte d'Allard

S'assurer de la gouvernance établie

La documentation mise en place doit être revue au moins annuellement, pour en améliorer l'efficacité si nécessaire et tenir compte des changements survenus dans les processus. Ensuite, les entreprises doivent s'assurer de la bonne compréhension des règles et de l'allocation des responsabilités au travers des différents niveaux hiérarchiques. Les départements Compliance et/ou Audit interne doivent enfin enrichir leurs plans de contrôle.

Les entreprises ayant nommé un DPO peuvent aujourd'hui faire un premier bilan et décider d'un recalibrage de la fonction par exemple en termes de ressources/profil(s) alloués ou bien même décider d'externaliser la fonction de DPO. En effet, l'externalisation permet de libérer les ressources internes et de profiter d'une expertise inspirée des meilleures pratiques du marché. Le recours à un DPO externe peut être attractif dans de nombreux cas.

Documenter les instructions vis-à-vis des sous-traitants

Il est impératif de s'assurer de la bonne application des principes décrits dans les contrats de sous-traitance. Les instructions données aux sous-traitants doivent être documentées et déclinées de manière pratique. Les points de contact respectifs ainsi que le protocole à suivre en cas de demande d'accès, de violation de données ou de fin de relation doivent être explicités (délai de notification, retour ou effacement des données, etc.).

Clarifier les exigences de conservation et d'effacement des données

Une table de conservation des données a probablement déjà été insérée dans la politique d'archivage et les entreprises connaissent les données qu'elles peuvent ou doivent conserver et pour quelles durées. En revanche, il est rare que les employés aient été formés en détail à l'utilisation de cette table et en comprennent l'application dans leur travail au quotidien et dans leurs différentes tâches.

Pour y parvenir, nous conseillons aux organisations d'avoir en premier lieu une vue claire par processus et de relier les traitements de données listés dans le registre avec les différentes durées de conservation. Par la suite, l'organisation devra en informer les employés et les former en fonction de leurs besoins journaliers.

Se conformer à la table de conservation des données

C'est peut-être là le plus gros défi et la difficulté est d'autant plus grande du fait de la multiplicité des supports.

Les documents papiers nécessitent un archivage et une indexation permettant le suivi des durées de conservation. Pour ce qui est des données informatiques, il faut revoir chaque application et évaluer les options, valider une solution d'effacement, de masquage ou anonymisation des données périmées. Une approche pragmatique est indispensable, en fonction de la sensibilité des données traitées (approche par le risque) et de la difficulté de mise en place (toute nouvelle application doit proposer une solution d'effacement). Des données informatiques non structurées peuvent également être présentes dans l'espace personnel de l'employé par exemple. Des instructions précises sur les bonnes pratiques à adopter pourront dissuader ou du moins encadrer la dispersion de ces données.

Assurer la sécurisation informatique des données personnelles

Le RGPD énonce en des termes généraux l'exigence de protection des données d'un point de vue technique. Les organisations restent pourtant responsables vis-à-vis des personnes concernées. Occupées à d'autres tâches plus prioritaires ou moins coûteuses, force est de constater que les entreprises ont souvent repoussé dans le temps, l'évaluation approfondie du niveau de sécurité des données personnelles qu'elles traitent.

La certification CARPA sur laquelle le régulateur luxembourgeois (CNPD) travaille actuellement et l'ISO 27701 promue par la CNIL pourront être des moyens de s'assurer de la sécurisation technique des données.

Quelle solution pour les organisations qui n'auront ni la taille, ni le budget pour s'engager dans un processus de certification?

Il existe de grands principes intangibles à la sécurité informatique qui sont tout à fait adaptés à de petites ou moyennes structures: restreindre au maximum et avoir une vue claire sur les droits d'accès, revoir régulièrement le bien-fondé de ces droits, minimiser les données traitées, distinguer les logs utiles, techniques et non nécessaires, effacer ces derniers et documenter cette classification dans une politique interne.

La confidentialité doit être améliorée, d'abord en sensibilisant les employés, et également grâce à des moyens techniques comme l'encryptage des emails, des appareils numériques et des serveurs, ainsi que le recours à la destruction physique des appareils et disques durs, lorsqu'ils sont décommissionnés. Les sauvegardes (back up) doivent également être hautement sécurisées, avec un nombre faible de personnes autorisées à y accéder.

Le tout est de définir une politique de sécurité raisonnable tenant compte du niveau d'impact et de probabilité, et enfin, de sensibiliser et former régulièrement les employés, pour qu'ils acquièrent les bons réflexes. ■

"S'assurer de la bonne compréhension des règles et de l'allocation des responsabilités"

Arendt Regulatory & Consulting
41A Avenue J-F Kennedy
L-2082 Luxembourg
Tél.: 26 09 10 1
arendt.com