#RGPD : Conseils d'une entrepreneure connectée

Sur le site de la CNIL, de nombreux tutoriels sont mis en ligne pour aider les chefs d'entreprise.

4) Avez-vous mis en œuvre des réponses adaptées aux droits des personnes, notamment dans vos mentions légales ?

5) Avez-vous réalisé une analyse d'impact du traitement de la donnée (un outil en open source est en ligne sur le site de la CNIL) ?

6) Avez-vous identifié des données sensibles dans l'entreprise et quelles précautions avez-vous mis en place ? (ex : certificats médicaux de vos collaborateurs) ?

Les outils de la CNIL

Pour se mettre en conformité avant le 28 mai 2018, voici deux outils développés par la CNIL, sur l'analyse d'impact et sur la nomination de votre futur DPO.

1) Un logiciel en open source d'analyse d'impact sur la protection des données (Privacy Impact Assessment, PIA ou DPIA) est un outil important pour la responsabilisation des organismes. Ce logiciel open source PIA facilite la conduite et la formalisation d'analyses d'impact sur la protection des données telles que prévues par le RGPD.
N'hésitez pas à consulter sur Youtube le tutoriel « Utiliser le logiciel PIA pour mener une étude d'impact sur la protection des données ».
Un autre outil d'analyse d'impact sur les objets connectés a été également développé par la CNIL. **https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-fr-2018-02-19.pdf**

2) Une fiche de poste du délégué à la protection des données personnelles : **Le site de la CNIL / rubrique https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees**

« Avez-vous établi un registre d'activité des traitements des données ? »

7) Avez-vous sensibilisé vos collaborateurs sur la protection des données personnelles ?

8) Avez-vous communiqué sur l'intérêt légitime en cas de collecte des données, vis à vis de vos collaborateurs ? (ex : cv des saisonniers)

Conseils : Si vous n'avez pas encore démarré votre mise en conformité, pas de panique ! Pour démarrer, voici une check list composée de 17 thèmes pour engager un état des lieux plus complet.
Pour accéder à l'outil : (https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles)

Pour structurer votre politique de protection des données personnelles

- Former des salariés à la privacy, à la cybersécurité, la cybermalveillance
- Cartographier les traitements (informatisées et archives papier, appels téléphoniques, formulaires sur le site internet, etc.)
- Refondre les chartes informatiques internes
- Informer sur votre site sur le traitement des données personnelles soit dans vos mentions légales, soit dans votre politique de confidentialité
- Intégrer une adresse email de contact dans votre politique de protection des données personnelles
- Sécuriser vos accès aux données et aux mots de passe (attention aux post it Mots de passe sur les ordinateurs)
- Redéfinir une gestion sécurisée des appareils personnels utilisés dans un cadre professionnel
- Communiquer sur votre politique de protection des données personnelles en interne et en externe
- Intégrer l'intérêt légitime de l'employeur dans la collecte de données à caractère personnel de l'employé
- Établir une mention de co-responsabilité du traitement des données personnelles avec vos sous-traitants dans les contrats et dans vos mentions légales.

Ma recommandation

Tous ces chantiers conduiront à mettre en place une traçabilité des actions de protection et traitement des données personnelles et des appréciations de conformité dont le dirigeant doit tenir compte.
Ces chantiers participent également à placer l'entreprise en situation de confiance vis-à-vis de ses clients et partenaires.
Elle placera de la même manière la direction en situation de confiance vis-à-vis des investisseurs, des administrateurs comme des salariés. ■
Bonus (consulter notre politique de confidentialité de l'agence) http://www.createurdeconnaissances.com/politique-de-confidentialite/

Profil de votre futur Data Protection Officer

Alliant des compétences juridiques et techniques, le DPO est un bon communiquant capable de résister aux pressions de la direction.
Rattaché directement auprès de la direction générale, il délivre en toute indépendance des recommandations aux différents métiers et services composant l'entreprise sur le traitement des données personnelles, même si elles vont à l'encontre du business !
Les entreprises ayant déjà nommé un correspondant informatique & libertés peuvent faire monter ce dernier en compétences. À défaut de trouver la perle rare en interne, les entreprises peuvent soit mutualiser cette ressource en prenant en compte que ce profil est actuellement très demandé ou externaliser cette fonction auprès de prestataires spécialisés (avocat, consultant…).

Une nouvelle gradation des sanctions en cas de non-respect du RGDP

Adopté le 27 avril 2016, le RGPD prévoit des sanctions extrêmement dissuasives :
2 % du chiffre d'affaires annuel mondial pour des manquements de protection des données personnelles ou d'analyse d'impact.
4 % du chiffre d'affaires annuel mondial pour manquement notamment aux droits des personnes (droits d'accès, de rectification, d'opposition, de suppression, droit à l'oubli, etc.).
Dans chacun des cas, le montant le plus élevé est celui pris en compte.