ebl lexington avocats

Votre société est-elle en conformité avec le Règlement Général sur la Protection des Données (« **RGPD** ») ?

Qu'est-ce que le RGPD ? Le Règlement Général sur la Protection des Données du 27 avril 2016 met en œuvre des **règles de protection des données harmonisées pour l'ensemble des États membres de l'UE**. L'accent est mis sur la prévention et l'audit. L'objectif est clair : **évolution de l'environnement technique des entreprises et déploiement de mesures organisationnelles appropriées**.

Quand le RGPD entre-t-il en vigueur ? Le RGPD est directement applicable depuis le **25 mai 2018** et a été complété, en France, par une Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles.

Quelles entreprises sont concernées par le RGPD ? Le RGPD s'applique à tous les traitements informatisés de données personnelles réalisés, au sein de l'UE ou non, lors d'activités se déroulant sur le territoire de l'UE. **99,99% des entreprises y sont soumises.**

Quelles sont les sanctions ? Des rappels à l'ordre, mises en demeure, injonctions de mise en conformité, **jusqu'à 4% du CA mondial HT ou 20 millions d'euros pour les manquements les plus graves**. La CNIL pourra, à tout moment, contrôler les sociétés afin de s'assurer du respect du RGPD. En outre, les dirigeants et les entreprises s'exposent à des sanctions pénales.

Quelle est la première étape ? Il convient de commencer par **dresser un état** de votre situation et **des données à caractère personnel qui sont collectées ou traitées** au sein de votre entreprise. Sur cette base, un **plan de conformité** peut être élaboré. Le tableau ci-contre synthétise les questions principales auxquelles il convient de répondre pour être en conformité avec le RGPD.

Êtes-vous en conformité avec le RGPD ?

Mesures générales	O/N
Avez-vous réalisé un audit pour répertorier les données traitées, vérifier leur pertinence, leur durée de conservation, leur niveau de sécurité, etc. ?	
Disposez-vous d'un registre de données ?	
Devez-vous désigner un Délégué à la protection des données ?	
Avez-vous revu vos procédures internes de collecte et traitement des données ? Avez-vous formalisé une charte sur le traitement des données ?	
Avez-vous procédé aux analyses d'impact pour les traitements à risques élevés ?	
Avez-vous revu vos procédures internes en cas de violation des données ? (ex. cyber-attaques, fraudes internes, pertes d'ordinateur ?)	
Volet « RH »	
Avez-vous adapté vos contrats de travail ?	
Avez-vous informé vos salariés ou recueilli leur consentement?	
Avez-vous revu vos procédures internes afin d'interdire tout traitement de données superflu ?	
Avez-vous revu vos contrats de prestation de service RH ?	
Avez-vous formé vos salariés en charge du traitement des données ?	
Volet « commercial & contrats »	
Avez-vous informé vos clients de leurs droits relatifs à leurs données personnelles (accès, suppression, rectification, opposition, etc.) ?	
Disposez-vous d'une charte de confidentialité ?	
Avez-vous revu vos contrats, CGV, CGU, CGA ?	
Avez-vous encadré la sortie des données de l'UE ?	

Ebl Lexington a mis en place une équipe transversale dédiée à la mise en conformité de votre société au RGPD. Pour plus d'information, contactez-nous !

ebl lexington avocats

Pour aller plus loin :

Quelles sont les obligations imposées par le RGPD?	Avez-vous entrepris les démarches nécessaires ? (exemples)
Mise en place d'un **Délégué à la Protection des Données**	➥ Analyse effectuée par votre société afin de vérifier si elle doit ou non nommer un DPD ; ➥ Si oui, les documents relatifs au choix du DPD et à ses obligations (par exemple, modification de son contrat de travail et/ou de sa fiche de poste, CR de réunions à ce sujet) ; ➥ Si non, désignation d'un référent interne (modification de son contrat de travail, détermination de ses missions).
Mise en place d'une **cartographie de traitement des données personnelles**	➥ Registres mis à jour retraçant : ○ le traitement effectué (qui héberge ? où?), les données personnelles concernées (⚠ la notion de donnée personnelle est large), les destinataires, les finalités du traitement (quel est l'objectif de la collecte des données ?) ; ○ les consentements recueillis, les méthodes utilisées ; ○ les contrats modifiés, les politiques de confidentialité… ○ les violations de données personnelles (ex. existe-t-il une procédure en cas de perte par un salarié d'une clé USB contenant des données personnelles ?) ; ➥ **L'ensemble des documents utilisés afin d'élaborer la cartographie doit être conservé (ex. questionnaires, retour des opérationnels sur les données collectées…).**
Études d'impact sur la vie privée	➥ Documents analysant le niveau de risque du traitement (en toute hypothèse, l'analyse est obligatoire) ; ➥ **Étude d'impact** (ex. gestion des adresses IP, véhicules de fonction, gestion des données de santé, des procédures d'alerte obligatoires pour les entreprises de + 50 salariés => information à « risque élevé »).
Obtenir le consentement des personnes dont les données sont traitées	➥ Procédure interne permettant d'identifier les cas dans lesquels le consentement est requis ➥ **Procédure de recueil du consentement** – matérialisé ou dématérialisé (la procédure est-elle adaptée à la donnée traitée ? Un tiers intervient-il ?)
Donner un droit d'accès, de rectification et d'effacement des données	➥ Existence d'une **procédure interne** qui permet à toute personne concernée d'avoir accès aux données : qui contacter (espace personnel en ligne, courriel dédié…) ? Dans quels délais ? Comment demander la suppression ? Sous quels délais (1 mois max) ? En quelle langue ? quelles informations doivent être communiquées ? ➥ Revue/**modification des contrats avec les hébergeurs** ou prestataires susceptibles d'intervenir dans le cadre de ce droit d'accès, de rectification, etc.
Notifier en cas de violation des données	➥ Procédure interne **en cas de violation des données** (Qui contacter ? Quels délais ? Premiers réflexes ?).

RGPD – Notre approche, notre méthodologie

- Nous proposons un accompagnement **« clé en main »** ou une intervention ponctuelle sur des points précis en fonction de l'avancement de votre mise en conformité
- Nous mettons en place des **audits adaptés à votre structure** afin d'élaborer la cartographie des risques et/ou les études d'impacts
- Nous identifions les **sujets sensibles et urgents** et mettons en place un rétro-planning de déploiement des procédures de conformité

RGPD – Exemples d'interventions récentes des équipes d'EBL Lexington

Élaboration et mise en place d'une politique interne relative à la gestion des données RH (recrutement, gestion des problèmes de santé, harcèlement, rupture du contrat, obtention du consentement) Modifications des contrats de travail, élaboration de fiches de poste sur les responsabilités d'un DPD

Réalisation d'un audit « données personnelles » afin de réaliser une cartographie des risques et des données

Recommandations s'agissant des mesures à mettre en œuvre en priorité

Élaboration des études d'impact sur la vie privée : analyse des zones de « risques élevés », élaboration d'un questionnaire d'analyse

Rédaction des notices d'information (site web, emails, CGV, CGU)

Modification des contrats commerciaux dont l'exécution implique un traitement de données personnelles

Modification des clauses de délégations de signatures, de pouvoirs et de responsabilité

Élaboration des procédures de consentement notamment pour les données sensibles

Audit des méthodes de conservation de données, élaboration de recommandations relatives aux durées de conservations des données au regard de leur caractère sensible



Contacter Karine Clolus-Dupont (social), Olivier d'Abo (commercial), Laurent Levy (IP)

(contact@lxt-law.com ou T +33 (0)1 83 75 41 41). www.lxt-law.com.