SQUIRE PATTON BOGGS

Conformité au RGPD
Comment se préparer à l'échéance du 25 mai 2018

Avez-vous votre rétro-planning conformité?

Le Règlement Général sur la Protection des Données (RGPD) s'applique à de nombreuses entreprises de l'UE, ainsi qu'à des entreprises qui, sans y être établies, y collectent des données. Les changements requis par le RGPD sont d'une ampleur considérable et les entreprises concernées doivent prendre sans plus tarder les mesures qui leur permettront de se mettre en conformité d'ici à mai 2018.

Cette fiche vous présente les principales étapes de la mise en conformité, en quoi elles sont importantes et la durée estimée de chacune d'entre-elles.

Notre équipe Données Personnelles & Cybersécurité vous assistera dans l'établissement et la mise en œuvre d'un plan et calendrier de mise en conformité adaptés à votre entreprise.

Stade I

Etape 1: Cartographie des Traitements

3-6 mois +

Action

Recensez et cartographiez vos traitements de données, en incluant les flux et la typologie d'utilisation des données, afin d'établir un registre exhaustif des activités de traitements.

Pourquoi?

Le RGDP exige que vous teniez un « registre des activités de traitement ». Ce registre peut vous permettre de faire le point sur les actions à mener. Il vous permettra aussi de réagir rapidement en cas de violation de données et de répondre aux demandes d'accès à leurs données par les personnes concernées.

Etape 2: Gouvernance Données Personnelles/ Délégué à la Protection des Données

1-3 mois

Action

Evaluez si vous devez nommer un Délégué à la Protection des Données et, le cas échéant, désignez un professionnel qui réponde aux exigences du RGPD. Indépendamment des obligations légales, révisez et, si besoin, améliorez les procédures et structures de gouvernance interne, de façon à ce qu'elles garantissent la prise en compte de la protection des données à tout moment.

Pourquoi?

La désignation d'un Délégué à la Protection des Données est obligatoire pour certaines entreprises. Une gouvernance solide de la protection des données est, en tout état de cause, essentielle afin de respecter les obligations qui s'imposent à tous au titre du principe de responsabilité (« accountability ») .

Stade II

Etape 3: Partage des Données

6 mois +

Action

Identifiez tout partage de données avec des tiers, déterminez le rôle de ces tiers et mettez en place des garanties appropriées. Cela peut nécessiter la conclusion de contrats ou la révision de contrats existants.

Pourquoi?

Le RGPD prévoit un contenu obligatoire pour certains contrats et exige que les obligations et rôles respectifs soient clairement définis.

Etape 4: Justification des Traitements

6 mois

Action

Revoyez ou déterminez la base juridique sur laquelle sont fondés vos traitements, à tout le moins pour les principales utilisations. Elaborez et mettez en œuvre un plan d'actions afin de corriger les écarts dans la conformité.

Pourquoi?

Le RGPD exige que tout traitement des données ait une base juridique (consentement de la personne, intérêt légitime, contrat, obligation légale etc.) et en rend l'utilisation plus difficile. Le RGPD contient également des restrictions et des obligations supplémentaires pour les traitements automatisés, y compris le profilage.

Etape 5: Mentions d'Information et Consentement

2-3 mois

Action

Réviser et modifiez le contenu des mentions et formulaires ainsi que les procédures liées à l'information des personnes et au recueil de leur consentement.

Pourquoi?

Le RGPD renforce le contenu minimum des mentions d'information et impose des conditions plus strictes au recueil du consentement.

Stade III

Etape 6: Analyses d'Impact Relatives à la Protection des Données

3 mois

Action

Identifiez s'il y a des traitements à « risques élevés » tels que définis par le RGPD. Si c'est le cas, réalisez une « analyse d'impact relative à la protection des données » (« *privacy impact assessment* » ou « PIA ») et, si nécessaire, consultez votre autorité de contrôle.

Pourquoi?

Il est obligatoire de procéder à une PIA pour tout traitement à « risques élevés » et, dans certains cas, de consulter les autorités de contrôle.

Etape 7: Politiques de Protection des Données

6 mois

Action

Révisez et complétez les politiques et les procédures existantes en matière de protection des données, y compris celles relatives à la conservation et à l'intégrité des données, et notamment la pertinence et l'exactitude des données.

Pourquoi?

Le RGPD impose des obligations plus strictes concernant le caractère exact et proportionnel des donnés ainsi que l'exigence qu'elles ne soient pas conservées plus longtemps que nécessaire.

Etape 8: Droits des Personnes Concernées

3 mois

Action

Identifiez les nouveaux droits des personnes concernées prévus par le RGPD. Révisez les modalités d'exercice des droits des personnes concernées et prévoyez en de nouvelles, le cas échéant, pour vous conformer aux obligations existantes et à venir.

Pourquoi?

Le RGPD étend les droits existants et introduit de nouveaux droits pour les personnes concernées, notamment le droit à la portabilité des données ou celui à l'effacement/l'oubli.

Etape 9: Protection Dès la Conception et Par Défaut (Privacy by Design and by Default)

6-9 mois

Action

Révisez ou mettez en place des procédures permettant de prendre en compte la protection des données personnelles dès la conception d'un service, produit, application ou traitement impliquant des données personnelles. Les paramètres par défaut doivent aussi être conformes au RGPD.

Pourquoi?

La conformité doit être intégrée dès leur conception et par défaut dans tous les traitements impliquant des données personnelles, par exemple en minimisation la collecte et le traitement des données.

Stade IV

Etape 10: Transferts Internationaux de Données

2-3 mois

Action

Identifiez et révisez les outils encadrant les transferts de données. Corrigez les écarts de conformité, notamment en concluant des Clauses Contractuelles Types avec vos prestataires et les sociétés du groupe. Envisagez le recours aux Règles d'Entreprise Contraignantes (ou « BCR »).

Pourquoi?

Le RGPD impose, comme par le passé, l'obligation d'encadrer les transferts de données personnelles hors de l'Espace Economique Européen, tout en augmentant de façon significative les sanctions en cas de manquement.

Etape 11: Sécurité des Données et Processus de Gestion des Violations

3-6 mois

Action

Vérifiez les mesures de sécurité existantes afin de vous assurer qu'elles sont suffisantes et évaluez si les mesures spécifiquement prévues par le RGPD sont en place ou devraient l'être. Révisez ou établissez un plan de gestion des « violations de données » (« data breach »).

Pourquoi?

Le RGPD contient des exigences plus strictes quant aux mesures techniques et organisationnelles garantissant la sécurité des données. Il exige aussi que les violations de données personnelles soient notifiées à l'autorité de contrôle dans les meilleurs délais et, si possible, dans les 72 heures (sauf justification de retard) ainsi qu'aux personnes concernées, si la violation est susceptible d'engendrer un « risque élevé ».

Stade V

Etape 12: Déploiement des Outils de Conformité et Formation du Personnel

6 mois +

Action

Déployez les mentions d'information et formulaires de consentement nouvellement créés ou révisés. Publiez les politiques et procédures nouvellement créées ou révisées et procédez à la formation du personnel clé sur la conformité au RGPD.

Exemple de domaines complémentaires dans lesquels notre équipe peut vous assister

- Conformité au RGPD
- BCR (Règles contraignantes d'entreprise)
- Privacy Shield
- Contrats de transfert de données
- Enquêtes internationales
- Gestion des violations de données
- Préparation à la cybersécurité et gestion de crise
- Objets connectés
- Revue de site web
- Consentement
- Etudes d'impact sur la vie privée (PIA)
- Politiques de protection des données
- Mentions d'information
- Données HR
- Alertes professionnelles
- Formation
- Affaires publiques et conseil sur la réglementation
- Contentieux auprès des tribunaux ou des autorités de contrôle

Contacts de l'équipe internationale de Protection de Données Personnelles et Cybersécurité