GUIDE PRATIQUE ET CONSEILS D'EXPERT

COMMENT SE PRÉPARER À LA RÉGLEMENTATION GÉNÉRALE DE PROTECTION DES DONNÉES (RGPD)

IRON MOUNTAIN®

COMMENT SE PRÉPARER À LA RÉGLEMENTATION GÉNÉRALE DE PROTECTION DES DONNÉES (RGPD) : GUIDE PRATIQUE ET CONSEILS D'EXPERT

La RGPD prendra effet en 2018. Elle va changer la manière dont les entreprises peuvent collecter, utiliser et transférer les données personnelles. Nous vous présentons ici les mesures pratiques que vous pouvez prendre pour vous préparer à un nouveau contexte de renforcement de la réglementation.

1. ACCROÎTRE LA SENSIBILISATION

Communiquez avec les preneurs de décision à propos des changements que la RGPD va impliquer. S'ils comprennent l'impact de cette réglementation, vous serez plus susceptible d'obtenir rapidement leur soutien. Consultez le registre des risques si vous en avez un.

CONSEIL D'EXPERT : Évaluez la conformité actuelle. Déterminez votre respect actuel de la Loi sur la protection des données, identifiez les nouvelles exigences et récapitulez vos conclusions.

2. LOCALISER LES INFORMATIONS

Documentez les données personnelles que vous conservez, d'où elles proviennent et avec qui vous les partagez. Regardez à l'intérieur et à l'extérieur de votre entreprise et dans des zones spécifiques. Envisagez l'intérêt d'un audit des informations.

CONSEIL D'EXPERT : Choisissez une fonction. Étudiez une zone ou un service tel que les ressources humaines, la fiscalité ou les approvisionnements, et traitez-le comme un cas type pour améliorer les processus internes. Examinez où et comment vous utilisez les informations que vous collectez. Faites un audit de vos modes de stockage et de suivi des informations.

3. ÉTUDIER ET METTRE À JOUR LES AVIS ET POLITIQUES DE CONFIDENTIALITÉ

Étudiez vos avis et politiques de confidentialité et établissez un plan de mise en œuvre des changements.

CONSEIL D'EXPERT : Soyez clair. Vos communications doivent être faciles à comprendre par les personnes concernées et par les employés qui doivent ensuite se conformer à ces avis. Les droits d'accès, de rectification, de suppression et de transfert doivent être expliqués aux parties prenantes internes.

4. CONNAÎTRE LES DROITS DES PERSONNES

Vos procédures doivent couvrir tous les droits accordés aux personnes, notamment corriger les inexactitudes, supprimer les informations et éviter le marketing direct sans consentement. Assurez-vous de savoir qui prend les décisions concernant la suppression des données et si vos systèmes prennent cette opération en charge. N'oubliez pas d'étudier la portabilité des données et les formats que vous utilisez pour fournir des informations.

CONSEIL D'EXPERT : Recherchez les copies. Vos fournisseurs et sous-traitants peuvent également détenir des copies des informations personnelles. Il est possible que les anciens systèmes informatiques ne soient pas conçus pour supprimer les informations. Dans ce cas, envisagez de quelle manière transférer les données, isoler les anciens équipements ou les déconnecter complètement.

5. ÊTRE PRÉPARÉ À RECEVOIR LES DEMANDES D'ACCÈS À L'INFORMATION

Mettez à jour vos procédures afin de pouvoir traiter plus rapidement les demandes, notamment les demandes de correction des informations inexactes. Si vous devez gérer un grand nombre de demandes, vous souhaiterez peut-être investir dans une solution d'accès en ligne.

CONSEIL D'EXPERT : Pensez à la planification. Les délais de traitement des demandes d'accès à l'information sont ramenés de 40 jours à un mois, mais les demandes complexes peuvent demander jusqu'à trois mois.

6. FAIRE REPOSER LE TRAITEMENT DES DONNÉES PERSONNELLES SUR UNE BASE LÉGALE

Sachez pourquoi vous collectez et utilisez les données personnelles et veillez à disposer d'une base légale avant de les traiter. Vous devez être en mesure de justifier votre intérêt légitime, au lieu de vous contenter de réclamer les données.

CONSEIL D'EXPERT : Soyez raisonnable. Souvenez-vous que vous ne pouvez collecter des informations personnelles que si vous avez : un motif légal (embauche, pour éviter le versement de pots-de-vin), un intérêt commercial légitime, ou le consentement totalement informé et librement consenti de la personne concernée. Vos intérêts ne doivent pas être en conflit avec ceux de la personne.

7. ÉTUDIER LE CONSENTEMENT

Évaluez la manière dont vous demandez, obtenez et enregistrez le consentement des personnes. Le consentement doit être donné librement, spécifique, informé et sans ambiguïté. Il ne doit pas être présumé.

CONSEIL D'EXPERT : Gardez à l'esprit que le consentement peut être révoqué à tout moment. Vous êtes tenu d'informer les personnes et de les aviser.

8. RECHERCHER LES ENFANTS

Réfléchissez à la manière dont vous allez vérifier l'âge des personnes et obtenir le consentement des parents et tuteurs. Votre avis de confidentialité doit être adapté aux enfants.

CONSEIL D'EXPERT : Les états membres sont autorisés à fixer l'âge de consentement à 13 ans.

9. METTRE EN PLACE DES PROCÉDURES EN CAS DE VIOLATION DES DONNÉES

Actuellement, les entreprises ne sont pas toutes tenues d'avertir le Commissariat aux Informations en cas de violation des données. La nouvelle réglementation exige que tout le monde le fasse. Établissez donc des procédures claires pour détecter, signaler et examiner les violations.

CONSEIL D'EXPERT : Les violations doivent être signalées dans un délai de 72 heures. À défaut, vous encourez une amende pouvant atteindre 10 millions d'euros ou 2 % de votre chiffre d'affaires international.

10. ÉVALUATION DE L'IMPACT SUR LA PROTECTION DES DONNÉES ET PROTECTION DES DONNÉES DÈS LA CONCEPTION

Certaines activités, telles que le traitement automatisé ou le traitement de données sensibles à grande échelle, exigent une évaluation préalable de l'impact sur la vie privée (EIVP). Le Commissariat aux Informations a créé un guide correspondant. De plus, les nouveaux systèmes et processus en particulier doivent être développés en tenant compte du respect de la vie privée afin que les solutions soient conformes aux principes de confidentialité.

CONSEIL D'EXPERT : N'oubliez pas les nouveaux projets. Contactez nos équipes informatiques afin qu'elles tiennent compte de la confidentialité dès la conception avant d'acheter ou de développer de nouvelles solutions.

11. NOMMER UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Les entreprises qui surveillent régulièrement des données à grande échelle ou qui traitent des données sensibles à grande échelle doivent embaucher un délégué à la protection des données.

CONSEIL D'EXPERT : Gérez la conformité avec le plus grand sérieux. Que vous ayez recours à un conseiller externe ou que votre équipe compte un délégué à la protection des données, une personne détenant les connaissances, l'autorité et les ressources nécessaires doit assumer cette responsabilité.

12. AVOIR UNE VUE D'ENSEMBLE

Si vous travaillez à l'international, déterminez de quelle autorité de contrôle de la protection des données vous dépendez.

CONSEIL D'EXPERT : Votre siège social détermine généralement l'autorité dont vous dépendez. Mais n'ignorez pas les données que vous conservez ni l'endroit où vous les conservez. Schématiser les référentiels de toutes vos données peut vous aider à vous préparer au changement.

Pour de plus amples informations sur nos solutions, rendez-vous sur notre site Web www.ironmountain.fr