La législation évolue, et la mise en conformité arrive le 25 mai 2018. Qu'est-ce que ça change pour vous et pour votre entreprise ?

Le Livre Blanc sur le RGPD

EXPERTCOM

C'EST QUOI LE RGPD ?

En 2016, l'Union Européenne a créé et publié un nouveau texte de référence pour la protection des données. Adopté, ce texte est aujourd'hui inscrit dans la législation et entrera en vigueur le 25 mai 2018.

Le Règlement Général sur la Protection des Données s'appliquera aussi bien au niveau des autorités publiques que sur notre façon de travailler. Il est donc capital de comprendre ses répercussions.

A quoi sert la législation Européenne ?

Il existe déjà des règles quant à la collecte et le traitement des données personnelles. Ainsi, la personne qui recueille et / ou traite des data personnelles a l'obligation de les protéger d'une utilisation abusive, et doit respecter des exigences légales. Le RGPD viendra renforcer ces règles.

Le RGDP s'appliquera aux données numériques ou papier ?

Aux deux ! Aussi bien aux data numériques (emails, bases de données etc.) qu'aux données papier. Vous devrez donc assurer la sécurité de vos copies papier. Et les éliminer totalement quand vous n'en aurez plus besoin (en utilisant un destructeur de papier sécurisé par exemple).

Quel risque mon entreprise court-elle en cas d'infraction ?

Si vous ne respectez pas le RGPD, vous risquez une forte amende ! En effet, le contrôleur de la CNIL peut vous imposer une pénalité allant jusqu'à 4% de votre chiffre d'affaires annuel global ou 20 millions d'euros selon l'entreprise. C'est bien sûr l'amende la plus lourde, et chaque infraction ne sera pas du même montant. Mais partez du principe qu'une pénalité n'est tout simplement pas envisageable, puisque vous respecterez la réglementation !

Mon entreprise devra-t-elle faire des efforts en plus ?

Et oui ! Vous aurez plus de responsabilités donc d'obligations. Notamment la mise en place de mesures techniques et organisationnelles pour le traitement des données. Vous devrez également examiner les risques liés à ce traitement pour évaluer le niveau de sécurité nécessaire. Et vous devrez être en mesure de présenter au contrôleur les mesures que vous avez prises et de les expliquer. Vous devrez aussi être vigilant quant aux personnes à qui vous communiquez ces données personnelles : prestataires externes, collaborateurs, société de destruction etc.

Des entreprises ont-elles déjà fait des erreurs ?

Et bien oui ! Et les conséquences en ont été douloureuses.

En Grande-Bretagne un contrôleur (aussi appelé Information Commmissioner's Office - ICO) a infligé une amende de 10 000 livres à une autorité locale. En effet, celle-ci s'est rendue coupable de ne pas avoir instauré de mesures de sécurité en cas de perte ou de destruction accidentelle lorsque des documents concernant les données personnelles d'une centaine de personnes ont été trouvés par l'acheteur d'un bâtiment à l'abandon. Celui-ci était auparavant occupé par la municipalité et celle-ci avait oublié quelques documents pendant son déménagement ...

Aux Pays-Bas, ce sont des exploitants de transports publics qui ont été sanctionnés, car ils conservaient des données transactionnelles bien plus longtemps que nécessaires. Au départ, le contrôleur avait décidé de supprimer ces données, mais elles ont finalement été conservées et anonymisées. Mais les techniques d'anonymisation n'étaient pas suffisantes dans au moins un cas, et les exploitants ont dû payer une amende de 125 000 euros.

En Espagne, ce sont plusieurs amendes qu'un contrôleur a dû donner. En effet, plusieurs documents contenant des données personnelles ont été jetés dans des poubelles et / ou dans la rue. Dans au moins un des deux cas, les fichiers papiers n'étaient que partiellement détruits voire pas détruits correctement.

Données inutiles ?

Vous devez les détruire en toute sécurité

Sous peine d'amende !

La protection des données est-elle importante ?

Oui, et vous allez devoir la placer au cœur de vos préoccupations ! La confidentialité des data devra s'intégrer à tous vos processus. Vous devrez mettre en place des moyens pour vous assurer que seules les données personnelles devant être traitées sont effectivement traitées.
Vous devrez vous poser les questions suivantes :

Ai-je besoin de ces données personnelles ?

Ai-je besoin de les traiter à cette fin ?

Les personnes qui y ont accès ont-elles besoin d'y avoir accès ?

Les données sont-elles obsolètes ?

Ai-je besoin d'une autorisation pour traiter des données ?

Oui, enfin une raison légitime. En effet, selon le RGPD, la personne doit donner son autorisation de manière libre, spécifique, informée et non ambiguë. Son silence, sa renonciation ou son inactivité ne suffisent donc pas. Il faut un véritable processus actif, comme par exemple cocher une case. Et votre entreprise devra démontrer que cette autorisation a effectivement été donnée.

Y-a-t-il de nouveaux droits ?

Plusieurs nouveaux droits même :

Droit à l'oubli

Cela permet aux personnes de demander la suppression de leurs données personnelles.

Droit à la portabilité des données

Les personnes peuvent demander que leurs données personnelles, détenues dans un format courant, soient transférées.

Droit de contestation

Les personnes ont l'autorisation de contester leur profilage. Quand leurs données personnelles sont traitées dans le cadre de marketing direct, Les personnes peuvent également s'y opposer.

Il existe des exceptions pour lesquelles il faut demander des conseils juridiques.

Qu'en est-il des personnes qui demandent à consulter leurs données ?

Il existe ce qu'on appelle "une demande d'accès" : le droit des personnes à consulter leurs données. Cela leur permet d'avoir accès aux données stockées les concernant. Avec le RGPD, vous devrez répondre à ces demandes d'accès dans un délai d'un mois suivant la réception de la demande. Selon circonstances particulières, vous avez la possibilité de prolonger jusqu'à deux mois maximum.

Ces demandes d'accès sont de plus en plus nombreuses. On peut même s'attendre à ce qu'elles augmentent : elles sont désormais gratuites ! En effet, la possibilité pour une entreprise de réclamer des frais pour répondre à une demande a été abolie. Vous devrez donc mettre en place des processus adaptés.

Dois-je nommer un responsable de la protection des données ?

Vous devriez. Le RGPD exige que les autorités publiques nomment un responsable de la protection des données (RPD). Et dans certaines circonstances, les entreprises doivent aussi en nommer un. Il est recommandé de demander conseil à un juriste selon votre taille, votre activité, votre emplacement etc. Mais, même s'il n'est pas techniquement nécessaire, une entreprise qui traite régulièrement des données devrait fortement envisager d'en nommer un !

Vais-je devoir signaler les violations de données ?

En effet. L'une des bases du RGPD est d'assurer la sécurité des données; et cela inclus de réagir en cas de violation des données. Ces violations et les mesures prises pour y remédier doivent être signalées au contrôleur de la protection des données dans un délai de 72h environ après constat de la violation. Vous devrez également en informer les personnes concernées dans un délai raisonnable (aucun délai officiel n'a été établi), quand la violation risque d'entraîner un risque élevé pour leurs droits et libertés. Il existe néanmoins des exceptions dans le signalement où vous pourrez demander conseil à un juriste. Sachez aussi que :

L'Autriche, l'Allemagne les Pays-Bas et d'autres pays ont déjà mis en place leurs propres obligations quant au signalement des violations des données.

Signaler des violations de données peut être nécessaire selon d'autres règles et règlements, par exemple dans le secteur financier ou le milieu médical.

Une législation supplémentaire à part doit être appliquée en Europe en conformité avec la directive européenne sur la cybersécurité.

Des indemnisations sont-elles prévues ?

En principe, si une personne a subi un préjudice suite à une violation des nouvelles règles, elle peut faire valoir un droit à l'indemnisation auprès des entités / personnes qui contrôlent ou traitent lesdites données personnelles pour le préjudice subi. Sauf quelques exceptions. Mais vu les pénalités prévues pour une infraction, surtout pour une violation de données, vous devez vous efforcer de minimiser les demandes d'indemnisation potentielles.

Votre entreprise doit donc mettre en place une politique et un plan d'action en matière de violation des données et former ses collaborateurs.

Faut-il évaluer l'impact sur la confidentialité ?

Et bien oui. En effet, dans la nouvelle réglementation, cela s'appelle "évaluations d'impact sur la protection des données" - c'est-à-dire EIPD. Quand des opérations de traitement de données (notamment celles utilisant les nouvelles technologies) peuvent entraîner un risque important pour les droits et libertés des personnes, il faut effectuer une évaluation de l'impact des opérations de traitement proposées sur la protection des données avant le traitement. Vous devez également consulter un contrôleur de la protection des données avant le traitement lorsque l'évaluation signale que le traitement des données personnelles peut créer un risque élevé en l'absence de mesures d'altération du risque.

> Ces évaluations vont devenir courantes et vont s'avérer être des outils très utiles pour permettre aux entreprises de réduire les risques. L'évaluation du risque relatif à la sécurité des données mais aussi la prise en compte des risques liés au traitement des données personnelles, par exemple une destruction accidentelle ou illégale des données.

Les transferts de données à des pays tiers ont-ils changé ?

Pas vraiment. Les règles spécifiques actuelles à propos du transfert de données depuis les Etats membres de l'Union Européenne vers des pays tiers (les Etats-Unis sont aussi inclus) restent les mêmes avec le RGPD. Et y compris la nécessite des pays tiers d'assurer un niveau de protection adéquat en cas de transfert de données. Ces règles sont en fait devenues plus détaillées. Ce thème est complexe et il est amené à évoluer dans le cadre du règlement actuel sur la protection des données. Nous vous conseillons d'en parler avec votre conseiller juridique.

LA RGPD EN UN COUP D'ŒIL

Portée

Toutes les entreprises du monde traitant les données personnelles de citoyens européens

Obligations

Les entreprises doivent notifier les violations de données

DANS UN DÉLAI DE 72 HEURES

Sanctions

Jusqu'à 4% du chiffres d'affaires

MONDIAL

Calendrier

Promulgation par les Etats membres de l'UE le

25 mai 2018

1

Mettez en place un processus d'évaluation de l'impact sur la confidentialité, cartographiez vos données et déterminez les zones à risque

2

Examinez attentivement les contrats fournisseurs: vous aurez besoin de leur aide, surtout pour signaler les violations de sécurité très rapidement. Vous devez vérifier que vous avez les droits contractuels nécessaires pour insister sur ce point

3

Mettez à jour les synthèses et documents. Préparez une nouvelle documentation détaillée et des registres en vue des inspections réglementaires

4

Examinez les principaux aspects pratiques, y compris la rétention des données en prenant compte de toutes celles détenues par l'entreprise

5

Vérifiez que vous avez pris vos dispositions pour détruire de manière sûre les données dont vous n'avez pas besoin

6

Consentement explicite, droit à l'oubli, à la portabilité des données et d'objection : vérifiez que les nouveaux aspects sont inclus dans les politiques et procédures

7

Mettez en place une procédure de notification des violations de données et des capacités de détection et de réaction. Entraînez-vous ensuite, comme pour un exercice d'incendie.

8

Envisagez de nommer un responsable de la protection des données

9

Formez vos collaborateurs sur tous les aspects ci-dessus. Les contrôleurs de la protection des données accordent une importance particulière à ce point.

10

Mettez en place et menez régulièrement des audits de conformité afin d'identifier et de rectifier les problèmes

EXPERTCOM

CONTACTEZ-NOUS

9-11 rue Pierre et Marie Curie

0 826 10 13 15

contact@expert-com.com