Livre Blanc sur le

RGPD

(Règlement Général sur la Protection des Données)

La législation évolue. Quel impact pour vous et votre entreprise ?

Cordery Legal.Compliance

Fellowes WORK BETTER™

De quoi s’agit-il et quelle est la situation actuelle ?

L’Union européenne (UE) a modifié sa réglementation en termes de protection des données. Ces modifications sont maintenant inscrites dans la loi et seront introduites partout en Europe le 25 mai 2018. Le Règlement général sur la protection des données (RGPD) s’applique de manière très large, des autorités publiques aux entreprises privées. Ces changements auront une incidence sur notre manière de travailler et nous concernent tous. Cette note vous présente brièvement le RGPD et surtout son incidence sur la partie administrative.

En quoi consiste la législation européenne ?

En Europe, il existe déjà des règles pour la collecte et le traitement des données personnelles. Toute personne qui recueille ou traite des données personnelles doit les protéger d’une utilisation abusive et respecter un ensemble d’exigences légales. Le RGPD renforce les règles existantes.

Ces nouvelles règles s’appliquent-elles aux données numériques et aux copies papier ?

Les deux. Le RGPD s’appliquera aux données numériques (e-mails et bases de données, entre autres) et aux copies papier (à quelques exceptions près). Ceci signifie que nous avons aussi des responsabilités pour les fichiers papier : nous devons en assurer la sécurité et les éliminer de manière sûre (par exemple, utiliser un destructeur sécurisé) quand nous n’en avons plus besoin.

Pénalités jusqu’à

20 millions d’euros

ou 4 % du chiffre d’affaires annuel global de l’entreprise

Quels types d’amendes mon entreprise risque-t-elle en cas d’infraction aux règles ?

Dans le cadre du nouveau règlement, le contrôleur peut imposer de lourdes amendes en cas de non-respect de la loi : l’amende la plus lourde s’élève à 20 millions d’euros ou 4 % du chiffre d’affaires annuel global d’une entreprise, selon le montant le plus élevé. Bien que chaque manquement n’entraînera pas l’amende la plus lourde, être sanctionné n’est tout simplement pas envisageable : nous devons tous respecter la règlementation sur la protection des données.

Les entreprises devront-elles en faire plus ?

Oui. Chaque organisation aura plus de responsabilités et d’obligations sous ces nouvelles règles. En particulier, les organisations doivent mettre en œuvre des mesures techniques et organisationnelles pour être sûres de traiter les données correctement. Pour évaluer le niveau de sécurité adéquat, vous devez examiner les risques présentés par le traitement des données, surtout en cas de destruction accidentelle ou illégale. Vous devrez pouvoir présenter les mesures que vous avez prises quand un contrôleur vous demandera en quoi elles consistent. Il faut notamment vérifier à qui vous envoyez des données personnelles. Par exemple, vous devez vérifier les procédures en place chez vos prestataires, comme les agences de mailing, les sociétés de destruction de documents et les agences d’intérim.

Y a-t-il des exemples de situations dans lesquelles des entreprises ont fait des erreurs ?

- **Les conséquences d'une non-conformité peuvent être douloureuses**. Le contrôleur britannique de la protection des données, appelé Information Commissioner's Office (ICO), a sanctionné d'une amende de 100 000 £ une autorité locale coupable de n'avoir pas mis en œuvre des mesures de sécurité pour protéger des données d'une perte ou d'une destruction accidentelle lorsque des documents contenant les données personnelles d'une centaine de personnes (dont des adultes et des enfants dans une situation vulnérable) ont été trouvés par l'acheteur d'un bâtiment à l'abandon auparavant occupé par la municipalité. La municipalité avait quitté le bâtiment et oublié certains documents pendant son déménagement.

- Aux Pays-Bas, le contrôleur de la protection des données a sanctionné d'une amende des exploitants de transports publics car ils conservaient des données transactionnelles plus longtemps que nécessaire. Initialement, le contrôleur avait demandé aux exploitants de supprimer les données transactionnelles ou de les anonymiser, mais ils ont décidé de conserver les données et de les anonymiser. Les techniques d'anonymisation n'étaient pas suffisantes dans au moins un cas, et l'exploitant concerné a dû payer une amende de 125 000 euros.

- En Espagne, le contrôleur de la protection des données a distribué plusieurs amendes lorsque des documents contenant des données personnelles ont été jetés dans des poubelles ou dans la rue. Dans au moins un cas, les documents étaient seulement partiellement détruits et, dans d'autres, les documents n'avaient pas été détruits correctement.

Vais-je devoir mettre la protection des données au cœur de mes préoccupations ?

Oui. La confidentialité des informations doit être intégrée à tous vos processus. Les entreprises devront mettre en place des moyens pour s'assurer que, par défaut, seules les données personnelles devant être traitées sont effectivement traitées. Vous devez donc vous poser les questions suivantes :

- Ai-je besoin de ces données personnelles ?
- Ai-je besoin de les traiter à cette fin ?
- Est-ce que toutes les personnes qui y ont accès ont besoin d'y avoir accès (par exemple si seules les RH doivent voir les documents, doivent-elles être placées dans une armoire de classement verrouillée, dont seules les RH ont la clé) ?
- Les données sont-elles obsolètes ?

Une autorisation sera-t-elle nécessaire pour le traitement des données ?

Oui. En général, il doit y avoir une raison légitime pour le traitement des données personnelles. Selon la nouvelle réglementation, la personne doit donner son autorisation de manière libre, spécifique, informée et non ambiguë. Le silence, les renonciations ou l'inactivité ne sont pas suffisants. Un processus actif tel que le fait de cocher une case devra être mis en place. Les entreprises doivent aussi pouvoir démontrer que l'autorisation a effectivement été donnée. Assurez-vous d'avoir mis en place des procédures qui répondent à toutes ces exigences.

Y a-t-il de nouveaux droits ?

Oui. Plusieurs nouveaux droits ont été introduits, notamment :

- Le droit à l'oubli – ce droit permet aux personnes de demander la suppression de leurs données personnelles ;
- Le droit à la portabilité des données – ce droit permet aux personnes de demander que leurs données personnelles, détenues dans un format courant, soient transférées ;
- Le droit de contestation – ce droit inclut l'autorisation pour les personnes de contester leur profilage. Lorsque les données personnelles sont traitées dans le cadre de marketing direct, les personnes peuvent aussi s'y opposer.

La mise en application de ces nouveaux droits représentera un défi pour les organisations, mais il faut noter que tous ces nouveaux droits sont qualifiés, en d'autres termes il existe des exceptions pour lesquelles il faut demander des conseils juridiques.

Et les personnes qui demandent à consulter leurs données ?

Le droit des personnes à consulter leurs données, qui s'appelle techniquement une « demande d'accès », continue d'exister dans la nouvelle réglementation. Ce processus permet à chacun d'exercer son droit d'accès aux données stockées les concernant. Selon la nouvelle règlementation, il faudra répondre aux demandes d'accès dans le mois qui suit la réception de la demande (bien qu'il puisse y avoir un prolongement à un maximum de deux mois supplémentaires dans certaines circonstances), et la possibilité pour une entreprise de réclamer des frais pour répondre à une demande d'accès a été abolie. On a constaté une croissance importante du nombre de demandes d'accès depuis quelques années. Quand elles seront gratuites, on peut s'attendre à une augmentation encore plus forte. Vu le nombre accru du recours aux courriels et au cloud en particulier, la réponse aux demandes d'accès est également plus coûteuse et plus complexe.

Un aspect essentiel de la stratégie future de protection des données de toute organisation consistera donc à mettre en place des processus adéquats pour répondre aux demandes d'accès.

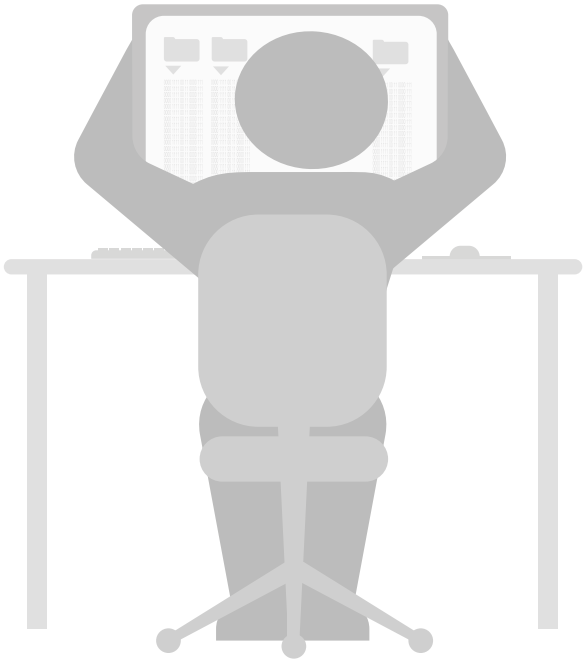
Vais-je devoir nommer un responsable de la protection des données ?

Peut-être. Le RGPD exige que les autorités publiques nomment un responsable de la protection des données (RPD). Un tel responsable devra aussi être nommé par les entreprises pour s'occuper de la conformité à la protection des données, dans certaines circonstances. Là aussi, il est préférable de demander conseil à un juriste, en fonction de ce que vous faites et de l'endroit où vous le faites. Vu l'importance de la conformité à la confidentialité à l'heure actuelle, même si un RPD n'est pas nécessaire techniquement, même une entreprise de taille moyenne qui traite régulièrement des données devrait envisager d'en nommer un.

Vais-je devoir signaler les violations des données ?

Oui. Assurer la sécurité des données représente l'une des bases des nouvelles règles, y compris la réaction en cas de violation des données.

Une violation des données peut prendre de nombreuses formes, comme la destruction, la perte, la modification, la divulgation ou l'accès non autorisé aux données personnelles.



Les violations doivent être signalées (y compris les mesures prises pour y remédier) au contrôleur de la protection des données compétent dans un délai raisonnable et (dans la mesure du possible) jamais plus de 72 heures après le constat de la violation. Les personnes touchées par la violation doivent également en être informées dans un délai raisonnable (mais aucun délai officiel n'a été défini) quand la violation risque d'entraîner un risque élevé pour leurs droits et libertés. Il existe des exceptions limitées en ce qui concerne le signalement à un contrôleur et l'information des personnes, pour lesquelles il convient de demander des conseils juridiques adéquats. Le signalement des violations de données est rendu encore plus compliqué par les aspects suivants :

- Certains pays (dont l'Autriche, l'Allemagne et les Pays-Bas) ont déjà mis en place leurs propres obligations en matière de signalement des violations de données ;
- Le signalement des violations de données peut être nécessaire selon d'autres règles et règlements, notamment dans le secteur financier et de la santé ;
- Une législation supplémentaire à part doit être appliquée en Europe en conformité avec la directive européenne sur la cybersécurité.

Quelles indemnisations sont prévues ?

En principe, toute personne qui a subi un préjudice suite à une violation des nouvelles règles peut faire valoir un droit d'indemnisation auprès des personnes ou entités qui contrôlent ou traitent les données personnelles en question pour le préjudice subi, sauf quelques exceptions. Vu les pénalités prévues pour une infraction à la protection des données dans le nouveau règlement, surtout lorsqu'il s'agit d'une violation de données, les entreprises doivent s'efforcer de minimiser les demandes d'indemnisation potentielles.

Les entreprises doivent donc prioritairement mettre en place une politique et un plan d'action clairs en matière de violation des données et former leur personnel.

Faudra-t-il évaluer l'impact sur la confidentialité ?

Oui. Dans la nouvelle réglementation, ces évaluations s'appellent « évaluations d'impact sur la protection des données » (EIPD). Lorsque des opérations de traitement de données (en particulier celles qui utilisent les nouvelles technologies) risquent d'entraîner un risque élevé pour les droits et libertés des personnes, il faut réaliser une évaluation de l'impact des opérations de traitement proposées sur la protection des données personnelles avant le traitement. Un contrôleur de la protection des données doit être consulté (également avant le traitement) lorsque l'évaluation indique que le traitement des données personnelles créerait un risque élevé en l'absence de mesures d'atténuation du risque.

Ces évaluations risquent de devenir courantes et devraient s'avérer 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 lié au traitement des données personnelles, par exemple une destruction accidentelle ou illégale des données.

Qu'est-ce qui a changé pour les transferts de données à des pays tiers ?

Pas grand-chose. Les règles spécifiques actuelles à propos du transfert de données depuis les États membres de l'Union européenne vers des pays tiers (y compris les États-Unis) restent les mêmes avec le RGPD, y compris la nécessité 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 susceptible d'évoluer dans le cadre du règlement actuel sur la protection des données. Vous devez donc en parler à votre équipe juridique.

Où trouver des informations supplémentaires ?

Le nouveau règlement est disponible sur le site Internet de la Commission européenne **ici**

Que dois-je faire maintenant ?

Pour vous conformer au RGPD, vous devez calculer votre budget et planifier vos ressources (y compris informatiques). Pensez aussi à bien utiliser votre période de planification pour vous adapter et adapter vos process. Voici une liste des dix principaux enjeux de la conformité à étudier dès maintenant :

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 l'aide de vos fournisseurs, surtout pour signaler les violations de sécurité très rapidement. Vous devez donc vérifier que vous avez les droits contractuels nécessaires pour insister sur ce point ;**
3. **Mettez à jour les systèmes et documents et 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, compte tenu de toutes les données utilisées 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. **Vérifiez que les nouveaux aspects, tels que le consentement explicite, le droit à l'oubli, le droit à la portabilité des données et le droit d'objection, sont tous inclus dans les politiques et procédures ;**
7. **Mettez en place une procédure de notification des violations de données, y compris des capacités de détection et de réaction, et entraînez-vous comme vous le feriez pour un exercice d'incendie ;**
8. **Envisagez de nommer un responsable de la protection des données ;**
9. **Formation, formation, formation : formez le personnel 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.**

Expertise

Jonathan Armstrong et André Bywater de Cordery Compliance ont une vaste expérience du conseil sur les questions liées au RGPD et nous ont aidés à rédiger ce livre blanc.

www.corderycompliance.com

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street,
London, EC4A 4HH
+44 (0)207 075 1784
jonathan.armstrong@corderycompliance.com

André Bywater
Cordery
Lexis House
30 Farringdon Street
London, EC4A 4HH
+44 (0)207 075 1785
andre.bywater@corderycompliance.com

A propos de Fellowes : Fellowes fabrique des solutions innovantes et de qualité pour le bureau (machines de bureau, accessoires ergonomiques, solutions d'archivage) afin de permettre à ses clients de travailler dans un environnement plus sûr, plus organisé et plus efficace.

www.fellowes.com

Fellowes France
Bat D
38, rue Jean Mermoz
78605 Maisons-Laffitte Cedex
France
Tel: +33 (0)1-78-64-91-00
Email: france-customerservice@fellowes.com

Cordery Legal.Compliance

Fellowes WORK BETTER™