Commission européenne

Le RGPD: nouvelles opportunités, nouvelles obligations

Tout ce que les entreprises doivent savoir à propos du règlement général européen sur la protection des données

Justice et consommateurs

Printed by Bietlot in Belgium

Luxembourg: Office des publications de l'Union européenne, 2018

Print	ISBN 978-92-79-79440-7	doi:10.2838/43972	DS-01-18-082-FR-C
PDF	ISBN 978-92-79-79412-4	doi:10.2838/975187	DS-01-18-082-FR-N

TABLE DES MATIÈRES

CHAPITRE 1

UNE OPPORTUNITÉ POUR LES ENTREPRISES

Le RGPD réglemente la manière dont les entreprises traitent et gèrent les données à caractère personnel. Il entrera en vigueur le 25 mai 2018 et s'appliquera à toutes les entreprises et organisations (par exemple, les hôpitaux, les administrations publiques, etc.). Il s'agit du plus grand changement aux règles européennes relatives à la protection des données opéré au cours de ces vingt dernières années et plus.

Non seulement le RGPD donne aux citoyens plus de contrôle sur la manière dont leurs données à caractère personnel sont utilisées, mais il rationalise également de manière considérable l'environnement réglementaire pour les entreprises. Pour ce faire, il instaure un cadre uniforme pour la législation en matière de protection des données dans l'ensemble de l'UE. En d'autres termes, au lieu d'avoir une législation en matière de protection des données par pays, une seule réglementation régit désormais l'ensemble de l'UE. Ainsi, une entreprise qui exerce des activités dans différents pays ne doit plus se conformer à plusieurs réglementations, souvent divergentes, mais uniquement au RGPD si elle souhaite proposer ses services au sein de l'UE.

Comment le RGPD peut être bénéfique pour votre entreprise

- **Une Union, une législation:** grâce à cet ensemble de règles unique, il sera plus simple et moins onéreux pour les entreprises d'exercer leurs activités dans l'UE.
- **Un guichet unique:** dans la plupart des cas, les entreprises ne doivent traiter qu'avec une seule autorité de protection des données (APD).
- **Des règles européennes sur le territoire européen:** les entreprises établies en dehors de l'UE doivent appliquer les mêmes règles que les entreprises européennes lorsqu'elles proposent leurs biens ou leurs services aux citoyens dans l'UE.
- **Approche fondée sur le risque:** le RGPD évite de devoir se conformer à une obligation fastidieuse et unique pour tous en adaptant en revanche les obligations aux risques respectifs encourus.
- **Des règles propices à l'innovation:** le RGPD est neutre sur le plan technologique.

Une question de confiance

La protection des données à caractère personnel inquiète beaucoup les citoyens. C'est pourquoi, ils se montrent très méfiants vis-à-vis des environnements numériques. Selon un sondage Eurobaromètre:

- huit personnes sur dix estiment qu'elles n'ont pas un contrôle total sur leurs données à caractère personnel;
- six personnes sur dix déclarent ne pas faire confiance aux entreprises qui opèrent en ligne;
- plus de 90 % des Européens souhaitent que les mêmes droits en matière de protection des données s'appliquent dans tous les pays de l'UE.

«Les entreprises qui échouent à protéger de manière appropriée les données à caractère personnel d'une personne risquent de perdre la confiance du consommateur qui sera réticent à utiliser de nouveaux produits et services.»

Le RGPD offre une nouvelle occasion à votre entreprise de renforcer la confiance des consommateurs grâce à une gestion des données à caractère personnel fondée sur le risque.

CHAPITRE 2

COMPRENDRE LE RGPD

Le RGPD s'applique-t-il à mon entreprise?

En résumé, le RGPD s'applique à ***toute*** entreprise qui:

traite des données à caractère personnel de manière **automatisée** ou **manuelle** (à condition que les données soient organisées selon certains critères).

Même si votre entreprise ne traite des données que pour le compte d'autres entreprises, vous devez toujours respecter les règles.

Le RGPD s'applique:

- si votre entreprise traite des données à caractère personnel et est établie dans l'UE, indépendamment de l'endroit où le traitement des données a lieu; ou
- si votre entreprise est établie en dehors de l'UE mais qu'elle propose des biens ou des services à des citoyens au sein de l'UE ou qu'elle surveille le comportement de personnes au sein de l'UE.

À quoi correspondent les données à caractère personnel?

Les données à caractère personnel désignent toute information se rapportant à une personne vivante identifiée ou identifiable. Il peut s'agir:

- du nom;
- de l'adresse et du numéro de téléphone;
- de la localisation;
- de dossiers médicaux;
- d'informations bancaires ou relatives aux revenus;
- de préférences culturelles;
- ... et d'autres renseignements.

Des données à caractère personnel qui ont été rendues anonymes, ou pseudonymisées, mais qui peuvent encore être utilisées pour identifier à nouveau une personne sont également couvertes par le RGPD. Toutefois, les données à caractère personnel qui ont été rendues anonymes de manière irréversible, de telle manière que la personne concernée ne puisse plus être identifiable, ne sont pas considérées comme des données à caractère personnel et ne sont donc pas régies par le RGPD.

En outre, le RGPD est neutre sur le plan technologique. En d'autres termes, il protège les données à caractère personnel indépendamment de la technologie utilisée ou de la manière dont les données à caractère personnel sont conservées. Le RGPD s'applique à votre entreprise si elle traite et conserve des données à caractère personnel, que ce soit en recourant à un système informatique complexe ou à des fichiers sur support papier.

«Le RGPD s'applique à votre entreprise si elle traite et conserve des données à caractère personnel, que ce soit en recourant à un système informatique complexe ou à des fichiers sur support papier.»

Soyez très vigilant avec les catégories spéciales (sensibles) de données à caractère personnel

Si les données à caractère personnel que vous collectez comprennent des informations sur la santé, la race, l'orientation sexuelle, la religion, les convictions politiques ou l'appartenance syndicale d'une personne, elles sont considérées comme sensibles. Votre entreprise ne peut traiter ces données que sous certaines conditions, et vous pourriez ainsi être amené à mettre en œuvre des garanties supplémentaires, comme le chiffrement.

En quoi consiste le traitement des données à caractère personnel?

Selon le RGPD, la définition du traitement des données à caractère personnel englobe toutes les actions telles que la collecte, l'utilisation et la suppression de données à caractère personnel.

Surveillez-vous votre établissement au moyen de la vidéosurveillance? Consultez-vous une base de données contenant des données à caractère personnel à des fins commerciales? Envoyez-vous des courriels promotionnels? Supprimez-vous des fichiers (numériques) relatifs à vos employés ou déchiquetez-vous des documents? Ou publiez-vous la photo d'une personne sur votre site internet ou vos réseaux sociaux?

Si vous avez répondu «oui» à une de ces questions, votre entreprise traite certainement des données à caractère personnel.

Comment le RGPD contribue-t-il à réduire les coûts?

Le RGPD tient compte des besoins des entreprises. Ainsi, le règlement vise à supprimer les exigences administratives afin de réduire les coûts et minimiser les charges administratives:

- **plus de notifications préalables:** la réforme supprime la plupart des notifications préalables aux autorités de contrôle, ainsi que leurs frais connexes;
- **délégués à la protection des données:** les entreprises doivent surtout nommer un DPD si leurs activités de base impliquent le traitement de données sensibles à large échelle ou le suivi régulier et systématique à grande échelle de personnes. Les administrations publiques ont l'obligation de nommer un DPD;
- **analyses d'impact relatives à la protection des données:** les entreprises ne sont tenues de réaliser une analyse d'impact relative à la protection des données que si une activité de traitement des données proposée engendre un risque élevé pour les droits et libertés des personnes concernées;
- **tenue de registres:** les entreprises qui comptent moins de 250 employés ne doivent pas tenir de registres sauf si le traitement des données n'est pas occasionnel ou s'il implique des informations sensibles.

«Le règlement vise à supprimer les exigences administratives afin de réduire les coûts et minimiser les charges administratives.»

CHAPITRE 3

VOS OBLIGATIONS AU TITRE DU RGPD

Le RGPD impose des obligations directes en matière de traitement des données aux entreprises à l'échelle européenne. Selon le RGPD, une entreprise ne peut traiter des données à caractère personnel que sous certaines conditions. Par exemple, le traitement doit être loyal et transparent, avoir une finalité spécifique et légitime, et être limité aux données nécessaires pour atteindre cette finalité. Il doit également être fondé sur un des motifs légaux suivants:

- le **consentement** de la personne concernée;
- une **obligation contractuelle** entre vous et la personne concernée;
- répondre à **une obligation légale**;
- protéger les **intérêts vitaux** de la personne concernée;
- effectuer une **mission d'intérêt public**;
- poursuivre les **intérêts légitimes** de votre entreprise, mais uniquement après avoir vérifié que les droits fondamentaux et les libertés de la personne dont vous traitez les données ne sont pas sérieusement affectés. Si les droits de la personne concernée prévalent sur vos intérêts, vous ne pouvez pas traiter ses données.

En clair: demandez le consentement pour utiliser des données à caractère personnel

Le RGPD applique des règles strictes pour le traitement de données qui repose sur le consentement. Ces règles visent à garantir que la personne comprend ce à quoi elle donne son consentement. En d'autres termes, le consentement doit être **donné librement**, **spécifique**, **éclairé** et **univoque**, et demandé en des termes clairs et simples. En outre, le consentement doit être donné par un **acte positif**, comme cocher une case en ligne ou signer un formulaire.

Si vous traitez des données à caractère personnel relatives à un **enfant** en vous basant sur le consentement, vous aurez besoin du consentement parental. Cependant, étant donné que la limite d'âge varie entre 13 et 16 ans selon le pays, il est recommandé de consulter la législation nationale.

«Rappel: lorsqu'une personne donne son consentement pour le traitement de ses données à caractère personnel, vous ne pouvez traiter les données que pour les finalités pour lesquelles le consentement a été donné. De plus, vous devez lui laisser la possibilité de retirer son consentement.»

Déterminez votre rôle et vos responsabilités

Après avoir déterminé que le RGPD s'applique à votre entreprise et que vous traitez des données à caractère personnel, la prochaine étape consiste à déterminer votre rôle.

Les règles de protection des données distinguent le responsable du traitement et le sous-traitant des données, qui doivent répondre à différentes obligations. Alors que le responsable du traitement détermine la finalité et les moyens de traiter les données à caractère personnel, le sous-traitant ne fait que traiter les données à caractère personnel pour le compte du responsable du traitement. Cependant, le sous-traitant ne peut pas pour autant se cacher derrière le responsable du traitement.

Le RGPD exige qu'un responsable du traitement n'engage un sous-traitant que s'il offre des garanties suffisantes. Ces garanties doivent être intégrées dans un contrat écrit conclu entre le responsable du traitement et le sous-traitant. Le contrat doit également comprendre un certain nombre de clauses obligatoires, dont, par exemple, une clause précisant que le sous-traitant ne traitera des données à caractère personnel que sur instruction documentée du responsable du traitement.

Obligations qui protègent les droits des personnes

Le RGPD comprend un certain nombre d'obligations destinées à protéger le droit d'une personne à avoir le contrôle sur ses données à caractère personnel.

Votre obligation: fournir des informations transparentes

Les entreprises doivent informer les personnes concernées: qui traite quoi et pourquoi. Ces informations doivent, au minimum, clairement spécifier:

- qui vous êtes;
- pourquoi vous traitez les données;
- quelle est la base juridique du traitement;
- qui recevra les données (le cas échéant).

Dans certains cas, les informations doivent également spécifier:

- les coordonnées du DPD;
- l'intérêt légitime (lorsque l'intérêt légitime est le motif légal du traitement);
- le motif du transfert des données vers un pays non membre de l'UE;
- la durée de conservation des données;
- les droits de la personne concernée à la protection des données (c'est-à-dire le droit d'accès, de rectification, à l'effacement, à la limitation, d'opposition, à la portabilité, etc.);
- la manière dont le consentement peut être retiré (lorsque le consentement est le motif légal du traitement);
- s'il existe une obligation réglementaire ou contractuelle de fournir les données;
- en cas de prise de décision automatisée, des informations sur la logique sous-jacente, l'importance et les conséquences de la décision.

«Les entreprises doivent informer les personnes concernées: qui traite quoi et pourquoi.»

Votre obligation: droit d'accès et droit à la portabilité des données

Les personnes ont le droit de demander à accéder sans frais à leurs données à caractère personnel dans un format accessible. Si vous recevez une telle demande, vous devez:

- informer la personne concernée si vous traitez ses données à caractère personnel;
- l'informer sur le traitement (notamment sur les finalités du traitement, les catégories de données à caractère personnel concernées, les destinataires de ses données, etc.);
- lui fournir une copie des données à caractère personnel traitées.

En outre, lorsque le traitement repose sur le consentement ou sur un contrat, la personne concernée peut demander que ses données à caractère personnel lui soient rendues ou qu'elles soient transférées à une autre entreprise. Il s'agit du droit à la portabilité des données. Les données doivent être fournies dans un format couramment utilisé et lisible par machine.

Même si ces deux droits sont étroitement liés, ils sont néanmoins distincts. Ainsi, vous devez éviter toute confusion entre eux et informer la personne concernée en conséquence.

Votre obligation: droit à l'effacement (droit à l'oubli)

Dans certains cas, une personne peut demander que le responsable du traitement efface ses données à caractère personnel, par exemple lorsque les données ne sont plus nécessaires au regard de la finalité du traitement. Toutefois, votre entreprise n'est pas obligée de se conformer à la demande d'une personne si:

- le traitement est nécessaire pour respecter la liberté d'expression d'une personne et le droit à l'information;
- vous devez conserver les données à caractère personnel pour vous conformer à une obligation légale;
- vous avez d'autres raisons d'intérêt public de conserver les données à caractère personnel, comme la santé publique ou à des fins de recherches scientifiques et historiques;
- vous avez besoin de conserver les données à caractère personnel pour mener une action en justice.

Votre obligation: droit de rectification et droit d'opposition

Si une personne estime que ses données à caractère personnel sont incorrectes, incomplètes ou inexactes, elle a le droit de les faire rectifier ou compléter dans les meilleurs délais.

Une personne peut également s'opposer à tout moment au traitement de ses données à caractère personnel pour une utilisation particulière lorsque votre entreprise les traite sur la base de votre intérêt légitime ou pour exécuter une mission d'intérêt public. À moins que vous n'ayez un intérêt légitime qui prévaut sur l'intérêt de la personne concernée, vous devez cesser de traiter les données à caractère personnel. De même, une personne peut demander une limitation du traitement de ses données à caractère personnel en attendant de déterminer si votre intérêt légitime prévaut sur le sien. Cependant, dans le cas de la prospection, vous devez toujours arrêter de traiter les données à caractère personnel à la demande de la personne concernée.

Une mise en garde sur la prise de décision automatisée et le profilage

Les personnes ont le droit de ne pas être soumises à une décision fondée exclusivement sur un traitement automatisé. Toutefois, il existe certaines exceptions à cette règle, notamment lorsque la personne a donné son consentement explicite à la décision automatisée. Sauf si la décision automatisée repose sur une loi, votre entreprise doit:

- informer la personne concernée de la prise de décision automatisée;
- accorder à la personne concernée le droit de demander qu'une personne examine la décision automatisée;
- accorder à la personne concernée la possibilité de contester la décision automatisée.

Par exemple, si une banque recourt à une prise de décision automatisée pour accorder ou non un prêt à une personne, cette dernière devrait être informée de la décision automatisée et avoir la possibilité de la contester et de demander une intervention humaine.

Obligations fondées sur le risque

En plus des obligations visant à protéger les droits des personnes, le RGPD contient également un certain nombre d'obligations dont l'application dépend du risque.

Votre obligation: nommer un délégué à la protection des données (DPD)

Un DPD est chargé de contrôler votre respect du RGPD. Une des principales missions du DPD consiste à informer et à conseiller les employés qui traitent les données à caractère personnel quant à leurs obligations. Le DPD coopère également avec l'APD et fait office de point de contact entre l'APD et les personnes concernées.

Votre entreprise doit nommer un DPD si:

- vous suivez régulièrement ou systématiquement des personnes ou traitez des catégories particulières de données;
- ce traitement est une activité de base de votre entreprise; et si
- vous effectuez ces opérations à grande échelle.

Par exemple, si vous traitez des données à caractère personnel pour diffuser des publicités ciblées sur les moteurs de recherche en fonction du comportement en ligne des personnes concernées, le RGPD vous oblige à désigner un DPD. En revanche, si vous n'envoyez une publicité à vos clients qu'une seule fois par an, vous ne devez pas nommer de DPD. De même, si vous êtes médecin et que vous collectez des données sur la santé de vos patients, il n'est probablement pas nécessaire que vous nommiez un DPD. Mais si vous traitez des données à caractère personnel portant sur la génétique et la santé pour le compte d'un établissement hospitalier, vous devrez nommer un DPD.

Votre obligation: protection des données dès la conception et par défaut

Le RGPD introduit deux nouveaux principes: la protection des données dès la conception et la protection des données par défaut.

La **protection des données dès la conception** permet de garantir qu'une entreprise tient compte de la protection des données dès les premières étapes de la planification d'une nouvelle manière de traiter les données à caractère personnel. Conformément à ce principe, un responsable du traitement doit prendre toutes les mesures techniques et organisationnelles nécessaires pour mettre en œuvre les principes de la protection des données et protéger les droits des personnes concernées. Ces étapes comprennent, par exemple, la pseudonymisation.

La protection des données dès la conception minimise les risques pour la vie privée et améliore la confiance. En plaçant la protection des données au premier rang du développement de nouveaux biens ou services, vous pouvez éviter tout problème éventuel lié à la protection des données dès les premières étapes. En outre, cette pratique permet de sensibiliser sur la protection des données dans tous les départements et à tous les niveaux d'une entreprise.

La **protection des données par défaut** vise à assurer que votre entreprise fasse toujours du paramètre le plus strict en matière de confidentialité le paramètre par défaut. Par exemple, si deux paramètres de confidentialité sont proposés et que l'un des paramètres bloque l'accès des données à caractère personnel à d'autres personnes, il devrait être utilisé comme paramètre par défaut.

«La protection des données dès la conception minimise les risques pour la vie privée et améliore la confiance.»

«La protection des données par défaut vise à assurer que votre entreprise fasse toujours du paramètre le plus strict en matière de confidentialité le paramètre par défaut.»

Votre obligation: notifier correctement en cas de violation de données

Une violation de données survient lorsque les données à caractère personnel dont vous êtes responsable sont divulguées, de manière accidentelle ou illicite, à des destinataires non autorisés, ou qu'elles sont temporairement inaccessibles ou altérées.

Il est essentiel pour une entreprise de mettre en œuvre des mesures techniques et organisationnelles appropriées pour éviter des violations de données. Toutefois, si une violation de données survient et que la violation engendre un risque pour les droits et libertés de la personne concernée, vous devez en informer votre APD dans les 72 heures après avoir pris connaissance de la violation.

Selon que la violation de données engendre ou non un risque élevé pour les personnes affectées, une entreprise peut également devoir informer toutes les personnes affectées par cette violation de données.

Transférer des données à caractère personnel en dehors de l'UE?

Le RGPD s'applique à l'Espace économique européen (EEE), qui comprend tous les pays de l'UE ainsi que l'Islande, le Liechtenstein et la Norvège. Lorsque des données à caractère personnel sont transférées en dehors de l'EEE, les protections offertes par le RGPD doivent accompagner les données. En d'autres termes, pour exporter des données à l'étranger, les entreprises doivent s'assurer que certaines garanties sont mises en place.

Le RGPD propose de nombreux mécanismes pour transférer les données vers des pays tiers. En vertu du RGPD, ces transferts sont autorisés lorsque:

1. les protections du pays sont jugées appropriées par l'UE; ou que
2. votre entreprise, par exemple, prend les mesures nécessaires pour fournir des garanties appropriées, notamment en intégrant des clauses spécifiques dans le contrat conclu avec l'importateur non européen des données à caractère personnel; ou que
3. votre entreprise, par exemple, s'appuie sur des motifs spécifiques pour le transfert (appelés «dérogations»), tels que le consentement de la personne concernée.

Pour plus d'informations sur les règles qui s'appliquent aux transferts internationaux de données, consultez la communication de la Commission européenne sur l'échange et la protection de données à caractère personnel à l'ère de la mondialisation: http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52017DC0007&from=FR

Devez-vous réaliser une analyse d'impact relative à la protection des données (AIPD)?

Réaliser une AIPD est obligatoire lorsque le traitement envisagé est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Tel peut, par exemple, être le cas lorsque de nouvelles technologies sont utilisées.

Au titre du RGPD, un risque aussi élevé survient lorsque:

- des mécanismes de traitement automatisé et de profilage sont utilisés pour examiner de manière systématique et considérable les personnes concernées;
- un espace public est systématiquement surveillé à grande échelle (par exemple, au moyen de la vidéosurveillance);
- des données sensibles sont traitées à grande échelle (par exemple, des données médicales).

L'objectif de l'AIPD consiste à déterminer les risques potentiels pour les droits et libertés des personnes concernées avant le début du traitement des données à caractère personnel et avant que le risque ne se matérialise. Atténuer le risque en amont permet d'éviter des dommages et de minimiser les coûts.

Si les mesures indiquées dans l'AIPD ne permettent pas de supprimer tous les risques élevés relevés, l'APD doit être consultée avant que le traitement des données envisagé ne débute.

«Réaliser une AIPD est obligatoire lorsque le traitement envisagé est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.»

Ce que vous devez faire

Répondre aux demandes

Si votre entreprise reçoit une demande d'une personne qui souhaite exercer ses droits, vous devez répondre à cette demande dans les meilleurs délais et, dans tous les cas, dans un délai d'un mois à compter de la réception de la demande. Cependant, le délai de réponse peut être prolongé de deux mois en cas de demande complexe ou multiple, pour autant que la personne concernée en soit informée. De plus, les demandes doivent être traitées **gratuitement**. Si une demande est rejetée, vous devez informer la personne concernée des raisons de ce rejet et de son droit à introduire une réclamation auprès de l'APD.

Prouvez que vous respectez les règles et tenez des registres!

Un des principes fondamentaux sous-jacents au RGPD est de s'assurer que les entreprises puissent démontrer qu'elles respectent les règles. Ainsi, vous devez pouvoir prouver que votre entreprise agit conformément au RGPD et qu'elle remplit toutes les obligations applicables — en particulier à la demande de l'APD ou en cas d'inspection par cette dernière.

Une manière de prouver ce respect consiste à tenir des registres détaillés, mentionnant notamment:

- le nom et les coordonnées de votre entreprise associée au traitement des données;
- la (les) raison(s) du traitement des données à caractère personnel;
- la description des catégories de personnes qui fournissent des données à caractère personnel;
- les catégories d'organisations recevant les données à caractère personnel;
- le transfert de données à caractère personnel vers un autre pays ou une autre organisation;
- la durée de conservation des données à caractère personnel;
- la description des mesures de sécurité utilisées pour le traitement des données à caractère personnel.

En outre, votre entreprise doit également maintenir — et régulièrement mettre à jour — des procédures écrites ainsi que des lignes directrices, et les communiquer à vos employés.

CHAPITRE 4

PRÊTS À VOUS CONFORMER AUX RÈGLES?

En ce qui concerne le traitement des données à caractère personnel, le RGPD place la balle dans votre camp. La première étape consiste à recenser vos activités actuelles de traitement des données et à réévaluer vos processus opérationnels internes. Vous devez notamment:

- recenser les données que vous détenez, ainsi que la finalité pour laquelle vous les détenez et la base juridique;
- évaluer tous les contrats en vigueur, en particulier ceux conclus entre les responsables du traitement et les sous-traitants;
- évaluer toutes les pistes disponibles pour les transferts internationaux; et
- revoir la gestion globale de votre entreprise (c'est-à-dire les mesures informatiques et organisationnelles que vous avez mises en place), que vous deviez ou souhaitiez ou non nommer un délégué à la protection des données.

Ce processus vise à garantir que le plus haut niveau de gestion de votre entreprise est engagé dans ces changements, en fournissant des informations et en étant régulièrement informé et consulté quant aux modifications apportées à la politique en matière de données.

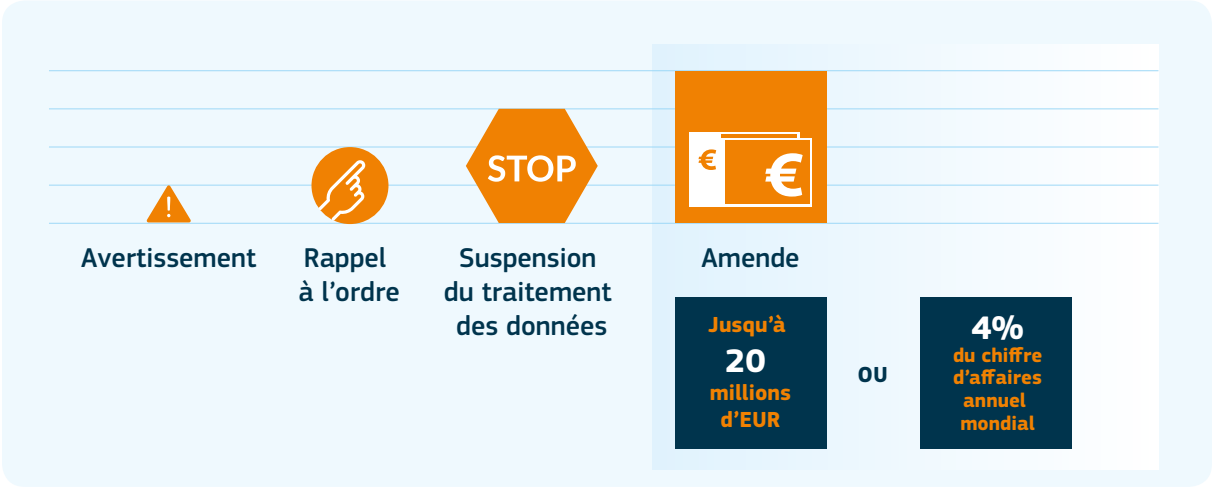
Vous traitez des données dans plus d'un pays?

Dans le cas d'un traitement dans plusieurs pays, une autorité de contrôle d'un autre pays peut être l'autorité compétente au lieu de votre APD nationale. En général, il s'agit de l'APD du pays dans lequel se situe l'établissement principal de votre entreprise (où les décisions relatives aux moyens et aux finalités du traitement sont prises) au sein de l'UE.

Les risques liés au non-respect des règles

Le non-respect du RGPD peut entraîner de lourdes amendes, qui peuvent s'élever jusqu'à 20 millions d'EUR ou 4 % du chiffre d'affaires global de votre entreprise pour certaines violations. L'APD peut imposer des mesures correctrices supplémentaires, telles que l'obligation de cesser le traitement des données à caractère personnel. Le non-respect du règlement pourrait également compromettre la réputation de votre entreprise.

En bref, les coûts liés au non-respect du RGPD sont bien plus importants que tout investissement réalisé pour s'y conformer.



Des questions? Des inquiétudes? Veuillez consulter votre APD nationale.

Trouver votre autorité de protection des données nationale en ligne

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

AVIS IMPORTANT

Les informations et orientations contenues dans cette brochure ont pour objectif de contribuer à une meilleure compréhension des règles de l'UE en matière de protection des données.

Elles servent d'orientation — seul le texte du règlement général sur la protection des données (RGPD) a une valeur juridique. Il en résulte que seul le RGPD est susceptible de créer des droits et obligations pour les personnes. Ces orientations ne créent aucun droit susceptible d'être invoqué ni aucune attente.

L'interprétation contraignante de la législation de l'UE relève de la compétence exclusive de la Cour de justice de l'Union européenne. Les avis exprimés dans ces orientations ne préjugent pas de la position que la Commission pourrait adopter devant la Cour de justice.

Ni la Commission européenne ni aucune personne agissant en son nom ne saurait être tenue responsable de l'utilisation qui pourrait être faite des informations contenues dans la brochure.

Cette brochure reflétant la situation au moment de sa rédaction, elle doit être considérée comme un «document vivant» susceptible d'être amélioré, et son contenu peut faire l'objet de modifications sans préavis.

Comment prendre contact avec l'Union européenne?

En personne

Dans toute l'Union européenne, des centaines de centres d'information Europe Direct sont à votre disposition. Pour connaître l'adresse du centre le plus proche, visitez la page suivante: https://europa.eu/european-union/contact_fr

Par téléphone ou courrier électronique

Europe Direct est un service qui répond à vos questions sur l'Union européenne. Vous pouvez prendre contact avec ce service:

– par téléphone: via un numéro gratuit: 00 800 6 7 8 9 10 11 (certains opérateurs facturent cependant ces appels),
– au numéro de standard suivant: +32 22999696;
– par courrier électronique via la page https://europa.eu/european-union/contact_fr

Comment trouver des informations sur l'Union européenne?

En ligne

Des informations sur l'Union européenne sont disponibles, dans toutes les langues officielles de l'UE, sur le site internet Europa à l'adresse https://europa.eu/european-union/index_fr

Publications de l'Union européenne

Vous pouvez télécharger ou commander des publications gratuites et payantes sur le site EU Bookshop à l'adresse suivante: https://publications.europa.eu/bookshop. Vous pouvez obtenir plusieurs exemplaires de publications gratuites en contactant Europe Direct ou votre centre d'information local (https://europa.eu/european-union/contact_fr).

Droit de l'Union européenne et documents connexes

Pour accéder aux informations juridiques de l'Union, y compris à l'ensemble du droit de l'UE depuis 1952 dans toutes les versions linguistiques officielles, consultez EUR-Lex à l'adresse suivante: http://eur-lex.europa.eu

Données ouvertes de l'Union européenne

Le portail des données ouvertes de l'Union européenne (http://data.europa.eu/euodp/fr) donne accès à des ensembles de données provenant de l'UE. Les données peuvent être téléchargées et réutilisées gratuitement, à des fins commerciales ou non commerciales.

DS-01-18-082-FR-C

Le règlement général sur la protection des données (RGPD) réglemente la manière dont les entreprises traitent et gèrent les données à caractère personnel. Grâce à cette législation européenne unique en matière de protection des données à caractère personnel, votre entreprise ne doit désormais se conformer essentiellement qu'à une seule législation en matière de protection des données tout en pouvant proposer des biens et des services dans l'ensemble de l'UE.

En simplifiant le cadre réglementaire pour les entreprises, le RGPD représente une nouvelle opportunité pour votre entreprise d'améliorer la gestion des données à caractère personnel et, ainsi, d'accroître la confiance des consommateurs en votre entreprise.

Cette brochure met l'accent sur les obligations de votre entreprise au titre du RGPD.

europa.eu/dataprotection/fr

Office des publications

ISBN 978-92-79-79440-7