Règlement Général sur la Protection des Données

GUIDE DE POCHE

JONES DAY® | One Firm Worldwide℠

TABLE DES MATIERES0

Introduction 1

Champ d'application 2

Fondements juridiques de traitement des données 3

Droits des personnes 4

Responsabilités et mécanismes de gouvernance 6

Obligations et contrats de sous-traitance 7

Sécurité des données et notification des violations de données personnelles 8

Codes de conduite et certifications 9

Transferts transfrontaliers de données personnelles 10

Supervision par les autorités de contrôle (AC) 11

Voies de recours, responsabilités et sanctions 12

Glossaire 13

Contacts 15

INTRODUCTION

En mai 2016, l'Union européenne (UE) a publié le Règlement Général sur la Protection des Données («RGPD»). Cet instrument juridique majeur représente le changement le plus significatif survenu dans le droit de l'UE sur la protection des données depuis 1995. Il sera applicable dans tous les Etats membres de l'UE à partir du 25 mai 2018.

Le RGPD est un texte d'envergure qui aura un impact significatif pour toutes les entreprises qui mettent en œuvre des traitements de données personnelles, y compris pour celles situées en dehors de l'UE. Il augmentera les sanctions en cas de non-respect, avec des amendes allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial. De plus, les autorités de contrôle disposeront d'un certain nombre de pouvoirs élargis.

Les entreprises devraient examiner le RGPD et commencer à se mettre en conformité avec le nouveau cadre juridique de protection des données de l'UE.

Ce guide, en proposant un rapide aperçu des nouvelles règles imposées par ce Règlement et les principaux changements qu'il entraînera, permettra d'aider les utilisateurs à se préparer pour le RGPD. Ce guide comprend également un court glossaire des termes utilisés dans le RGPD, et chaque section prévoit une courte «to-do list» pour pouvoir se mettre en conformité. Ce guide sera rapidement suivi d'orientations supplé-mentaires, de briefings et de «checklists» pratiques sur le RGPD.

Nous espérons que ce guide vous sera utile. N'hésitez pas à contacter l'un des avocats listés à la page 15 si vous souhaitez recevoir des informations complémentaires.

CHAMP D'APPLICATION

ARTICLES 2 ET 3

Bref aperçu

Le RGPD s'applique aux traitements automatisés de données à caractère personnel ou faisant partie d'un fichier. Les champs d'application matériel et territorial du RGPD sont tous deux plus larges que ceux de la Directive Européenne sur la Protection des Données («Directive»).

Application

- Le RGPD s'applique aux responsables du traitement tout comme aux sous-traitants.
- Le RGPD ne s'applique pas dans un nombre limité de domaines, tels que le traitement de données effectué dans un cadre strictement personnel ou domestique.

Champ d'application territorial

Le RGPD s'applique aux traitements :

- Réalisés dans le cadre des activités d'un établissement situé dans l'UE ;
- Effectués par un responsable du traitement ou par un sous-traitant - non établi au sein de l'UE - de données des personnes concernées dans l'UE, lorsque ces traitements sont liés à :
  - *L'offre de biens et de services à ces personnes concernées ; ou*
  - *Au suivi du comportement des personnes concernées.*

Prochaines étapes

- ✓ Identifier les traitements de données personnelles pertinents.
- ✓ Confirmer quels établissements au sein de l'UE participent au traitement de données personnelles et quels traitements de données concernent l'offre de biens et de services dans l'UE ou le suivi du comportement de personnes concernées dans l'UE.
- ✓ Evaluer si le traitement est effectué en tant que responsable du traitement ou en tant que sous-traitant.
- ✓ Déterminer s'il est nécessaire d'avoir recours à un représentant au sein de l'UE.

FONDEMENTS JURIDIQUES DE TRAITEMENT DES DONNEES

ARTICLES 6, 7 ET 8

Bref aperçu

Les fondements juridiques de traitement des données personnelles au titre du RGPD sont essentiellement les mêmes que ceux de la Directive. Néanmoins, le RGPD prévoit de nouvelles restrictions concernant le consentement, le traitement à des fins d'intérêt légitime ainsi que le traitement pour des finalités autres.

Fondements juridiques de traitement de données personnelles

Les fondements juridiques pour le traitement de données prévus par le RGPD sont :

- Le consentement de la personne concernée ;
- Lorsque le traitement est nécessaire :
  - *Pour l'exécution ou la négociation d'un contrat avec la personne concernée ;*
  - *Pour respecter une obligation légale ;*
  - *Pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne lorsque la personne concernée est incapable de donner son consentement ;*
  - *Pour l'exécution d'une mission d'intérêt public ou l'exercice de l'autorité publique ; ou*
  - *Aux fins d'intérêts légitimes (sous réserve des droits et des libertés fondamentaux).*

Nouvelles restrictions portant sur le consentement, le traitement à des fins d'intérêt légitime ainsi que le traitement pour des finalités autres.

- Pour les traitements fondés sur le consentement, le responsable du traitement doit être en mesure de prouver que le consentement a été donné librement par la personne concernée, et la demande de consentement doit être clairement distinguée.
- Le RGPD précise les cas dans lesquels les «intérêts légitimes» peuvent servir de fondement pour un traitement (p. ex. la prospection, la prévention de la fraude, le partage de données personnelles au sein d'un groupe de sociétés à des fins administratives internes ou pour assurer la sécurité des informations et des réseaux) et exige que le responsable du traitement informe la personne concernée lorsqu'il se fonde sur des intérêts légitimes pour procéder au traitement.
- Le RGPD fournit une liste de critères à prendre en compte pour déterminer si le traitement de données pour des nouvelles finalités est compatible avec la finalité initiale pour laquelle les données ont été collectées.

Prochaines étapes

- ✓ Evaluer les fondements juridiques des traitements des données en cours et vérifier qu'ils demeurent valables avec le RGPD.
- ✓ S'assurer que le consentement a été donné conformément aux nouvelles exigences et que le responsable du traitement est en mesure de le prouver.
- ✓ Lorsque le traitement est fondé sur des «intérêts légitimes», s'assurer que :
  - *l'équilibre entre les intérêts légitimes et les droits de la personne concernée est documenté ; et*
  - *lorsqu'un responsable du traitement se fonde sur des intérêts légitimes pour procéder aux traitements, cette information doit être fournie à la personne concernée.*
- ✓ S'assurer que les processus de gouvernance interne documentent les motifs poussant à prendre la décision d'utiliser les données aux fins de traitements ultérieurs.

DROITS DES PERSONNES

ARTICLES 12 A 17, 19, 20 ET 21

Bref aperçu

Les responsables du traitement des données doivent être plus transparents avec les personnes concernées, lesquelles se voient conférer des droits renforcés en termes d'accès à leurs données et d'importants nouveaux droits d'exiger la rectification ou l'effacement de leurs données personnelles et de restreindre les traitements ultérieurs.

Communication d'informations

Les personnes physiques doivent recevoir des informations sur la manière dont leurs données seront traitées, y compris des informations relatives à :

- L'identité du responsable de traitements et ses coordonnées ;
- Tout délégué à la protection des données ;
- Les finalités et le fondement juridique de traitement des données ;
- Tout «intérêt légitime» utilisé comme fondement de traitement des données ;
- Tout transfert international et les mesures de protection applicables ;
- La durée de conservation ou les critères permettant de la déterminer ;
- Le droit à la portabilité des données et le droit de s'opposer au traitement, d'exiger des restrictions et de retirer son consentement au traitement ;
- Le droit d'introduire une réclamation auprès de l'autorité de contrôle (AC) ; et
- Toute obligation légale ou contractuelle de fournir des données, ainsi que les conséquences en cas de non-communication.

Cette information doit être concise, claire et intelligible ; doit être fournie sous une forme facilement accessible ; et doit utiliser des termes clairs et simples, tout particulièrement lorsqu'elle est destinée à des enfants.

Lorsque les données sont obtenues de manière directe, le responsable du traitement doit expliquer quelles informations sont obligatoires et les conséquences de leur non-communication. Lorsque les données sont obtenues de manière indirecte, le responsable du traitement doit indiquer la source d'information, y compris lorsqu'il s'agit de sources d'informations publiquement accessibles.

Droit d'accès

Les personnes concernées ont le droit d'obtenir des copies de leurs données personnelles, ainsi que les détails essentiels portant sur la manière dont les données sont traitées. Les personnes physiques bénéficient d'un droit d'accès accru à leurs données.

- Les responsables du traitement ne peuvent pas exiger de paiement au titre du droit d'accès mais peuvent prévoir un coût administratif raisonnable pour les copies supplémentaires.
- Les personnes physiques doivent se voir fournir des informations concernant les transferts internationaux ; les durées de conservation ; les droits de rectification, d'effacement, et la limitation des traitements ; ainsi que le droit de s'opposer au traitement et d'introduire une réclamation auprès de l'AC.
- Les responsables du traitement doivent divulguer toute source tierce des données ainsi que la portée et les conséquences de tout traitement fondé sur des décisions automatisées.

Droits des personnes concernées

Les personnes concernées disposent d'importants droits liés à leurs données personnelles, incluant notamment :

- Le droit d'obtenir la rectification des données personnelles dans les meilleurs délais et le droit de faire compléter toutes les données personnelles incomplètes ;
- Le droit d'effacer les données personnelles («droit à l'oubli») lorsque le traitement n'est plus nécessaire, que le consentement est retiré, qu'il n'y a plus d'intérêt légitime, que le traitement est illégal ou que l'effacement est exigé par la loi, et le responsable du traitement doit prendre les mesures raisonnables pour en informer les autres responsables du traitement s'il a rendu ces données publiques ;
- Le droit de limiter le traitement des données personnelles («restriction») lorsque l'exactitude est contestée, lorsqu'une opposition au traitement a été acceptée, lorsque le traitement est illicite et que la personne concernée s'oppose à l'effacement, ou lorsque le responsable du traitement n'a plus besoin des données mais que celles-ci sont nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ; et

- Le droit de demander que les données fournies par les personnes concernées pour des traitements avec leur consentement ou en vertu d'un contrat soient fournies sous une forme couramment utilisée et lisible par machine, et de les transmettre à un autre responsable du traitement («portabilité des données»).

Les responsables du traitement doivent notifier aux destinataires des données toute rectification, effacement et restriction, à moins que cela soit impossible ou que cela implique de fournir des efforts disproportionnés. Si les personnes concernées le requièrent, les responsables du traitement doivent informer les personnes concernées de l'identité des destinataires des données.

Prochaines étapes

- ✓ Revoir les notices d'information et les chartes de respect de la vie privée.
- ✓ Revoir les procédures en place pour gérer le droit d'accès des personnes concernées.
- ✓ Evaluer les méthodes permettant de se conformer aux requêtes de portabilité et de restriction des données.
- ✓ Examiner l'incidence du droit à l'oubli pour les systèmes informatiques.
- ✓ Envisager des moyens pour automatiser les réponses aux requêtes individuelles.

RESPONSABILITES ET MECANISMES DE GOUVERNANCE

ARTICLES 24, 25, 30, 32, 35, 37, 40 ET 42

Bref aperçu : les nouvelles règles

Contrairement à la Directive, le RGPD impose aux responsables du traitement de mettre en place des programmes permettant d'assurer la mise en conformité et d'en fournir la preuve aux AC ainsi qu'aux personnes concernées.

Mesures techniques et organisationnelles appropriées

Les responsables du traitement doivent mettre en place des mesures techniques et organisationnelles appropriées. Lesquelles peuvent inclure :

- La mise en place de politiques de protection des données ;
- L'adhésion à des codes de conduite approuvés ; et
- L'adhésion à des mécanismes de certification approuvés.

Protection des données dès la conception et protection des données par défaut

Les responsables du traitement doivent mettre en place des mesures techniques et organisationnelles conçues pour mettre en œuvre les principes de protection des données (tels que la pseudonymisation et la minimisation des données), tant lorsqu'ils déterminent les moyens du traitement qu'à l'occasion du traitement lui-même. Par défaut, seules les données personnelles nécessaires pour une finalité déterminée peuvent faire l'objet d'un traitement.

Analyse d'impact relative à la protection des données

Avant que le traitement soit mis en œuvre, les responsables du traitement doivent mener une étude d'impact si le traitement peut engendrer un risque élevé pour les droits des personnes concernées (p. ex. les décisions fondées sur des procédés automatisés ou sur du profilage, le traitement de données sensibles à grande échelle, la surveillance systématique à grande échelle d'une zone accessible au public).

Désignation d'un délégué à la protection des données

Les responsables du traitement et les sous-traitants doivent chacun désigner un délégué à la protection des données («DPD») si leurs activités de base requièrent une surveillance à grande échelle régulière et systématique des personnes concernées ou le traitement à grande échelle de données sensibles. Les autorités ou les organismes publics doivent également désigner des DPD. La désignation volontaire d'un DPD est possible. Par ailleurs, le droit national peut prévoir que la désignation soit obligatoire dans d'autres cas que ceux prévus par le RGPD.

Documentation (registre des activités de traitement)

Les responsables du traitement doivent conserver un registre de leurs activités de traitement comportant un certain nombre d'informations prédéfinies (y compris la finalité du traitement, une description des catégories de personnes concernées, les données personnelles et les destinataires de ces données, les mesures techniques et organisationnelles mises en œuvre, et tout transfert de ces données vers des
pays tiers).

Prochaines étapes

- ✓ Attribuer la responsabilité et prévoir un budget pour la conformité en matière de protection des données, et s'assurer du soutien de l'équipe de direction.
- ✓ Revoir les niveaux de conformité existants. (Cela implique de revoir les politiques de protection des données et de sécurité des systèmes informatiques existants et d'identifier les activités de traitement des données pertinentes).
- ✓ Conduire une analyse des lacunes par rapport aux exigences de responsabilité au titre de la protection des données.
- ✓ Mettre à jour les procédures existantes pour assurer la mise en conformité et développer de nouvelles procédures lorsque cela est nécessaire.
- ✓ Déterminer si la désignation d'un DPD est obligatoire ; sinon, envisager une désignation volontaire.

OBLIGATIONS ET CONTRATS DE SOUS-TRAITANCE

ARTICLES 28 A 33 ET 37

Bref aperçu : les nouvelles règles

Le RGPD prescrit des exigences applicables aux contrats conclus entre les responsables du traitement et les sous-traitants pour le traitement de données personnelles. Ces exigences sont plus détaillées que celles prévues par la Directive.

De plus, le RGPD prévoit de nouvelles obligations pour les sous-traitants.

Exigences liées aux contrats de sous-traitance de données pour les responsables du traitement et pour les sous-traitants

- Les responsables du traitement doivent uniquement avoir recours à des sous-traitants qui fournissent des garanties techniques et organisationnelles suffisantes pour satisfaire les exigences du RGPD.
- Le contrat entre le responsable du traitement et le sous-traitant doit être écrit.
- Le contrat de traitement doit prévoir que :
  - *Le sous-traitant traite les données uniquement selon les instructions du responsable du traitement ;*
  - *Le sous-traitant doit s'assurer que son personnel est soumis à une obligation de confidentialité ;*
  - *Le sous-traitant doit mettre en place des mesures techniques et organisationnelles appropriées pour assurer aux données personnelles un niveau de sécurité proportionnel au risque ;*
  - *Le sous-traitant ne peut pas sous-traiter le traitement des données sans l'autorisation préalable écrite du responsable du traitement ;*
  - *Tout contrat entre un sous-traitant et un sous-traitant de rang ultérieur doit prévoir les mêmes obligations de protection des données que celles prévues par le contrat conclu avec le responsable du traitement ;*
  - *Le sous-traitant doit assister le responsable du traitement pour assurer la conformité aux obligations de sécurité, à l'évaluation de l'impact sur la vie privée, et à la consultation préalable avec les AC pour le traitement des données à haut risque ;*
  - *Le sous-traitant doit effacer ou retourner les données personnelles une fois le traitement terminé ; et*
  - *Le sous-traitant doit fournir au responsable du traitement toutes les informations nécessaires pour démontrer la conformité et permettre ou contribuer aux audits.*

Obligations directes des sous-traitants

A l'exception d'un nombre limité de cas d'entreprises ou d'organisations qui emploient moins de 250 personnes :

- Le sous-traitant doit conserver un registre écrit de toutes les catégories de traitements mises en œuvre pour le compte de chaque responsable du traitement ; et
- Le sous-traitant doit rendre son registre accessible aux AC sur requête. De plus, chaque sous-traitant doit :
- Mettre en place des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité approprié ;
- Prendre des mesures pour s'assurer que les membres du personnel ayant accès aux données personnelles procèdent au traitement uniquement conformément aux instructions du responsable du traitement ;
- Notifier toute violation des données personnelles au responsable du traitement, dès que le sous-traitant en a connaissance et sans délai ; et
- Désigner un DPD dans des cas précis, y compris lorsque : (i) le traitement requiert un suivi régulier et systématique des personnes concernées à une grande échelle, et (ii) les données faisant l'objet du traitement sont liées à des condamnations pénales et à des infractions.

Prochaines étapes

- ✓ Les responsables du traitement doivent s'assurer que tous les contrats avec des sous-traitants sont conformes au RGPD.
- ✓ Les sous-traitants doivent déterminer si des registres liés au traitement des données pour un responsable du traitement doivent être conservés.
- ✓ Les sous-traitants doivent mettre en place des mesures techniques et organisationnelles pour garantir un niveau de sécurité approprié des données personnelles et doivent mettre en place une politique de déclaration des violation des données.
- ✓ Les sous-traitants doivent déterminer si un DPD est nécessaire.

SECURITE DES DONNEES ET NOTIFICATION DES VIOLATIONS DE DONNEES PERSONNELLES

SECTIONS 32 A 34 ET 37

Bref aperçu : les nouvelles règles

Les responsables du traitement et les sous-traitants sont maintenant soumis à un régime de notification des violations. Lorsque cela est possible, les responsables du traitement doivent notifier les violations les plus sérieuses dans un délai de 72 heures.

Exigences de sécurité des données

- Les responsables du traitement et les sous-traitants doivent chacun mettre en œuvre des mesures de sécurité techniques et organisationnelles appropriées pour garantir un niveau adéquat de protection des données personnelles.
- Si nécessaire, les mesures de sécurité doivent comprendre la pseudonymisation et le cryptage, la capacité à restaurer rapidement les données personnelles, ainsi que des évaluations et des tests réguliers.
- Les responsables du traitement et les sous-traitants ayant des activités de traitement ou de suivi à grande échelle doivent désigner un DPD.

Régime de notification des violations de données personnelles

Les responsables du traitement et les sous-traitants sont maintenant soumis à un régime de notification des violations de données personnelles :

- Les responsables du traitement doivent notifier dans les meilleurs délais aux AC pertinentes toute violation de données personnelles (si possible, dans un délai de 72 heures à compter de la prise de connaissance de la violation), à moins que la iolation ne soit pas de nature à porter atteinte aux droits et aux libertés des personnes concernées.
- Les responsables du traitement doivent avertir les personnes concernées par la violation si celle-ci fait courir un risque sérieux à leurs droits et à leurs libertés.
- Les sous-traitants doivent notifier, dans tous les cas, dans les meilleurs délais toute violation de données personnelles au responsable du traitement.

Prochaines étapes

- ✓ Mettre en place des procédures permettant d'identifier les incidents de sécurité, d'y répondre et d'effectuer les notifications requises.
- ✓ Attribuer la responsabilité pour la sécurité des données personnelles.
- ✓ S'assurer que les sous-traitants sont obligés de notifier les violations des données personnelles, et qu'ils mettent en œuvre des systèmes de sécurité adéquats.
- ✓ Vérifier l'étendue de la couverture d'assurance en termes de cyber risques.
- ✓ Evaluer la sécurité et conduire des tests de manière régulière.

CODES DE CONDUITE ET CERTIFICATIONS

ARTICLES 40 A 43

Bref aperçu : les nouvelles règles

Le RGPD prévoit l'approbation de codes de conduite et l'accréditation de certificats, labels et marques, particulièrement au niveau de l'UE, pour aider les responsables du traitement et les sous-traitants à démontrer leur conformité aux règles de protection des données. Les codes de conduite, bien que mentionnés dans la Directive, jouaient un rôle bien moins important que celui qu'ils jouent dans le RGPD. Avec le RGPD, les certifications sont régulées pour la première fois à un niveau paneuropéen.

Codes de conduite

- Avec le RGPD, les associations et les autres entités représentatives peuvent préparer, modifier ou étendre un code de conduite dans le but de préciser de quelle manière le RGPD s'applique à certains secteurs industriels.
- Un code de conduite doit être soumis à l'AC compétente pour être approuvé, enregistré et publié.
- Dans les cas de traitements transfrontaliers, un code de conduite doit être soumis au Comité européen de la protection des données («Comité»), lequel délivre un avis. La Commission européenne («Commission») peut décider que le code de conduite est d'application générale au sein de l'UE. Le Comité rassemblera tous les codes de conduite au sein d'un registre accessible au public.
- La conformité à un code de conduite est sujette au suivi par des organismes accrédités. En cas d'infraction, la société en cause peut voir son statut d'adhérent au code suspendu et l'infraction pourra être rapportée à l'AC compétente.
- L'adhésion à un code de conduite permet aux responsables du traitement de données et aux sous-traitants situés en dehors de l'Espace economique européen («EEE») de démontrer qu'ils ont mis en œuvre des mesures de protection adéquates afin de permettre le transfert des données depuis les pays membres de l'EEE vers des pays en dehors de l'EEE.

Mécanismes de certification, de labels et de marques

- La mise en place de mécanismes de certification de protection des données, de labels et de marques est encouragée afin de démontrer la conformité.
- L'adhésion aux mécanismes de certification, de labels et de marques permet aux responsables du traitement et aux sous-traitants situés en dehors de l'EEE de démontrer qu'ils ont mis en œuvre des mesures de protection adéquates afin de permettre le transfert des données depuis les pays membres de l'EEE vers des pays en dehors de l'EEE.
- L'AC compétente ou le Comité approuveront les critères de certification. Le Comité pourra développer des critères pour une certification commune, *i.e.* le Label européen de protection des données.
- Les certifications seront délivrées par des organismes de certification accrédités. Les accréditations des organismes de certification seront délivrées pour une période maximum de cinq ans et seront soumises à la possibilité de leur renouvellement ou de leur retrait lorsque les conditions d'accréditation ne sont plus remplies. Les certifications seront valables pour une durée maximum de trois ans et pourront être renouvelées ou retirées si les conditions de certification ne sont plus remplies.
- Le Comité tiendra un registre accessible au public de tous les mécanismes de certification, de labels et de marques.

Prochaines étapes

- ✓ Identifier ou créer des associations ou des organismes de représentation pouvant développer des codes de conduite, en particulier pour les traitements de données transfrontaliers.
- ✓ Suivre les accréditations des organismes de certification et envisager de déposer des demandes de certification.
- ✓ Comprendre les systèmes de certification et se renseigner sur les certifications, les labels et les marques lors de la sélection de prestataires de services.

TRANSFERTS TRANSFRONTALIERS DE DONNEES PERSONNELLES

ARTICLES 44 A 50

Bref aperçu : les nouvelles règles

Comme la Directive, le RGPD exige une base légale adéquate pour les transferts de données personnelles vers des pays situés en dehors de l'EEE. Le RGPD a élargi les bases légales possibles pour le transfert des données en incluant des codes de conduite approuvés et des mécanismes de certification.

- La Commission peut adopter des décisions d'adéquation selon lesquelles certains pays tiers, ou des territoires ou des secteurs au sein desdits pays, sont réputés offrir un niveau de protection suffisant pour les transferts transfrontaliers. Les transferts vers de tels pays, territoires ou secteurs ne nécessitent aucune autorisation particulière. La liste de la Commission relative aux pays tiers offrant un niveau de protection adéquat demeure en vigueur et comprend le «Privacy shield» UE-États-Unis pour le transfert de données depuis les pays de l'EEE vers les États-Unis.
- En l'absence d'une décision d'adéquation, les données personnelles peuvent être transférées vers des pays tiers situés en dehors de l'EEE uniquement lorsque des garanties appropriées sont mises en place. De telles garanties comprennent les clauses type de protection des données qui peuvent être adoptées ou approuvées par la Commission, tout comme des règles d'entreprise contraignantes («BCR») dont le contenu requis est maintenant détaillé par le RGPD. D'autres transferts sujets à des garanties particulières sont ceux permis lorsqu'un code de conduite approuvé, un mécanisme de certification approuvé ou instrument juridique contraignant entre des autorités publiques est mis en œuvre.
- En l'absence d'une décision d'adéquation ou de garanties appropriées, les transferts transfrontaliers sont possibles à l'une des conditions suivantes : (i) le consentement explicite est donné par la personne concernée après qu'elle a été informée des risques potentiels de tels transferts ; (ii) le transfert est nécessaire à l'exécution d'un contrat ou à la mise en œuvre de mesures précontractuelles entre le responsable du traitement et la personne concernée ; (iii) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne morale concernée ; (iv) le transfert est nécessaire pour des motifs importants d'intérêt public ; (v) le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ; (vi) le transfert est nécessaire à la sauvegarde d'intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ; (vii) le transfert à lieu au départ d'un registre public.
- Le RGPD aborde également les situations d'e-discovery des pays tiers en énonçant que les jugements ou les décisions des autorités administratives de pays tiers, requérant le transfert de données personnelles, peuvent être reconnus ou appliqués seulement s'ils sont fondés sur un accord international, tel qu'un traité d'entraide judiciaire entre le pays tiers requérant et l'Union européenne ou un Etat membre de l'UE, sans préjudice des fondements mentionnés ci-dessus permettant le transfert en vertu du RGPD.

Prochaines étapes

- ✓ Etablir la cartographie des flux des données.
- ✓ Revoir les bases légales pour tous les transferts de données transfrontaliers existants vers des pays situés en dehors de l'EEE.
- ✓ Revoir le contenu des BCR et s'assurer de leur conformité aux exigences du RGPD.
- ✓ Envisager de nouveaux fondements pour les transferts de données, tels que des codes de conduite et des certifications.
- ✓ Se tenir informé des développements législatifs concernant les décisions d'adéquation.

SUPERVISION PAR LES AUTORITES DE CONTROLE (AC)

ARTICLES 51 A 76

Bref aperçu : les nouvelles règles

Le RGPD prévoit des règles détaillées et harmonisées applicables à l'organisation et aux pouvoirs des AC. Il prévoit également des mécanismes de coopération et de coordination pour répondre aux problèmes relatifs aux procédures de transferts transfrontaliers.

Autorités de contrôle

Les Etats membres de l'UE conserveront au moins une AC par pays.

- L'indépendance des AC sera, entre autres, renforcée par des règles relatives à la création des AC, à la nomination et à la révocation de ses membres.
- Les missions et les pouvoirs des AC seront élargis, y compris le pouvoir de réaliser des audits et d'accéder aux locaux des responsables du traitement et des sous-traitants.
- Le RGPD met en place un mécanisme de «guichet unique» par lequel les AC désignent une autorité chef de file (principalement sur le fondement de l'établissement principal du responsable du traitement ou du sous-traitant) et coopèrent afin d'adopter des décisions sur le traitement transfrontalier des données.

Comité Européen de la Protection des Données

Le Comité Européen de la Protection des Données remplacera le groupe de travail de l'article 29.

- Le Comité sera composé du directeur d'une AC de chaque Etat membre de l'UE et du Contrôleur Européen de la Protection des Données («CEPD»). Il bénéficiera d'un secrétariat permanent fourni par le CEPD, basé à Bruxelles.
- Le Comité rend des décisions et des orientations et s'assure de la cohérence dans la mise en œuvre du RGPD.
- Le Comité a un pouvoir de décision contraignant en cas de désaccord entre les AC dans le cadre de la procédure de «guichet unique» (p. ex. décider quelle AC devrait être l'autorité chef de file ou déterminer le contenu de la décision finale lors de la résolution d'un litige).

Prochaines étapes

- ✓ Suivre les développements juridiques nationaux modifiant la structure institutionnelle des AC.
- ✓ Comprendre les pouvoirs d'enquête élargis des AC pour l'organisation de la conformité en interne.
- ✓ Déterminer qui sera l'AC chef de file pour l'entreprise.
- ✓ Se préparer à la possibilité d'intervenir devant le Comité et de faire appel de ses décisions.

VOIES DE RECOURS, RESPONSABILITES ET SANCTIONS

ARTICLES 77 A 84

Bref aperçu : les nouvelles règles

Le RGPD prévoit des voies de recours étendues pour les personnes concernées et des responsabilités accrues pour les responsables du traitement et les sous-traitants, ainsi que des sanctions renforcées de manière significative comportant des amendes similaires à celles prévues par le régime anti monopole de l'UE. A l'inverse de la Directive, le RGPD prévoit, en détail, les conditions pour prononcer des amendes ainsi que leur montant maximum.

Recours

Les personnes concernées ont les droits suivants à l'encontre des responsables du traitement et des sous-traitants :

- Le droit d'introduire une réclamation (*via* les associations représentatives, entre autres) auprès des AC de l'Etat membre de l'UE de résidence de la personne concernée, de son lieu de travail ou du lieu de l'infraction, y compris la possibilité de former des appels dans le cas où l'AC ne traiterait pas la réclamation ;
- Le droit de former un recours contre une décision contraignante d'une AC devant les juridictions nationales ; et
- Le droit d'engager des procédures judiciaires devant les juridictions nationales du lieu d'établissement du responsable du traitement ou du sous-traitant ou du lieu de résidence de la personne concernée.

Indemnisation et responsabilité

Sous le RGPD, le responsable du traitement et le sous-traitant ont l'obligation d'indemniser intégralement la personne concernée pour tous les dommages matériels et moraux résultant d'une violation des dispositions du RGPD. Cela s'applique également s'il existe plus d'un responsable du traitement ou sous-traitant, ou si un responsable du traitement et un sous-traitant partagent la responsabilité du dommage causé par le traitement («responsabilité solidaire»).

Sanctions

Les AC peuvent imposer des amendes administratives.

- En fonction du type d'infraction, les amendes peuvent s'élever jusqu'à 20 millions d'euros ou, dans le cas d'entreprises, à 4% du chiffre d'affaires annuel mondial, selon ce qui est le plus élevé des deux montants.
- Les amendes doivent être déterminées sur la base des critères listés par le RGPD et sont soumises à un contrôle juridictionnel et à des garanties procédurales.
- Les Etats membres de l'UE peuvent prévoir des sanctions supplémentaires, y compris des sanctions pénales.

Prochaines étapes

- ✓ Prendre en considération les nouvelles responsabilités et sanctions pour définir la stratégie de mise en conformité.
- ✓ Evaluer les risques de responsabilité découlant des contrats existants avec des clients ou prestataires et comportant une clause de limitation de responsabilité.
- ✓ Déterminer quelle sera la juridiction la plus probable pour les procédures.
- ✓ Suivre les développements législatifs nationaux prévoyant des sanctions additionnelles.

GLOSSAIRE

Règles d'Entreprise Contraignantes (BCR)	Les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous- traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe. (RGPD, Article 4 (20))
Consentement de la personne concernée	Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement. (RGPD, Article 4 (11))
Responsable du traitement	La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. (RGPD, Article 4 (7))
Sous-traitant	La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. (RGPD, Article 4 (8))
Destinataire	La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. (RGPD, Article 4 (9))
Personne Concernée	Une personne physique identifiée ou identifiable dont les données personnelles font l'objet d'un traitement. (RGPD, Article 4 (1))
Règlement Général sur la Protection des Données (RGPD)	Règlement (UE) 2016/679 du 27 avril 2016, abrogeant la directive 95/46/CE, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
Donnée à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. (RGPD, Article 4 (1))
Traitement	Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. (RGPD, Article 4 (2))

Suite à la page 13

GLOSSAIRE

Profilage	Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique. (RGPD, Article 4 (4))
Tiers	Une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel. (RGPD, Article 4 (10))

CONTACTS

Dr. Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Jonathon Little
Londres
+44.20.7039.5224
jrlittle@jonesday.com

Elizabeth A. Oberle-Robertson
Londres
+44.20.7039.5204
erobertson@jonesday.com

Paloma Bru
Madrid
+34.91.520.3985
pbru@jonesday.com

Olivier Haas
Paris
+33.1.56.59.38.84
ohaas@jonesday.com

Dr. Jörg Hladjk
Bruxelles
+32.2.645.15.30
jhladjk@jonesday.com

Giuseppe Mezzapesa
Milan
+39.02.7645.4001
gmezzapesa@jonesday.com

Laurent De Muyter
Bruxelles
+32.2.645.15.13
ldemuyter@jonesday.com

CONTACTS HORS EUROPE

Daniel J. McLoon
Los Angeles
+1.213.243.2580
djmcloon@jonesday.com

Richard J. Johnson
Dallas
+1.214.969.3788
jjohnson@jonesday.com

Todd S. McClelland
Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Jeff Rabkin
San Francisco
+1.415.875.5850
jrabkin@jonesday.com


JONES DAY
One Firm Worldwide℠