LE RGPD en 10 points

Se mettre en conformité d'ici le 25 mai 2018

EDITIONS LEGISLATIVES

Sommaire

1 Présentation du RGPD et contexte

Le RGPD sera applicable à partir du 25 mai 2018 dans tous les États membres de l'Union européenne. Adapté à l'ère numérique, le texte remplace la directive sur la protection des données qui date de 1995.

Fruit de quatre années de travail et de négociations, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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 (règlement général sur la protection des données, dit RGPD) abroge la directive 95/46/CE du 24 octobre 1995 du même nom. Entré en vigueur le 25 mai 2016, il comporte 99 articles et 173 considérants, en comparaison des 34 articles de la directive. Il est applicable à partir du 25 mai 2018, date à laquelle tous les organismes - tant privés que publics - devront s'y conformer.

Contexte

Le RGPD s'inscrit dans un contexte bien différent de celui d'il y a vingt ans. L'évolution rapide des technologies, la mondialisation, l'augmentation de l'ampleur de la collecte et du partage de données, l'utilisation accrue des données tant par les entreprises privées que par les autorités publiques, le développement des réseaux sociaux ont fait naître de nouveaux enjeux pour la protection des données. Ces évolutions ont créé le besoin d'« un cadre de protection des données solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles ».

Si le cadre juridique issu de la directive de 1995 demeurait globalement satisfaisant en ce qui concerne ses objectifs et ses principes, ce texte n'a pas permis d'éviter une fragmentation de la mise en œuvre de la protection des données dans l'UE. En pratique, les divergences d'application dans les États membres ont posé de sérieux obstacles aux entreprises exerçant leurs activités au niveau européen.

Il a dès lors été décidé que la réforme serait portée par un règlement, d'application directe dans l'ensemble de l'UE et ne nécessitant pas de transposition dans les Etats membres.

Objectifs et contenu

Si la directive 95/46/CE s'est préoccupée de la protection des libertés et droits fondamentaux des personnes physiques, en particulier de la vie privée, le RGPD va plus loin. Il protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel. Mais dans le nouveau texte, comme dans l'ancien, il s'agit aussi de garantir le bon fonctionnement du marché intérieur, ainsi que de faciliter le libre flux des données. La libre circulation des données à caractère personnel au sein de l'UE n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Ce double objectif apparaît clairement dans son intitulé, ainsi qu'à l'article 1er, § 1 qui précise que le RGPD établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données. Les articles 1er à 4 posent des dispositions générales applicables à tous les traitements, ainsi que des principes directeurs aux articles 5 à 11, tandis qu'à l'inverse, les articles 85 à 91 consacrent des dispositions spécifiques à certains traitements ou données.

2 Champ d’application du RGPD

Le champ d’application territorial de RGPD est beaucoup plus large que celui de la directive de 1995. Le RGPD s’appliquera dès lors qu’un responsable du traitement ou un sous-traitant est établi sur le territoire de l’UE ou qu’un résident européen est directement visé par un traitement de données.

Champ d'application matériel

Traitements de données personnelles visés

Le RGPD s'applique au traitement de données personnelles, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données personnelles contenues ou appelées à figurer dans un fichier. Cette définition reprend mot pour mot celle de la directive 95/46/CE du 24 octobre 1995.

Le RGPD s'applique aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données personnelles. Il ne couvre pas les traitements des données personnelles qui concernent les personnes morales, y compris le nom, la forme juridique et les coordonnées de la personne morale.

Traitements de données personnelles exclus

Sont en revanche exclus les traitements effectués dans le cadre de politiques qui ne relèvent pas de la compétence de l'UE mais de celle des États membres, ainsi que ceux réalisés par des personnes physiques dans le cadre de leur vie privée. Ces deux catégories d'exclusion étaient déjà prévues par la directive 95/46/CE, bien qu'exprimées différemment.

Les services numériques ont portant évolué et les activités personnelles ou domestiques pourraient inclure l'échange de correspondance et la tenue d'un carnet d'adresses, mais aussi l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités. Toutefois, le RGPD s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données personnelles pour de telles activités personnelles ou domestiques. En d'autres termes, les fournisseurs de services de réseaux sociaux, tel Facebook, sont soumis au RGPD.

Champ d'application territorial

Le législateur européen a souhaité protéger le plus amplement possible les données personnelles des Européens. Aussi a-t-il consacré un champ d'application large, au point que l'on peut parler d'extraterritorialité.

Lieu d'établissement du responsable du traitement ou d'un sous-traitant

Tout d'abord, le RGPD s'applique au traitement des données personnelles effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'UE, que le traitement ait lieu ou non dans l'UE. Si le critère du lieu d'établissement du traitement était déjà consacré par la directive 95/46/CE, une première nouveauté tient ici au fait que l'on prend désormais aussi en considération le lieu d'établissement du sous-traitant. En effet, la responsabilité de ce nouvel acteur étant désormais susceptible d'être engagée, il est logique par souci d'efficacité de prendre aussi en considération sa situation géographique pour décider de l'application du RGPD.

Lieu de situation des personnes concernées

Le RGPD prévoit désormais un deuxième critère de rattachement tenant à la situation géographique des personnes concernées par les traitements de données personnelles. Quand ces dernières se situent sur le territoire de l'UE, le RGPD aura vocation à s'appliquer, alors même que le responsable du traitement ou un sous-traitant ne l'est pas, dans deux hypothèses :

- lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'UE, qu'un paiement soit exigé ou non desdites personnes ;
- lorsque de telles activités sont liées au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'UE.

La simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'UE, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention. En revanche, des facteurs tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'UE, peuvent indiquer clairement que le responsable du traitement envisage d'offrir des biens ou des services à des personnes concernées dans l'UE.

Ces critères ont déjà été retenus par la Cour de justice dans les arrêts Pammer et Hôtel Alpenhof (CJUE, 7 déc. 2010, aff. jtes C-585/08 et C-144/09). L'objectif ici est de tenir compte des activités des services numériques pour lesquelles les opérateurs sont souvent situés aux États-Unis et opèrent dans l'UE tout en refusant d'en appliquer les règles. Est pris en compte le fait que le service proposé peut l'être à titre gratuit, ce qui est nécessaire dans la mesure où la gratuité des services est souvent compensée par la collecte des données personnelles ou la publicité, souvent ciblée. En revanche, les contours de la notion de « suivi du comportement » sont difficiles à percevoir, même si elle comprend l'idée de traçabilité et de profilage sous-entendue ici. Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données personnelles qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit.

3 Désignation d’un délégué à la protection des données

Héritier du CIL, le délégué à la protection des données est le véritable « chef d’orchestre de la conformité » au sein des organismes.

Le délégué à la protection des données (ou DPO pour *Data Protection Officer*) est au cœur du dispositif d'*accountability* mis en œuvre par le RGPD. Le responsable du traitement et le sous-traitant doivent veiller à ce que le DPO soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel au sein de l'organisme.

Du CIL au DPO

Si le DPO est le successeur naturel du CIL, des différences majeures peuvent être soulignées. Le RGPD précise les exigences portant sur le DPO s'agissant de ses qualifications (qualités professionnelles, connaissances spécialisées du droit et des pratiques en matière de protection de données) et de sa formation continue (entretien de ses connaissances spécialisées).

En outre, ses prérogatives et missions sont renforcées, en particulier son rôle de conseil et sensibilisation sur les nouvelles obligations du RGPD (ex. : conseil et vérification de l'exécution des analyses d'impact).

Par ailleurs, les organismes doivent fournir à leur DPO les ressources nécessaires à ses missions (notamment l'associer d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données, lui donner accès aux données ou encore lui permettre de se former).

Enfin, contrairement au CIL dont la désignation est facultative, celle du DPO est obligatoire dans certains cas.

Les missions du DPO sont plus larges que celles de CIL, aussi ces derniers ne sont-ils pas automatiquement reconduits en DPO.

Désignation du DPO

Désignation obligatoire du DPO

Les responsables du traitement, comme les sous-traitants, doivent obligatoirement désigner un DPO dans trois cas :

- lorsque le traitement est effectué par une autorité publique (ou un organisme public), à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle. Si le législateur doit préciser cette notion, nous pouvons d'ores et déjà considérer que doivent notamment nommer un DPO les personnes morales de droit public comme l'État, les collectivités territoriales (communes, départements, régions), ainsi que les établissements publics (hôpitaux, universités…) ;
- lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement exigeant un suivi régulier et systématique à grande échelle des personnes concernées ;
- lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de données ou de données personnelles relatives à des condamnations pénales et à des infractions.

Désignation facultative mais recommandée du DPO

En dehors des cas de désignation obligatoire, la désignation d'un DPO est logiquement facultative, mais fortement encouragée car elle permet de confier à un expert l'identification et la coordination des actions à mener en matière de protection des données personnelles.

Lorsqu'un organisme désigne un DPO volontairement, les conditions prévues par le RGPD s'appliqueront à sa désignation, à son poste et à ses missions, comme si la désignation était obligatoire.

DPO mutualisé

Le RGPD donne la possibilité de mutualiser un DPO au sein d'un groupe d'entreprises à condition qu'il soit facilement joignable à partir de chaque lieu d'établissement.

DPO interne ou externe

Le DPO peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

Compétences du DPO

Le DPO est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées par le RGPD.

Le niveau de connaissances spécialisées requis devrait être déterminé en fonction des opérations de traitement des données effectuées et de la protection exigée pour les données personnelles en cours de traitement.

Le DPO doit avoir une expertise dans les lois et pratiques nationales et européennes en matière de protection des données, ainsi qu'une compréhension approfondie du RGPD. Cette expertise s'ajoute à la connaissance du secteur des entreprises et de l'organisme du responsable du traitement ou encore des règles administratives et procédures si le responsable est une autorité ou un organisme public.

Missions du DPO

Les missions du DPO sont, *a minima*, les suivantes :

- informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du RGPD et d'autres dispositions du droit de l'UE ou du droit des États membres en matière de protection des données ;
- contrôler le respect du RGPD, d'autres dispositions du droit de l'UE ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données, y compris en ce qui concerne la répartition des

responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

- dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci ;
- coopérer avec l'autorité de contrôle ;
- faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement et mener des consultations, le cas échéant, sur tout autre sujet.

En outre, le DPO est au cœur du dispositif de l'analyse de risque puisqu'il lui est demandé de tenir compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Comment le DPO exerce-t-il ses fonctions ?

Le responsable du traitement et le sous-traitant doivent aider le DPO à exercer ses missions. Cette obligation implique de lui fournir les ressources nécessaires pour exercer ces missions, de lui donner l'accès aux données personnelles et aux opérations de traitement et enfin, de lui permettre d'entretenir ses connaissances spécialisées, ce qui implique une obligation de le former.

Le responsable du traitement et le sous-traitant doivent veiller à ce que le DPO ne reçoive aucune instruction en ce qui concerne l'exercice des missions. En outre, le DPO ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions.

Enfin, le DPO fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant, si bien que si le responsable du traitement ou le sous-traitant prennent des décisions incompatibles avec le RGPD et les conseils du DPO, ce dernier doit avoir la possibilité de rendre une opinion dissidente directement au niveau le plus élevé de la direction.

Par ailleurs, si le DPO peut exécuter d'autres missions et tâches, le responsable du traitement ou le sous-traitant doivent veiller à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts. Sont ainsi exclus des postes de cadres supérieurs ou de direction (comme le directeur général, le directeur d'exploitation, le directeur financier, le directeur médical, le directeur du département marketing, le DRH, le DSI), mais aussi des rôles moins importants dans la structure organisationnelle si ces postes ou rôles conduisent à la détermination des objectifs et moyens de traitements de données personnelles

Responsabilité du DPO

Le DPO n'est pas personnellement responsable en cas de violation des dispositions du RGPD. Ce dernier prévoit la responsabilité du responsable du traitement et celle du sous-traitant. Mais la désignation d'un DPO n'a pas pour effet de lui transférer cette responsabilité.

4 Registre des activités de traitement

Dans le cadre de sa démarche de mise en conformité avec le RGPD, l'organisme doit faire l'inventaire des traitements de données personnelles qu'il met en œuvre. Cet inventaire se matérialise sous la forme d'un registre.

Le registre des activités de traitement est tenu par le responsable du traitement mais le sous-traitant en tient un aussi. Il est un des principaux outils permettant aux organismes de prouver le respect des obligations imposées par le RGPD, ce qui implique qu'il soit mis à la disposition de la CNIL.

Organisation de plus de 250 employés

Tout organisme a l'obligation de tenir un registre de ses activités de traitements dès lors que son organisation compte plus de 250 employés.

Organisation de moins de 250 employés

La tenue du registre n'est pas obligatoire pour les entreprises ou organisations comptant moins de 250 employés, sauf dans trois cas :

- le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées ;
- le traitement n'est pas occasionnel ;
- le traitement porte sur certaines catégories de données (données sensibles ou données relatives à des condamnations pénales et à des infractions).

Ainsi, il y a de fortes chances que les entreprises concernées tombent dans l'un de ces cas, en particulier le deuxième.

Contenu du registre

Le RGPD précise la forme du registre (écrite y compris électronique) ainsi que son contenu :

- nom et coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du DPO ;
- les finalités du traitement ;
- une description des catégories de personnes concernées et données personnelles ;
- les catégories de destinataires auxquels les données personnelles ont été ou seront communiquées ;
- les transferts de données personnelles vers un pays tiers ;
- dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données :
- une description générale des mesures de sécurité techniques et organisationnelles.

S'agissant du registre tenu par le sous-traitant, les mêmes informations doivent être fournies, à l'exception notable de l'indication des délais prévus pour l'effacement des différentes catégories de données, puisque la politique d'effacement est décidée par le responsable du traitement. S'agissant des coordonnées à indiquer, outre celles du ou des sous-traitants, il faut ajouter celles de chaque responsable du traitement pour le compte duquel le sous-traitant agit, ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du DPO.

5 Violation de données personnelles

Le RGPD généralise l'obligation de notifier la violation de données à la CNIL et impose, dans certains cas, d'informer les personnes concernées.

La violation de données personnelles est définie comme toute violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données personnelles faisant l'objet d'un traitement.

Elle peut être, d'une part, accidentelle, telle que la divulgation par erreur par un salarié de données clients ou, d'autre part, illicite ou malveillante, tel qu'un piratage informatique.

Le responsable du traitement doit documenter toute violation de données personnelles en indiquant les faits concernant la violation, ses effets et les mesures prises pour y remédier

Notification d'une violation de données à la CNIL

Le responsable du traitement doit informer la CNIL de toute violation de données personnelles. Une nouvelle téléprocédure de notification sera mise en ligne en mai 2018.

Le responsable du traitement a l'obligation de notifier la violation de données dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance.

La notification peut s'effectuer de manière échelonnée dans la limite de 72 heures. Au-delà des 72 heures, le responsable du traitement doit justifier son retard.

Le RGPD impose au sous-traitant de notifier au responsable du traitement toute violation de données personnelles dans les meilleurs délais après en avoir pris connaissance.

Information des personnes concernées

Lorsqu'une violation de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement doit communiquer la violation de données personnelles à la personne concernée dans les meilleurs délais.

Toutefois, le RGPD prévoit trois hypothèses dans lesquelles la communication à la personne concernée n'est pas nécessaire :

- le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées, en particulier les mesures qui rendent les données personnelles incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;
- le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser ;
- elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

6 Réalisation d'analyses d'impact relatives à la protection des données

L'analyse d'impact est une mesure phare du RGPD et doit être prise très au sérieux par le responsable du traitement. S'il est difficile de savoir a priori si une telle analyse doit être menée, avant de connaître précisément les risques, sans doute faut-il considérer prudemment que le simple doute sur la pertinence d'une analyse d'impact doit conduire à en mener une.

Le RGPD est fondé sur une logique de rendre compte auprès de la CNIL, en particulier par le calcul des risques, réalisé par le responsable du traitement.

L'étude des risques conditionne ainsi les mesures techniques et organisationnelles que ce dernier va décider de prendre. Il en est particulièrement ainsi lorsqu'il doit prendre la décision de réaliser ou non une analyse d'impact relative à la protection des données (AIPD, en anglais *Data protection impact assessment* ou DPIA, l'expression *Privacy impact assessment* ou PIA étant utilisée avant le RGPD).

Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données personnelles.

Une seule et même analyse peut porter sur un ensemble d'opérations de traitement identiques qui présentent des risques élevés similaires.

Cette analyse d'impact doit prendre en compte la nature, la portée, le contexte et les finalités du traitement et exige que le responsable du traitement prenne conseil auprès du DPO.

L'analyse d'impact est cependant obligatoire dans trois hypothèses :

- en cas d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- le traitement à grande échelle de données sensibles ou de données relatives à des condamnations pénales et à des infractions ;
- la surveillance systématique à grande échelle d'une zone accessible au public.

En outre, la CNIL établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact est également requise, de même qu'elle peut, à l'inverse, établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact n'est nécessaire.

L'analyse d'impact doit au moins contenir :

- une description des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques pour les droits et libertés des personnes concernées ;
- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité.

Le respect, par les responsables du traitement ou sous-traitants concernés, de codes de conduite approuvés est dûment pris en compte lors de l'évaluation de l'impact des

opérations de traitement effectuées.

Si l'analyse d'impact révèle l'existence d'un risque élevé, le responsable du traitement doit consulter la CNIL.

Lorsque cette dernière est d'avis que le traitement envisagé constituerait une violation du RGPD, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, la CNIL fournit par écrit, dans un délai maximum de 8 semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant, sous réserve des possibilités d'extension prévues.

La consultation de la CNIL implique de lui communiquer notamment l'analyse d'impact elle-même.

7 Droit à l'oubli

Le RGPD consacre le droit pour une personne de demander l'effacement de ses données personnelles auprès du responsable du traitement sous réserve de respecter certaines conditions.

La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données personnelles la concernant.

Le responsable du traitement doit effacer ces données personnelles dans les meilleurs délais. Toutefois, ce droit n'est pas général, mais a vocation à ne s'appliquer que pour des motifs limitativement énumérés, ce qui en limite fortement la portée.

Il s'applique lorsque :

- les données personnelles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
- la personne concernée retire le consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique au traitement ;
- la personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement ;
- les données personnelles ont fait l'objet d'un traitement illicite ;
- les données personnelles doivent être effacées pour respecter une obligation légale prévue par le droit de l'UE ou par le droit de l'État membre auquel le responsable du traitement est soumis ;
- les données personnelles ont été collectées dans le cadre de l'offre de services de la société de l'information.

Toutes les hypothèses visées supposent que le traitement en cause ne soit pas ou plus conforme au RGPD, ce qui était la formulation générale de la directive 95/46/CE du 24 octobre 1995.

Si on peut se réjouir des précisions apportées et d'une formulation plus affirmée, on constate également que, sur le fond, aucun droit n'est finalement accordé. Au demeurant, la formulation générale de la directive avait pour mérite d'englober tout type de violation, alors que l'énumération précise du RGPD perd cette souplesse au profit de la précision.

Cependant la portée de ce droit à l'oubli est limitée. Lorsqu'il a rendu publiques les données personnelles et qu'il est tenu de les effacer, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, doit prendre des mesures raisonnables, y compris d'ordre technique, pour informer les tiers qui traitent ces données que la personne concernée a demandé l'effacement.

Les mesures prises pour informer les tiers trouvent donc leur limite, compte tenu du coût et de la difficulté, ce que prévoyait aussi la directive 95/46/CE, en cas d'impossibilité ou d'effort disproportionné. De ce point de vue, la logique des deux textes est identique.

Par ailleurs, des dérogations au droit à l'oubli sont prévues dans la mesure où le traitement est nécessaire :

- à l'exercice du droit à la liberté d'expression et d'information ;
- pour respecter une obligation légale qui requiert le traitement prévu par le droit de l'UE ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

- pour des motifs d’intérêt public dans le domaine de la santé publique ;
- à des fins archivistiques dans l’intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ;
- à la constatation, à l’exercice ou à la défense de droits en justice. Ces dispositions viennent donc encore restreindre la portée du droit à l’oubli.

8 Droit à la portabilité des données personnelles

Le RGPD introduit le nouveau droit à la portabilité qui permet aux personnes de recevoir les données personnelles les concernant et de les transmettre à un autre responsable du traitement. Ce droit vise à accroître la concurrence et à diminuer les coûts.

Le RGPD a créé un droit à la portabilité des données. Désormais, les personnes concernées ont le droit de recevoir les données personnelles les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine.

Elles ont aussi le droit de transmettre ces données à un autre responsable du traitement, sans que le responsable du traitement auquel les données personnelles ont été communiquées y fasse obstacle.

Il y a alors transmission des données, lorsque :

- le traitement est fondé sur le consentement ou sur un contrat ;
- le traitement est effectué à l'aide de procédés automatisés.

Lorsque la personne concernée exerce son droit à la portabilité des données, elle a le droit d'obtenir que les données soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.

Par ailleurs, l'exercice du droit à la portabilité s'entend sans préjudice du droit à l'effacement des données.

Ce droit ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Ce droit ne doit pas porter atteinte aux droits et libertés de tiers.

Ce droit à la portabilité des données est à mettre en lien avec les objectifs du droit de la consommation et de la concurrence. La portabilité des données facilite le changement d'opérateur et de service, ce qui stimule la concurrence.

De ce fait, on espère une baisse des prix au profit des consommateurs. En effet, certaines pratiques courantes des acteurs dominants de l'économie numérique peuvent non seulement porter atteinte à la protection des données personnelles, mais aussi au droit de la concurrence (v. Rapp. Autorité conc., Droit de la concurrence et données, 10 mai 2016).

9 Transferts de données hors Union européenne

Le RGPD renforce les exigences en matière de transferts de données vers les pays tiers. Ainsi, il reprend les outils de transferts déjà existants, notamment les règles d'entreprise contraignantes (binding corporate rules ou BCR) ou encore les clauses contractuelles types, tout en affirmant le principe de l'interdiction des transferts vers des pays tiers.

Un transfert, vers un pays tiers ou à une organisation internationale, de données personnelles qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si les conditions définies dans le RGPD sont respectées par le responsable du traitement et le sous-traitant.

Transferts fondés sur une décision d'adéquation de la Commission européenne

Un transfert de données personnelles vers un pays tiers ou à une organisation internationale peut avoir lieu, lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question, assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.

L'acte d'exécution par lequel la Commission décide d'un niveau de protection adéquat prévoit un mécanisme d'examen périodique, au moins tous les 4 ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale. L'acte d'exécution précise son champ d'application territorial et sectoriel.

La Commission publie au *Journal officiel de l'Union européenne* et sur son site internet une liste des pays tiers, des territoires et des secteurs déterminés dans un pays tiers et des organisations internationales pour lesquels elle a constaté par voie de décision qu'un niveau de protection adéquat est ou n'est plus assuré.

Transferts moyennant des garanties appropriées

Dès lors que le pays destinataire des données ne bénéficie pas d'une décision d'adéquation, le responsable du traitement ou le sous-traitant ne peut transférer des données personnelles vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.

Garanties appropriées sans autorisation de la CNIL

De telles garanties peuvent être fournies, sans que cela ne nécessite une autorisation particulière de la CNIL, par : un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics ; des règles d'entreprise contraignantes ; des clauses types de protection des données adoptées par la Commission ; des clauses types de protection des données adoptées par la CNIL et approuvées par la Commission ; un code de conduite approuvé ou un mécanisme de certification approuvé, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

Règles d'entreprises contraignantes

Si les règles d'entreprise contraignantes n'ont pas besoin d'être autorisées par la

CNIL, cette dernière peut tout de même les approuver, à condition que :

- ces règles soient juridiquement contraignantes et soient mises en application par toutes les entités concernées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe, y compris leurs employés ;
- elles confèrent expressément aux personnes concernées des droits opposables en ce qui concerne le traitement de leurs données personnelles.

Ces règles doivent, en outre, préciser un certain nombre d'informations, comme les transferts ou l'ensemble des transferts de données, y compris les catégories de données personnelles, le type de traitement et ses finalités, le type de personnes concernées affectées et le nom du ou des pays tiers en question ; l'application des principes généraux relatifs à la protection des données (notamment la limitation de la finalité, la minimisation des données, la limitation des durées de conservation des données, la qualité des données, la protection des données dès la conception et la protection des données par défaut, la base juridique du traitement, le traitement de catégories particulières de données personnelles, les mesures visant à garantir la sécurité des données), ainsi que les droits des personnes concernées par le traitement.

Garanties appropriées avec autorisation de la CNIL

En outre, sous réserve de l'autorisation de la CNIL, les garanties appropriées peuvent aussi être fournies :

- soit par des clauses contractuelles entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données personnelles dans le pays tiers ou l'organisation internationale ;
- soit par des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées.

Ces mécanismes de protection, destinés à conférer des garanties appropriées, existaient en pratique et ont été consacrés par le RGPD.

Dérogations pour des situations particulières

En l'absence de décision d'adéquation ou de garanties appropriées, un transfert ou un ensemble de transferts de données personnelles vers un pays tiers ou à une organisation internationale peut tout de même avoir lieu dans les cas suivants :

- la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées ;
- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ;
- 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 physique ou morale ;

- le transfert est nécessaire pour des motifs importants d'intérêt public ; le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;
- le transfert est nécessaire à la sauvegarde des 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 ;
- le transfert a lieu au départ d'un registre qui est destiné à fournir des informations au public, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'UE ou le droit de l'État membre sont remplies.

Les dérogations ainsi prévues ont naturellement pour effet de vider de leur substance les mécanismes de protection précédemment énoncés. En particulier, les dérogations fondées sur le consentement de la personne concernée ou sur la conclusion d'un contrat sont particulièrement discutables car, outre le fait que l'on peut douter de la pleine compréhension par la personne concernée des risques encourus, la volonté de conclure un contrat, en vue de bénéficier des services proposés par les entreprises de l'économie numérique, risque d'être plus forte que la prudence que l'on pourrait attendre des personnes. Autrement dit, ces dernières ne sont pas nécessairement en mesure d'assurer leur propre protection.

Transfert non répétitif, limité et impérieux

Par ailleurs, même si le transfert ne peut être fondé sur une décision d'adéquation ou des garanties appropriées, telles que précédemment évoquées, et même si le transfert ne bénéficie d'aucun cas de dérogation tel qu'énoncé, un transfert vers un pays tiers ou à une organisation internationale peut néanmoins avoir lieu si ce transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée. Le responsable du traitement doit en outre avoir évalué toutes les circonstances entourant le transfert de données et offrir des garanties appropriées en ce qui concerne la protection des données personnelles. Le responsable du traitement doit informer la CNIL du transfert et la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit.

Remarque : les dérogations sont finalement considérables et corroborées par ce cas qui paraît très spécifique mais qui concerne les transferts isolés de données, susceptibles d'être particulièrement nombreux. On peut aussi douter de la bonne compréhension des enjeux par la personne concernée qui serait ainsi informée du transfert.

10 Amendes administratives et sanctions

La violation des dispositions du RGPD fait l'objet d'amendes administratives pouvant s'élever jusqu'à 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent

Amendes administratives

La CNIL veille à ce que les amendes administratives imposées pour des violations du RGPD soient, dans chaque cas, effectives, proportionnées et dissuasives.

Pour juger qu'il y a lieu d'imposer une amende administrative et pour décider de son montant, elle doit notamment tenir compte de la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi.

Si un responsable du traitement ou un sous-traitant viole délibérément ou par négligence plusieurs dispositions du RGPD, dans le cadre de la même opération de traitement ou d'opérations de traitement liées, le montant total de l'amende administrative ne peut pas excéder le montant fixé pour la violation la plus grave.

Font l'objet d'amendes administratives pouvant s'élever jusqu'à 10 000 000 € ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu, en cas de violation des dispositions suivantes :

- les obligations incombant au responsable du traitement et au sous-traitant en vertu des articles suivants du RGPD : 8 (conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information), 11 (traitement ne nécessitant pas l'identification), 25 à 39 (obligations générales, sécurité des données, analyse d'impact et DPO), 42 et 43 (certification) ;
- les obligations incombant à l'organisme de certification ;
- les obligations incombant à l'organisme chargé du suivi des codes de conduite.

Les violations des dispositions suivantes font l'objet d'amendes administratives pouvant s'élever jusqu'à 20 000 000 € ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu :

- les principes de base d'un traitement, y compris les conditions applicables au consentement ;
- les droits dont bénéficient les personnes concernées ;
- les transferts de données personnelles à un destinataire situé dans un pays tiers ou à une organisation internationale ;
- toutes les obligations découlant du droit des États membres adoptées en vertu du chapitre IX du RGPD (dispositions relatives à des dispositions particulières de traitement) ;
- le non-respect d'une injonction, d'une limitation temporaire ou définitive du traitement ou de la suspension des flux de données ordonnée par la CNIL ou le fait de ne pas accorder l'accès au traitement prévu.

Le non-respect d'une injonction émise par la CNIL fait l'objet d'amendes administratives pouvant s'élever jusqu'à 20 000 000 € ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Chaque État membre peut établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire.

L'exercice, par la CNIL, des pouvoirs de sanction administrative est soumis à des garanties procédurales appropriées, conformément au droit de l'UE et au droit des États membres, y compris un recours juridictionnel effectif et une procédure régulière.

Si le système juridique d'un État membre ne prévoit pas d'amendes administratives, le RGPD peut être appliqué, de telle sorte que l'amende est déterminée par la CNIL et imposée par les juridictions nationales compétentes, tout en veillant à ce que ces voies de droit soient effectives et aient un effet équivalent aux amendes administratives imposées par les autorités de contrôle.

En tout état de cause, les amendes imposées sont effectives, proportionnées et dissuasives.

Sanctions

Les États membres déterminent le régime des autres sanctions applicables en cas de violations du RGPD, en particulier pour les violations qui ne font pas l'objet des amendes administratives, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre.

Ces sanctions sont effectives, proportionnées et dissuasives.

Chaque État membre notifie à la Commission européenne les dispositions légales qu'il adopte au plus tard le 25 mai 2018 et, sans tarder, toute modification ultérieure les concernant.

NOUVEAU

PROTECTION DES DONNÉES PERSONNELLES

Se mettre en conformité d'ici le 25 mai 2018

Découvrez l'ouvrage « Protection des données personnelles », indispensable à la mise en place du nouveau dispositif.

Rédigé par des experts et praticiens reconnus de la protection des données personnelles.

Un mode d'emploi pour se mettre en conformité avec le RGPD.

Des modèles de nouvelles clauses et documents opérationnels.

Pour toute commande rendez-vous sur **www.editions-legislatives.fr**
ou contactez-nous au **01 40 92 36 36**

EDITIONS LEGISLATIVES