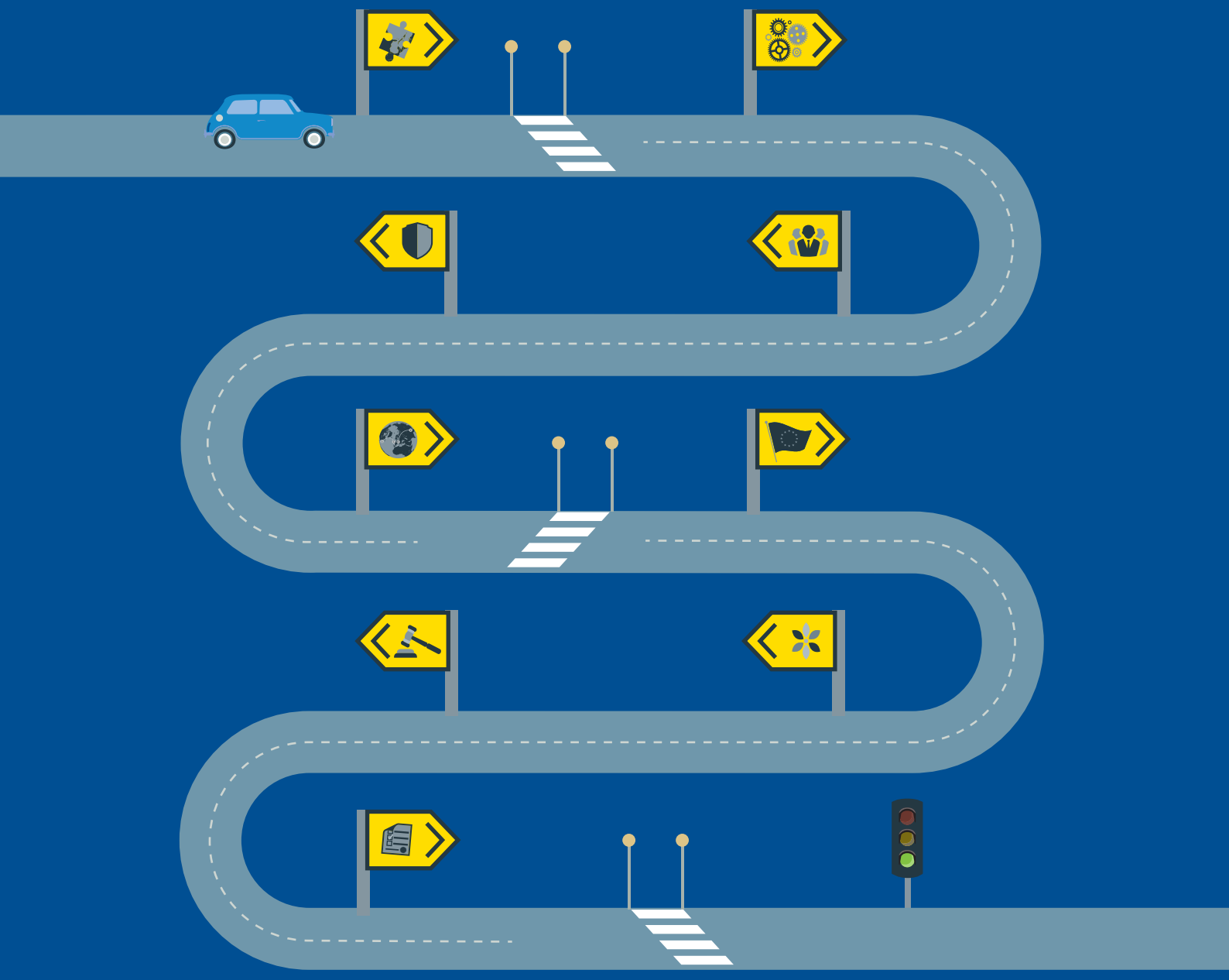
Bird & Bird &

Guide sur le Règlement Européen relatif à la protection des données personnelles

Avril 2017



Le nouveau Règlement Général sur la Protection des Données Personnelles (RGPD, ou en anglais GDPR) a finalement été publié au Journal Officiel de l'Union Européenne le 4 mai 2016, et entrera en application le 25 mai 2018. Il fait suite à quatre années de débats, de négociations et de lobbying, d'une ampleur que l'Union européenne (UE) n'avait jamais connue auparavant.

Ce guide fournit une synthèse du Règlement ayant résulté de ce processus, un texte qui va considérablement refondre la législation fondamentale de l'Europe en matière de protection des données personnelles, à l'heure où les systèmes d'information et le numérique conditionnent désormais la vie quotidienne des personnes.

Les changements qui devront être mis en œuvre, en application du GDPR en mai 2018, s'avèrent substantiels et ambitieux. Le GDPR constitue l'une des plus vastes législations que l'UE ait adoptées ces dernières années, et un certain nombre de concepts à mettre en œuvre, tels que le terme "droit à l'oubli numérique", la portabilité des données, la notification des violations de données, et la responsabilité dite "accountability" (pour n'en citer que quelques-uns) nécessiteront un certain temps d'adaptation. La nature juridique même de ce texte- un règlement plutôt qu'une directive - fait du GDPR un type de législation que les juristes n'ont pas pour habitude d'analyser.

Ce guide vise à synthétiser les principaux changements induits par le nouveau texte, et à souligner les mesures les plus importantes que les organisations devront prendre afin de se préparer à se conformer au texte.

Nous présentons notre synthèse en différents chapitres, qui correspondent globalement à la structure du Règlement, à ceci près que chacun de ces chapitres est sous-divisé en différents thèmes. Chaque sous-chapitre débute par un résumé synthétique rapide, une liste des mesures prioritaires que nous suggérons, ainsi que notre estimation du degré de changement qu'apportera chaque section du GDPR analysée (sous forme d'un cadrant visuel en couleurs

(depuis le vert pour un changement minime jusqu'au rouge pour un changement important). Nous avons également intégré à chaque chapitre un panneau indiquant le ou les articles du GDPR au sein duquel/desquels vous pourrez trouver les informations pertinentes.

La législation européenne sur la protection des données a toujours été rédigée selon une terminologie quelque peu spécifique, et le GDPR ne fait pas exception. Afin de vous aider à intégrer ce nouveau langage, ce guide inclut un glossaire terminologique.

Le GDPR a finalement été adopté le 27 avril 2016 (veuillez-vous reporter au Glossaire pour plus d'informations sur le nom complet). Cette version du Guide inclut les lignes directrices publiées par le Groupe de travail de l'article 29 (G29) en décembre 2016.

À mesure que de nouvelles orientations relatives au GDPR et dispositions relatives à son application émaneront des législateurs, des régulateurs et des tribunaux, nous publierons des mises à jour ainsi que nos propres recommandations. Si vous souhaitez obtenir davantage de renseignements, n'hésitez pas à nous solliciter. Dans cet intervalle, nous espérons que ce guide vous sera utile.

Ruth Boardman
Associée, UK

James Mullock
Associée, UK

Ariane Mole
Associée, FR

Table des matières

Champ d'application matériel et territorial

En bref

- En comparaison à la Directive 95/46/CE (la *"Directive sur la protection des données personnelles"*) qu'il vient remplacer, le GDPR vise à étendre la portée du champ d'application de la législation de l'UE concernant la protection des données.
  - Les responsables du traitement et les sous-traitants basés dans l'UE tombent dans son champ d'application dès lors que des données à caractère personnel sont traitées *"dans le cadre de leurs activités"*, ce qui peut être interprété largement.
  - Lorsqu'il n'y pas de présence dans l'UE, le GDPR s'appliquera dès lors que : (1) les données à caractère personnel d'un résident de l'UE sont traitées en lien avec les biens/services qui lui sont proposés ; ou dès lors que (2) les comportements d'individus au sein de l'UE sont *"suivis"*.
- Malgré sa qualité de Règlement, le texte permet aux États membres de légiférer dans de nombreux domaines. Il faut s'attendre à ce que cette possibilité présente un défi quant à l'application de l'objectif de cohérence énoncé par le Règlement, notamment concernant le traitement des données des employés.
- Le GDPR ne s'applique pas à certaines activités, parmi lesquelles les traitements couverts par la Directive relative à la protection des données personnelles traitées à des fins répressives ayant pour finalité la sécurité nationale, ainsi que les traitements effectués par les personnes physiques dans le cadre d'activités exclusivement personnelles/domestiques.
- Le GDPR prendra effet le 25 mai 2018.

A faire

☐ Les organisations non présentes dans l'UE mais qui ciblent ou suivent des personnes dans l'UE ont tout intérêt à:

- comprendre l'impact du GDPR ; et à
- déterminer les mesures à mettre en œuvre leur permettant de se conformer au GDPR.

☐ Les organisations opérant dans des domaines au sein desquels *des règles "particulières" / sectorielles* sont couramment appliquées ont tout intérêt à:

- évaluer la nécessité de législations nationales spécifiques, et les promouvoir si nécessaire ; et à
- se tenir au fait de la promulgation de telles lois susceptibles de leur être défavorables

Champ d'application territorial

Responsables du traitement et sous-traitants "établis" dans l'UE

Le GDPR s'appliquera aux organisations disposant d' *"établissements"* dans l'UE, dès lors que des données à caractère personnel sont traitées *"dans le cadre des activités"* de tels établissements.

Si cette condition est remplie, le GDPR s'appliquera indépendamment du fait que le traitement des données ait effectivement lieu ou non dans l'UE.

La notion d' *"établissement"* a été éclaircie par la Cour de justice de l'Union européenne ("CJUE") dans l'affaire de 2015 Weltimmo c. NAIH (C-230/14). La Cour a confirmé que la notion d'établissement était une notion *"large"* et *"souple"*, qui ne devait pas dépendre de la forme juridique de *l'établissement*. Une organisation peut être considérée comme *"établie"* dès lors qu'elle exerce *"toute activité réelle et effective – même minime"* – au moyen d' *"une installation stable"* sur le territoire de l'UE. La présence d'un seul représentant peut être suffisante. Dans cette affaire, Weltimmo a été considérée comme établie en Hongrie, dans la mesure où cette société utilisait un site Internet hongrois faisant la promotion de biens immobiliers hongrois (la société ayant par conséquent été considérée comme *"principalement voire entièrement tournée vers ledit État membre"*), recourait à un agent local (qui était responsable de la collecte des paiements locaux, et agissait en tant que représentant dans le cadre des procédures administratives et judiciaires), et utilisait une adresse postale et un compte bancaire hongrois à des fins commerciales indépendamment du fait que Weltimmo ait été constituée en Slovaquie.

Les organisations qui disposent de bureaux de vente dans l'UE, qui promeuvent ou vendent de la publicité ou du marketing ciblant des résidents de l'UE seront susceptibles d'être soumises au GDPR – dans la mesure où le traitement de données à caractère personnel associé est considéré comme *"inextricablement lié"* au, et par conséquent effectué dans, *"le cadre des activités de"* ces établissements établis dans l'UE (Google Spain SL, Google Inc. c. AEPD, Mario Costeja González (C-131/12)).

Organisations non "établies" dans l'UE et ciblant ou effectuant un suivi des personnes concernées dans l'UE

Les organisations non établies dans l'UE seront soumises au GDPR dès lors qu'elles traiteront des données à caractère personnel relatives à des personnes concernées basées dans l'UE dans le cadre:

- d'une *"offre de biens ou services"* (sans qu'il y ait nécessairement lieu à paiement) ; ou
- d'un *"suivi"* de leur comportement à l'intérieur de l'UE.

Concernant l'offre de biens et de services (mais pas le suivi), une simple accessibilité à un site à partir de l'UE n'est pas suffisante. Il doit apparaître que l'organisation *"envisage"* que des activités cibleront des personnes concernées à l'intérieur de l'UE.

L'existence d'adresses de contact accessibles depuis l'UE, et le recours à une langue utilisée dans le propre pays du responsable du traitement ne sont pas non plus suffisants. Toutefois, l'utilisation d'une langue/monnaie de l'UE, la capacité à passer des commandes dans cette autre langue, ainsi que le fait de faire référence à des utilisateurs ou clients dans l'UE entreront en considération.

La CJUE s'est penchée sur la question de savoir dans quels cas une activité (telle que l'offre de biens et services) pouvait être considérée comme *"tournée vers"* des États membres de l'UE dans un contexte distinct (c.-à-d. en vertu du Règlement *"Bruxelles I"* (44/2001/CE) régissant la *"compétence des tribunaux... en matière civile et commerciale"*). Ses commentaires sont susceptibles de faciliter l'interprétation des dispositions équivalentes du GDPR. Outre les considérations énoncées ci-dessus, la CJUE explique qu'une intention de cibler des clients dans l'UE peut être illustrée par : (1) une preuve *"manifeste"*, telle que le paiement de sommes d'argent auprès d'un moteur de recherche dans le but de faciliter l'accès de ceux situés au sein d'un État membre, ou lorsque les États membres ciblés sont nommément désignés ; et (2) d'autres facteurs – susceptibles d'être combinés les uns aux autres – parmi lesquels la *"nature internationale"* de l'activité en question (ex : certaines activités de tourisme), le fait de mentionner des numéros de téléphone présentant un code international, l'utilisation d'un nom de domaine de premier niveau autre que celui de l'État dans lequel l'entité commerciale est établie (ex : .de ou .eu), la description d' *"itinéraires... depuis les États membres vers le lieu où le service est fourni"*, ainsi que le fait de mentionner une *"clientèle internationale composée de clients domiciliés dans différents États membres"*. Cette liste est *"non exhaustive"*, et la question doit être tranchée au cas par cas (Pammer c. Reederei Karl Schlüter GmbH & Co, et Hotel Alpenhof c. Heller (Affaires jointes (C-585/08) et (C-144/09)).

La question de savoir si les entreprises non basées dans l'UE offrant des biens et des services à des entreprises basées dans l'UE (et non des individus) tomberont dans le champ d'application de l'article 3(2)(a), concernant la nécessaire condition relative à la *"fourniture de biens et de services"*, n'est pas claire.

Le terme de *"suivi"* désigne spécifiquement le fait de procéder à un suivi de personnes en ligne afin de créer des profils, y compris lorsque cette démarche se destine à une prise de décisions consistant à analyser/prédire les préférences, comportements et attitudes des personnes.

Les organisations soumises au GDPR doivent désigner un représentant basé dans l'UE.

En vertu de la Directive sur la protection des données, les organisations ciblant des personnes dans l'UE sont seulement tenues de se conformer aux règles de l'UE si elles utilisent également des *"moyens de traitement"* au sein de l'UE pour procéder au traitement de données à caractère personnel. Ceci a conduit les autorités de contrôle, désireuses d'affirmer leur compétence juridictionnelle, à élaborer des arguments selon lesquels le fait de placer des témoins de connexion (cookies) ou de demander aux utilisateurs de remplir des formulaires, revenait à utiliser des *"moyens"* au sein de l'UE. Il sera désormais plus facile de déterminer les cas dans lesquels la législation de l'UE s'appliquera. (Néanmoins, dès lors que des organisations n'ont pas une présence au sein de l'UE, il faut s'attendre à ce que l'application des règles se révèle aussi difficile qu'auparavant).

Cas dans lesquels la législation des États membres de l'UE s'applique en vertu du droit international public

Le considérant 25 énonce l'exemple d'une mission diplomatique ou d'un poste consulaire.

Exclusions

Certaines activités (énoncées ci-dessous) sont intégralement exclues du champ d'application du GDPR.

En outre, le GDPR reconnaît que les droits relatifs à la protection des données ne revêtent pas de caractère absolu, et doivent être mis en balance (de manière proportionnelle) avec d'autres droits fondamentaux – parmi lesquels la *"liberté d'entreprise"*. (Concernant la capacité des États membres à introduire des exemptions, veuillez-vous reporter à la section relative aux dérogations et conditions spécifiques). Dans la mesure où le GDPR renforce la rigueur des dispositions dans de nombreux domaines de la protection des données, en usant davantage de répression que d'incitation réglementaire, il peut être utile pour les entreprises de prendre particulièrement note du considérant (4), en cas de besoin à l'avenir.

Le GDPR ne s'applique pas au traitement de données à caractère personnel lorsque ce traitement est effectué (ces exemptions générales sont très similaires aux dispositions équivalentes figurant dans la Directive sur la protection des données):

- dans le cadre d'activités excluent du champ d'application du droit de l'UE (ex: activités relatives à la sécurité nationale) ;
- dans le cadre de la politique étrangère et de sécurité commune de l'UE ;
- par des autorités compétentes à des fins de prévention, d'enquête, de détection ou de poursuite d'infractions ainsi qu'à des fins s'y rattachant (c.-à-d. dès lors que la Directive relative à la protection des données personnelles traitées à des fins répressives, qui a été adoptée le 26 avril 2016 sous la référence 2016/618, s'applique) ;
- par des institutions de l'UE, lorsque le Règlement 45/2001/CE continue de s'appliquer en lieu et place du GDPR. Ce Règlement sera mis à jour afin de garantir une cohérence par rapport au GDPR.
- par une personne physique dans le cadre d'une activité *"exclusivement personnelle ou domestique"*. Ceci englobe les correspondances ainsi que la tenue de registres d'adresses, et désormais les activités effectuées sur Internet et sur les réseaux sociaux à des fins sociales et domestiques. Ceci représente un possible élargissement de l'exemption résultant des principes énoncés dans l'arrêt Bodil Lindqvist (C-101/01), avant l'avènement des médias sociaux. Dans cette affaire, la CJUE avait considéré que le partage de données sur Internet consistant à rendre ces données *"accessibles à un nombre indéfini de personnes"* ne pouvait rentrer dans le champ d'application de cette exemption, dont la Cour précise qu'elle doit rester limitée à des activités *"qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers"*. Il convient également de noter que le GDPR sera applicable aux responsables du traitement et sous-traitants qui *"fournissent les moyens d'un traitement"* relevant du champ d'application de cette exemption.

Il est énoncé que le GDPR s'applique *"sans préjudice"* des règles figurant dans la Directive relative au commerce électronique (2000/31/CE), et notamment des règles concernant la responsabilité des *"prestataires de services intermédiaires"* (qui visent à limiter leur risque de s'exposer à une responsabilité pécuniaire et pénale lorsque ces prestataires ne font qu'héberger des données, procéder à leur mise en cache, ou effectuer une *"simple transmission"*). La relation à la Directive sur le commerce électronique n'est pas claire, dans la mesure où celle-ci énonce que les problématiques relatives au traitement de données à caractère personnel sont exclues de son champ d'application, et *"exclusivement régies"* par la législation applicable en

[1] Full title: Directive *"on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data."*

matière de protection des données. Les deux textes peuvent sembler cohérent si l'on considère que la responsabilité des prestataires de services intermédiaires du fait des actes des utilisateurs sera déterminée par la Directive sur le commerce électronique, mais que les autres problématiques (telles que l'obligation d'effacer ou de rectifier des données, ou l'obligation d'un prestataire de services intermédiaires concernant sa propre utilisation de données à caractère personnel) seront régies par le GDPR. Néanmoins, ce point n'est pas clair.

Règlement versus droit national

Puisqu'il s'agit d'un règlement, celui-ci entrera directement en vigueur au sein des États membres, sans nécessiter de législation de transposition.

Néanmoins, dans de nombreux cas, le GDPR permet aux États membres de légiférer sur des problématiques relatives à la protection des données. Cette possibilité englobe les cas dans lesquels le traitement de données à caractère personnel est nécessaire au respect d'une obligation légale, lorsqu'il entre dans le cadre d'une démarche d'intérêt public, ou lorsqu'il est effectué par une autorité publique. De nombreux articles énoncent également que leurs dispositions pourront être précisées ou restreintes par le droit des États membres. Le traitement des données des employés fait partie des exemples pour lesquels les Etats membres pourront adopter des approches différentes.

Les organisations opérant dans des secteurs au sein desquels des *"règles particulières"* s'appliquent souvent (ex: services de santé et services financiers) ont tout intérêt à: (1) déterminer si elles auraient intérêt à bénéficier de telles *"règles particulières"*, qui particulariserait ou libéraliserait le GDPR ; et à (2) les promouvoir en conséquence. Ces organisations ont également tout intérêt à surveiller les États membres désireux d'introduire des *"règles particulières"* susceptibles de se révéler restrictives ou incohérentes au sein des États Membres.

Où puis-je trouver ces dispositions?

Champ d'application matériel	*Champ d'application territorial*
Article 2	*Article 3*
Considérants 15-21	*Considérants 22-25*

Concepts nouveaux et concepts significativement modifiés

En bref

Le GDPR introduit des changements significatifs, notamment via les concepts suivants:

- *Transparence et consentement* – C.-à-d. les informations à fournir aux personnes et les autorisations à solliciter de celles-ci afin de justifier l'utilisation de leurs données à caractère personnel. Les obligations imposées par le GDPR, notamment concernant la nécessité pour le consentement d'être univoque, et de ne pas être déduit d'une simple absence d'action, impliqueront la modification de nombreuses notices d'information des personnes.
- *Mineurs et consentement* – Pour les services en ligne qui s'appuient sur le consentement pour pouvoir procéder à un traitement, le consentement parental vérifiable est exigé afin de pouvoir utiliser les données à caractère personnel d'un enfant. Les États membres sont libres de fixer leurs propres règles concernant les mineurs âgés de 13 à 15 ans (inclus). Si les États membres choisissent de ne pas fixer leurs propres règles, un consentement parental est exigé pour les mineurs de moins de 16 ans.
- Données réglementées – Les définitions des notions de "données à caractère personnel" et de "données sensibles" ont été élargies, les données sensibles englobant désormais les données génétiques et biométriques.
- *Pseudonymisation* – Il s'agit d'un mécanisme de protection renforcée de la vie privée grâce auquel les informations permettant aux données d'être attribuées à un individu spécifique sont conservées séparément et soumises à des mesures techniques et organisationnelles visant à garantir une non attribution.
- *Violation des données à caractère personnel* – Une nouvelle obligation de notifier les violations de sécurité est introduite pour tous les responsables du traitement, quel que soit leur secteur d'activité.

En bref (suite)

- *Protection des données dès leur conception ("Privacy by design"), responsabilité ("Accountability")* – Les organisations sont tenues d'adopter de nouvelles mesures techniques et organisationnelles significatives afin de démontrer leur conformité au GDPR.
- *Droits renforcés* – Les personnes concernées se voient conférer des droits substantiels, parmi lesquels le droit à l'oubli numérique, le droit à la portabilité des données, ainsi que le droit de s'opposer à une prise de décision automatisée.
- *Autorités de contrôle et Comité Européen de protection des Données* – Le contrôle réglementaire régissant la protection des données changera significativement, notamment via l'introduction d'un nouveau point de référence unique – l'autorité chef de file - pour certaines organisations.

A faire

Les actions spécifiques pour la mise en œuvre de ces nouveaux concepts sont explicitées dans les chapitres suivants de ce guide.

Les dispositions du GDPR, ainsi que les obligations qu'il comporte, sont étendues. L.es aspects suivants se démarquent toutefois en tant que concepts matériels nouveaux ou modifiés. D'autres informations relatives à chacun de ces concepts figurent dans d'autres parties de ce guide.

Consentement

Les conditions relatives à l'obtention du consentement sont rendues plus strictes :

- la personne concernée doit avoir le droit de retirer son consentement à tout moment ; et
- il existe une présomption selon laquelle le consentement ne sera pas valable, sauf si des consentements séparés ont été obtenus pour des activités de traitement distinctes. Les mécanismes de consentement forcés ou "omnibus" sont présumés non valables. Bien que des orientations supplémentaires soient attendues, les organisations ont tout intérêt à examiner leurs mécanismes de consentement existants afin de veiller à présenter un choix véritable et détaillé.

Le consentement n'est pas le seul mécanisme permettant de justifier le traitement de données à caractère personnel. Un certain nombre de concepts tels que la nécessité contractuelle, la conformité à l'égard d'une obligation légale (d'un État membre ou de l'UE), ou encore le cas dans lequel le traitement est nécessaire pour la poursuite des intérêts légitimes, demeurent dans le GDPR.

Pour plus d'informations sur ce sujet, veuillez- vous reporter aux sections relatives au consentement, aux mineurs, aux données sensibles, et à la licéité du traitement (au sein du chapitre sur les principes).

Transparence

Les organisations seront tenues de fournir de nombreuses informations aux personnes concernant le traitement de leurs données à caractère personnel.

Le GDPR combine les différentes obligations de transparence qui s'appliquent à travers l'UE. Bien que la liste des informations à fournir s'étende sur 6 pages dans le GDPR, il est demandé aux responsables du traitement d'accomplir ce que les législateurs de l'UE n'ont pas réussi à faire, à savoir fournir ces informations de manière concise, transparente, compréhensible, et aisément accessible.

L'utilisation d'icônes normalisées est évoquée dans le GDPR, et la Commission européenne se voit conférer la possibilité de choisir d'introduire ultérieurement ces icônes au moyen d'actes délégués.

Pour plus d'informations sur ce sujet, veuillez-vous reporter à la section relative aux notices d'information.

Mineurs

Les mineurs de moins de 13 ans ne peuvent en aucun cas donner eux-mêmes leur propre consentement au traitement de leurs données à caractère personnel aux fins d'une fourniture de services en ligne.

Concernant les mineurs âgés de 13 à 15 ans (inclus), la règle générale veut que lorsqu'une organisation sollicite le consentement pour procéder au traitement de leurs données à caractère personnel, le consentement parental doit alors être obtenu, à moins que la législation de l'État membre dont le mineur concerné est ressortissant réduise ce seuil d'âge requis – étant toutefois entendu que ce seuil ne peut jamais être inférieur à 13 ans.

À partir de 16 ans et plus, les mineurs peuvent donner leur propre consentement au traitement de leurs données à caractère personnel.

Le GDPR ne comporte pas de règles spécifiques relatives au consentement parental en ce qui concerne le traitement des données hors ligne : dans ce cas, ce sont les règles habituelles des États membres qui s'appliquent.

Pour plus d'informations sur ce sujet, veuillez- vous reporter au chapitre portant sur les mineurs.

Où puis-je trouver ces dispositions?

Définitions
Article 4
Divers (principalement 26-35)

Données à caractère personnel/données sensibles ("catégories particulières de données")

Le GDPR s'applique aux données à partir desquelles un être humain vivant est identifié ou peut être identifié (par quiconque), que ce soit directement ou indirectement. Le critère actuel de la Directive, consistant à déterminer *"tous les moyens susceptibles d'être raisonnablement utilisés"* pour cette identification, est conservé.

Les considérants du GDPR soulignent le fait que certaines catégories de données en ligne peuvent revêtir un caractère personnel – identifiants en ligne, identifiants d'appareil, données collectées via les cookies et adresses IP. En octobre 2016, dans l'affaire Patrick Breyer v Germany (c-582/14), la CJUE a fourni des précisions longuement attendues sur le statut des adresses IP dynamiques en énonçant qu'une adresse IP constitue une donnée à caractère personnel lorsqu'elle est détenue par un prestataire de services intermédiaires, mais ne constitue pas une donnée à caractère personnel lorsqu'elle est détenue par une partie qui n'a pas "les moyens susceptibles d'être raisonnablement mis en œuvre pour identifier la personne concernée". De façon intéressante, la CJUE n'a pas fait référence aux lignes directrices du G29, lesquelles énoncent que les identifiants uniques qui "permettent à la personne concernée d'être "ciblée" à des fins de suivi de son comportement alors qu'elle est en train de naviguer sur différents sites internet" ne peuvent être qualifiés de données à caractère personnel (Avis 188). Néanmoins, il ne serait pas avisé pour les personnes engagées dans des activités de publicité comportementale en ligne ou des activités similaires d'accorder trop d'importance à l'absence de cette condition au sein de la décision de la CJUE (en tout cas, post GDPR), dans la mesure où le considérant 30 du GDPR énonce que de tels identifiants doivent être considérées comme des données à caractère personnel dès lors qu'ils sont utilisés pour créer des profils relatifs à des personnes et à les identifier.

Les *"Catégories particulières de données"* (souvent appelées données sensibles) sont conservées et étendues afin d'englober les données génétiques et biométriques. De manière identique à l'actuelle Directive sur la protection des données, le traitement de ces données est soumis à des conditions plus strictes que le traitement d'autres formes de données à caractère personnel.

Pseudonymisation

Une nouvelle définition a été introduite et fait référence à une technique de traitement des données à caractère personnel au moyen de laquelle lesdites données ne peuvent désormais plus être attribuées à une "personne concernée" spécifique sans l'utilisation d' informations supplémentaires, lesquelles doivent être conservées séparément et faire l'objet de mesures techniques et organisationnelles permettant de garantir cette non attribution.

Les données pseudonymes restent juridiquement des données à caractère personnel. L'utilisation de la pseudonymisation est toutefois encouragée, notamment dans la mesure où la pseudonymisation :

- constitue un critère à considérer pour déterminer si le traitement est *"compatible"* ou non avec les finalités pour lesquelles les données à caractère personnel ont été initialement collectées et traitées ;
- est également présentée comme un exemple de technique permettant de répondre aux exigences de mise en œuvre de *"mesures de protection de la vie privée dès la conception et par défaut"* (veuillez-vous reporter à la section relative aux obligations de gouvernance des données) ;
- peut constituer un moyen de répondre aux obligations énoncées par le GDPR qui imposent d'assurer la sécurité des données (veuillez-vous reporter à la section relative aux violations de données à caractère personnel et à leur notification); et
- pour les organisations souhaitant utiliser des données à caractère personnel à des fins de recherches historiques ou scientifiques, ou à des fins statistiques, l'utilisation de données pseudonymes est encouragée.

Notification des violations de données à caractère personnel

Le GDPR introduit une obligation de notification des violations de sécurité, qui concerne l'ensemble des responsables du traitement, quel que soit le secteur dans lequel ils opèrent.

Les obligations de notification (aux autorités de contrôle et aux personnes concernées) peuvent potentiellement être déclenchées par *"la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé, qu'ils soient accidentels ou illicites, (à) des données à caractère personnel"*. Pour plus d'informations sur ce sujet, veuillez-vous reporter à la section relative aux violations de données à caractère personnel et à leur notification.

Protection des données dès la conception *("Privacy by design")*/responsabilité *("Accountability")*

Les organisations doivent être en mesure de démontrer qu'elles se conforment aux principes du GDPR, et notamment qu'elles mettent en œuvre certaines mesures de *"protection des données dès la conception"* (ex: l'utilisation de techniques de pseudonymisation), des programmes de formation, et adoptent des politiques et des procédures.

En cas de traitement à "risque élevé" (de type activités de contrôle des personnes, évaluations systématiques, ou traitement de catégories particulières de données), une étude d'impact sur la vie privée détaillée ("EIVP"), également appelée "Privacy Impact Assessment (PIA)", devra être entreprise et documentée. Dans le cas où une EIVP aboutirait à la conclusion qu'il existe effectivement un risque élevé et non atténué pour les personnes concernées, les responsables du traitement devront en informer l'autorité de contrôle et obtenir son avis sur l'adéquation des mesures proposées par l'EIVP afin de réduire les risques liés au traitement.

Les responsables du traitement et les sous-traitants pourront décider de désigner un délégué à la protection des données ("DPO"). Cette désignation est obligatoire pour les organismes du secteur public, les organisations impliquées dans certains traitements sensibles énumérés, ou activités de contrôle, ou dès lors que le droit national impose une telle désignation (la loi allemande est susceptible de continuer à imposer cette obligation après mai 2018). Les groupes de sociétés pourront désigner conjointement un DPO.

Pour plus d'informations sur ces sujets, veuillez-vous reporter à la section relative aux obligations de gouvernance des données.

Des droits renforcés pour les personnes

Le GDPR consacre un large ensemble de droits à la fois existants et nouveaux pour les personnes concernant leurs données à caractère personnel.

Parmi ces droits figurent le droit à l'oubli numérique, le droit à la portabilité qui permet à toute personne physique d'exiger que ses données à caractère personnel soient transmises à un nouveau prestataire de services, ou encore le droit de s'opposer à certaines activités de traitement ainsi qu'à des décisions prises par des processus automatisés.

Pour plus d'informations sur ces sujets, veuillez-vous reporter à la section relative aux notices d'information.

Autorités de contrôle et CEPD

Les autorités de protection des données sont désignées par le GDPR comme autorités de contrôle. Une autorité de contrôle unique, une "Autorité Chef de file" située dans l'État membre au sein duquel une organisation possède son établissement "principal" sera chargée de veiller à ce que cette organisation se conforme au GDPR.

Un Comité Européen de Protection des Données (CEPD) sera créé afin (entre autres nombreuses missions) d'émettre des avis concernant des problématiques particulières, et de trancher les litiges découlant des décisions des autorités de contrôle.

Pour plus d'informations sur ce sujet, veuillez-vous reporter à la section relative à la désignation des autorités de contrôle.

Principes relatifs à la protection des données

En bref

- Bien que les principes relatifs à la protection des données aient été révisés, ils se révèlent être globalement semblables aux principes énoncés dans la Directive 95/46/CE (la "Directive sur la protection des données") : loyauté, licéité et transparence, finalités déterminées, minimisation des données, qualité des données, sécurité, intégrité et confidentialité.
- Un nouveau principe de responsabilité ("accountability") vient imposer aux responsables du traitement la charge de démontrer qu'ils se conforment aux principes relatifs à la protection des données.

A faire

- ☐ Revoyez vos politiques relatives à la protection des données, vos codes de conduite et vos programmes de formations, afin de vous assurer qu'ils sont en conformité avec les principes modifiés.
- ☐ Identifiez les moyens permettant de *"démontrer votre conformité"* – par exemple : adhésion à des codes de conduite approuvés, documentation / trace documentaire concernant les décisions liées au traitement de données, et études d'impact sur la vie privée, le cas échéant..

Degré de changement

Commentaire

Les principes énoncés par le GDPR sont globalement semblables aux principes prévus par la Directive sur la protection des données, mais certains aspects sont nouveaux et apparaissent ci-dessous en italique.

Licéité, loyauté et transparence

Les données à caractère personnel doivent être traitées de manière licite, loyale, et *de manière transparente au regard de la personne concernée.*

Limitation de la finalité

Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Le traitement ultérieur de données à caractère personnel à des *fins archivistique dans l'intérêt public*, ou à des fins statistiques, de recherches scientifiques ou historiques, n'est pas considéré comme incompatible avec les finalités initiales du traitement. Toutefois, les conditions énoncées dans l'article 89(1) (qui énumère les garanties et dérogations liées au traitement pour de telles finalités) doivent être satisfaites.

Minimisation des données

Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire pour l'accomplissement des finalités pour lesquelles ces données sont traitées.

Exactitude

Les données à caractère personnel doivent être exactes et mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes, au regard des finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.

Limitation de la durée de conservation

Les données à caractère personnel doivent être conservées sous *une forme permettant l'identification des personnes concernées* pour une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles ces données à caractère personnel sont traitées. Les données à caractère personnel peuvent être conservées pour des durées plus longues sous réserve qu'elles soient traitées exclusivement à des *fins archivistiques dans l'intérêt public*, à des fins de recherches scientifiques ou historiques, ou encore à des fins statistiques, conformément à l'article 89, pour autant que soient mises en œuvres les mesures techniques et organisationnelles appropriées.

Intégrité et confidentialité

Les données à caractère personnel doivent être traitées d'une manière qui garantisse une sécurité appropriée de ces données, y compris la protection contre le traitement non autorisé ou illicite, contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

Responsabilité

Le responsable du traitement est responsable du respect de ces principes, et doit être *en mesure de démontrer* que ceux-ci sont respectés.

Où puis-je trouver ces dispositions?

Article 5 et Considérant 39

Licéité du traitement initial et du traitement ultérieur

En bref

- Les bases juridiques d'un traitement de données à caractère personnel prévues par le GDPR sont globalement les mêmes que celles énoncées dans la Directive sur la protection des données.
- Des nouvelles restrictions sont toutefois introduites concernant le recours au consentement et le traitement des données relatives aux mineurs.
- Plusieurs restrictions spécifiques sont prévues quant à la possibilité de se fonder sur "l'intérêt légitime" du responsable du traitement en tant que base juridique du traitement. Plusieurs éclaircissements concernant la manière dont cette base légale peut être utilisée sont également apportés.
- Le GDPR fournit une liste non exhaustive de facteurs à prendre en compte afin de déterminer si un traitement de données visant une finalité nouvelle est compatible ou non avec les finalités pour lesquelles ces données ont initialement été collectées.

A faire

☐	Déterminez clairement les bases légales des traitements mis en œuvre par votre organisation, et vérifiez que ces bases légales demeureront applicables en vertu du GDPR.
☐	En cas de recours au consentement, vérifiez que la qualité du consentement réponde aux nouvelles obligations (pour plus d'informations, veuillez-vous reporter à la section relative au consentement).
☐	Déterminez si votre organisation est susceptible d'être affectée par les nouvelles règles régissant le traitement de données relatives aux mineurs. Dans l'affirmative, vérifiez les règles nationales auxquelles votre organisation devra se conformer (pour plus d'informations, veuillez-vous reporter à la section relative aux mineurs).
☐	Vérifiez que vos processus de gouvernance interne vous permettront de démontrer la façon dont sont prises les décisions autorisant l'utilisation des données pour des finalités de traitement ultérieur, et que les critères adéquats conformes au Règlement auront bien été pris en compte.

Degré de changement

Commentaire

L'article 6(1) du GDPR énonce les conditions qui doivent être remplies pour assurer la licéité du traitement de données à caractère personnel (pour les dispositions relatives aux données sensibles, veuillez-vous reporter à la section portant sur les données sensibles et la licéité du traitement). Ces fondements sont globalement les mêmes que ceux prévus par la Directive sur la protection des données. Ces conditions sont les suivantes:

6(1)(a) - Consentement des personnes concernées

Le GDPR aborde la notion de consentement de manière plus restrictive ; il vise en particulier à garantir que le consentement soit donné de manière spécifique pour chaque finalité distincte du traitement (veuillez-vous reporter à la section relative au consentement). Des conditions particulières sont applicables à l'égard des mineurs pour les services en ligne (veuillez-vous reporter à la section relative aux mineurs).

6(1)(b) - Traitement nécessaire à l'exécution d'un contrat auprès de personnes concernées, ou à la prise de mesures précontractuelles nécessaires au contrat

Aucun changement de position par rapport à la Directive sur la protection des données.

6(1)(c) - Traitement nécessaire au respect d' une obligation légale

Cette disposition du GDPR reproduit un fondement équivalent énoncé par la Directive sur la protection des données. Toutefois, l'article 6(3) ainsi que les considérants 41 et 45 énoncent clairement que l'obligation légale en question doit être:

- une obligation émanant de la législation d'un État membre ou de l'UE qui s'impose au responsable du traitement ; et
- *"claire et précise"*, et que l'application de cette obligation doit être prévisible pour ceux qui y sont soumis.

Les considérants énoncent clairement que l' "obligation légale" en question ne doit pas nécessairement être réglementaire (c.-à-d. que le droit commun pourrait suffire, si le critère de l'obligation *"claire et précise"* est rempli). Il est possible qu'une obligation légale couvre plusieurs opérations de traitement effectuées par le responsable du traitement, de telle sorte qu'il ne sera pas nécessairement requis d'identifier une obligation légale spécifique pour chaque activité de traitement intéressant les personnes.

6(1)(d) - Traitement nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouverait dans l'incapacité de donner son consentement

Le considérant 46 suggère que ce fondement pourrait s'appliquer au traitement nécessaire à des fins humanitaires (ex: suivi des épidémies) ou relatif à des urgences humanitaires (ex: réponse aux catastrophes).

Ce considérant énonce que dans les cas où des données à caractère personnel seraient traitées à des fins de sauvegarde des intérêts vitaux d'une personne autre que la personne concernée, ce fondement permettant le traitement devra uniquement être utilisé dès lors que le traitement ne peut pas être fondé sur une autre base juridique.

6(1)(e) - Traitement nécessaire à l'exécution d'une mission effectuée dans l'intérêt général ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement

L'article 6(3) et le considérant 45 énoncent clairement que cette base juridique s'appliquera uniquement lorsque la mission effectuée, ou l'autorité du responsable du traitement, est prévue par la législation de l'Union ou d'un État membre à laquelle est soumis le responsable du traitement.

6(1)(f) - Traitement nécessaire à des fins d'intérêts légitimes

Cette base juridique ne peut désormais plus être invoquée par des autorités publiques traitant des données à caractère personnel dans l'exercice de leurs fonctions; les considérants 47-50 apportent des précisions sur ce qui peut être considéré comme un *"intérêt légitime"*. (Veuillez-vous reporter à la section relative aux intérêts légitimes pour plus d'informations).

Les États membres sont autorisés à introduire des mesures spécifiques visant à établir des bases juridiques en vertu des articles 6(1)(c) et 6(1)(e) (traitement nécessaire au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public, ou à l'exercice d'une autorité publique) et concernant d'autres situations particulières de traitement (ex: journalisme et recherche). Il est probable que ceci engendre un certain degré de variation au sein de l'UE. (Pour plus d'informations, veuillez-vous reporter à la section relative aux dérogations et conditions particulières).

Où puis-je trouver ces dispositions?

Licéité du traitement (données à caractère personnel)
Article 6-10 Considérants 40-50

Traitement ultérieur

Le GDPR prévoit également des règles (à l'article 6(4)) relatives aux facteurs que doit considérer un responsable du traitement afin d'évaluer si une nouvelle finalité de traitement est compatible ou non avec la finalité pour laquelle les données ont été initialement collectées. Lorsqu'un tel traitement ne se fonde pas sur le consentement, ou sur la législation de l'Union ou d'un État membre relative aux problématiques spécifiées dans l'article 23, les facteurs suivants doivent être pris en compte pour déterminer la compatibilité :

- tout lien entre les finalités initiales et les nouvelles finalités proposées ;
- le contexte dans lequel les données à caractère personnel ont été collectées (en particulier la relation entre les personnes concernées et le responsable du traitement) ;
- la nature des données (en particulier leur éventuelle nature de données sensibles ou de données criminelles) ;
- les conséquences potentielles du traitement ultérieur envisagé ; et
- l'existence de garanties (comme le chiffrement ou la pseudonymisation).

Le considérant 50 énonce qu'un traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche historiques ou scientifiques, ou statistiques, doit être considéré comme un traitement compatible (veuillez-vous reporter à la section relative aux dérogations et conditions particulières).

Intérêts légitimes

En bref

- Dans les cas autres que le cas des autorités publiques, la notion d' *"intérêts légitimes"* en tant que base juridique d'un traitement licite, n'est pas significativement modifiée par le GDPR.
- Les autorités publiques ne pourront pas invoquer des *"intérêts légitimes"* pour légitimer un traitement de données réalisé dans le cadre de leurs fonctions.
- Les responsables du traitement invoquant des *"intérêts légitimes"* devront tenir un registre de l'évaluation à laquelle ils auront procédé afin qu'ils puissent démontrer avoir pris en considération, de manière adéquate, les droits et libertés des personnes concernées.
- Les responsables du traitement doivent être conscients que les données à caractère personnel traitées sur la base d'intérêts légitimes sont susceptibles de faire l'objet d'un droit d'opposition qui ne pourra être rejeté que lorsqu'il existe des raisons *"impérieuses"*.

Degré de changement

A faire

- ☐ Déterminez clairement les bases légales des traitements mis en œuvre par votre organisation, et vérifiez que ces bases légales demeureront applicables en vertu du GDPR (veuillez-vous reporter à la section relative à la licéité du traitement initial et du traitement ultérieur).
- ☐ Si votre organisation est une autorité publique s'appuyant à l'heure actuelle sur des *"intérêts légitimes"* pour traiter des données à caractère personnel dans l'exercice de ses fonctions, cherchez à identifier une autre base légale pour le traitement de ces données (ex: traitement nécessaire à l'intérêt public ou à l'exercice d'une autorité publique).
- ☐ Pour vous appuyer sur des *"intérêts légitimes"*, veillez à ce que le processus décisionnel relatif à l'équilibre entre les intérêts du responsable du traitement (ou du tiers concerné) et les droits des personnes concernées soit documenté, en particulier lorsque des mineurs sont concernés. Veillez également à ce que les personnes concernées puissent raisonnablement s'attendre à ce que leurs données soient traitées sur la base des intérêts légitimes du responsable du traitement ou du tiers concerné.
- ☐ Lorsque des *"intérêts légitimes"* sont invoqués, veillez à ce que cette information figure parmi celles qui doivent être fournies aux personnes concernées en vertu des articles 13 et 14. (Veuillez-vous reporter à la section relative aux notices d'information)

Commentaire

L'article 6(1) du GDPR énonce que le traitement des données n'est licite que lorsqu'au moins une des dispositions de l'article 6(1) (a)-(f) s'applique.

L'article 6(1)(f) s'applique lorsque :

"le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée, qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant."

L'article 6(1) énonce clairement que le point (f) ne s'applique pas au *"traitement effectué par les autorités publiques dans l'exécution de leurs missions."*

Ceci reproduit globalement une disposition équivalente qui figure dans la Directive sur la protection des données, à la différence que:

- la nécessité de prendre spécifiquement en considération les intérêts et droits des mineurs est une nouveauté (veuillez-vous reporter à la section relative aux mineurs). En pratique, cette nouveauté est susceptible de contraindre les responsables du traitement à s'assurer que toute décision relative au traitement de données concernant des mineurs fondée sur des "intérêts légitimes" soit bien documentée, ainsi qu'à effectuer une analyse des risques ; et
- Des *"intérêts légitimes"* ne peuvent désormais plus être invoqués par des autorités publiques comme base juridique d'un traitement de données réalisé dans le cadre de leurs fonctions.

Que sont des "intérêts légitimes"?

Les considérants fournissent plusieurs exemples de traitements potentiellement nécessaires aux intérêts légitimes d'un responsable du traitement. Ces exemples comprennent:

- Considérant 47: traitement à des fins de marketing direct ou de prévention des fraudes;
- Considérant 48: transmission de données à caractère personnel au sein d'un groupe d'entreprises à des fins administratives internes, y compris le traitement de données à caractère personnel relatives aux clients et employés (notez que les obligations relatives aux transferts à l'international demeureront applicables - veuillez-vous reporter à la section relative aux transferts de données à caractère personnel);
- Considérant 49: traitement ayant pour finalité de garantir la sécurité des réseaux et des informations, notamment la prévention d'un accès non autorisé à des réseaux de communications électroniques, ainsi que la prévention de dommages susceptibles d'affecter les systèmes informatiques et de communication électronique; et
- Considérant 50: signalement, auprès d'une autorité compétente, d'éventuels actes criminels ou de menaces à la sécurité publique.

Le considérant 47 énonce que les responsables de traitement doivent prendre en considération les attentes des personnes concernées au moment d'évaluer si leurs intérêts légitimes prévalent sur les intérêts des personnes concernées. Les intérêts et droits fondamentaux des personnes concernées *"pourraient en particulier prévaloir sur"* ceux du responsable du traitement lorsque les personnes concernées *"ne peuvent raisonnablement pas s'attendre à un traitement ultérieur."*

Les notices d'information doivent désormais énoncer les intérêts légitimes

Lorsque des *"intérêts légitimes"* constituent la base juridique d'un traitement de données à caractère personnel spécifique, cette information devra désormais apparaître dans les notices d'information en question, conformément aux articles 13(1)(d) et 14(2)(b).

Droit d'opposition spécifique et renforcé

Les individus ont la capacité de s'opposer au traitement de leurs données à caractère personnel lorsqu'il est fondé sur des intérêts légitimes. La charge de la preuve pèse désormais sur les responsables de traitement qui devront prouver qu'ils ont des arguments incontestables leur permettant de continuer à procéder au traitement des données. Cela pourra conduire à l'exercice de droits visant à restreindre et effacer les données à caractère personnel (veuillez-vous reporter à la section relative aux droits d'opposition pour plus information).

Tenez compte des codes de conduite

L'article 40 impose aux États membres, aux autorités de contrôle, au Comité Européen de Protection des Données et à la Commission, d'encourager la création de codes de conduite dans un vaste éventail de domaine, parmi lesquels la question des intérêts légitimes poursuivis par les responsables du traitement dans des circonstances particulières. Les membres d'associations professionnelles ou d'organismes similaires opérant dans des secteurs spécifiques ont tout intérêt à se tenir au fait de la création de tels codes de conduite, susceptibles de leur imposer des contraintes supplémentaires particulières.

Transferts de données, un fondement nouveau, toutefois peu susceptible d'être mis en œuvre en pratique.

Un dernier point concernant les intérêts légitimes figure dans l'article 49(1) (h), qui énonce que des transferts peuvent être effectués sur la base d' *"intérêts légitimes impérieux"* lorsque ces transferts ne présentent pas un caractère répétitif, qu'ils se limitent à un nombre limité de personnes concernées, et à condition que le responsable du traitement en ait évalué et garanti l'adéquation. Néanmoins, ce fondement peut uniquement être invoqué lorsque le responsable du traitement ne peut utiliser aucune autre des méthodes visant à garantir l'adéquation, parmi lesquelles les clauses types, les règles d'entreprises contraignantes "BCR", les contrats approuvés, et toutes les dérogations énoncées dans l'article 49(1)(a)-(f). Le responsable du traitement serait alors contraint par la suite d'informer l'autorité de contrôle qu'il s'était basé sur ce fondement pour le transfert. Il semble peu probable qu'une organisation soit en mesure de démontrer ne pas avoir pu se baser sur un autre fondement juridique pour effectuer le transfert. (Pour plus d'informations, veuillez-vous reporter à la section relative aux transferts de données à caractère personnel).

Où puis-je trouver ces dispositions?

Intérêts légitimes
Articles 6(1)(f), 13(1)(d), 14(2)(b) et 49(1),
Considérants 47, 48, 49, 50

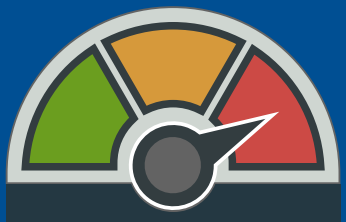
Consentement

En bref

- Le consentement est soumis à des conditions supplémentaires prévues par le GDPR.
- Ces exigences supplémentaires incluent l'interdiction effective des consentements *"groupés"* et des offres de services subordonnées à l'obtention du consentement pour permettre le traitement de données à caractère personnel.
- Le consentement doit désormais également être séparable des autres accords écrits, être clairement présenté, et être aussi simple à retirer qu'à donner.
- Des règles spécifiques s'appliqueront aux mineurs concernant les services de la société de l'information.

A faire

- ☐ Déterminez clairement les bases juridiques sur lesquelles se fonde votre organisation afin de mettre en place des traitements de données à caractère personnel licites, et vérifiez que ces fondements demeureront applicables en vertu du GDPR (veuillez-vous reporter à la section relative à la licéité du traitement initial et du traitement ultérieur).
- ☐ Déterminez si les règles applicables aux données à caractère personnel de mineurs collectées en ligne sont susceptibles de vous affecter et, dans l'affirmative, vérifiez les règles nationales auxquelles votre organisation devra se conformer lors de l'obtention du consentement (pour plus d'informations, veuillez-vous reporter à la section relative aux mineurs).
- ☐ Si, au sein de votre organisation, des traitements de données à caractère personnel à des fins de recherches scientifiques reposent sur le consentement, envisagez de donner la possibilité aux personnes concernées de ne consentir qu'à certains domaines de recherche, ou qu'à certaines parties des projets de recherche.



Degré de changement

A faire (suite)

Lorsque vous vous fondez sur le consentement comme base juridique d'un traitement licite, veillez à ce que :

- le consentement soit actif, et qu'il ne soit pas déduit d'un simple silence, d'une inaction, ou de cases pré-cochées ;
- le consentement au traitement soit dissociable, clair, et qu'il ne soit pas "groupé" avec d'autres déclarations ou accords écrits ;
- l'offre de services ne soit pas subordonnée à l'obtention du consentement qui n'est pas nécessaire à la fourniture dudit service :
- les personnes concernées soient informées de leur droit de retirer leur consentement à tout moment, sans que ceci n'affecte la licéité du traitement fondé sur le consentement donné avant le retrait dudit consentement ;
- des méthodes simples soient mises à disposition afin de permettre le retrait du consentement, y compris des méthodes utilisant le même support que celui utilisé en premier lieu pour obtenir le consentement ;
- des consentements distincts soient obtenus pour des opérations de traitement distinctes ; et à ce que
- le consentement ne constitue pas une base juridique d'un traitement lorsqu'existe un déséquilibre clair entre la personne concernée et le responsable du traitement (en particulier si le responsable du traitement est une autorité publique).

Commentaire

Consentement - une définition élargie

L'article 4(11) du GDPR définit le *"consentement de la personne concernée"* comme *"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."*

L'exigence d'un consentement *"univoque"* n'est pas nouvelle; l'article 7(a) de la Directive 95/46/CE (la "Directive sur la protection des données") énonçait qu'un consentement sollicité pour effectuer un traitement légitime de données devait être donné *"sans équivoque"*. Le considérant 32 suggère qu'un consentement univoque peut être donné :

"En cochant une case lors de la consultation d'un site Internet, en optant pour certains paramètres techniques... ou au moyen d'autre déclaration ou d'un autre comportement indiquant clairement... que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivités."

Un consentement explicite demeure exigé pour justifier le traitement de données à caractère personnel sensibles (à moins que d'autres fondements ne s'appliquent (veuillez-vous reporter à la section relative aux données sensibles et à la licéité du traitement). En outre, un consentement explicite, en l'absence d'adéquation ou d'autres conditions, peut constituer un fondement en vertu du GDPR pour les transferts de données à caractère personnel en dehors de l'UE (veuillez-vous reporter à la section relative aux transferts de données à caractère personnel) et une des bases juridiques pour la prise de décision automatisée relative à un individu (veuillez-vous reporter à la section relative à la prise de décision automatisée).

Étapes nécessaires à la validité - consentement dissociable, révocable et détaillé

L'article 7(1) du GDPR exige que lorsque le traitement repose sur le consentement pour être licite, les responsables du traitement doivent être capables de démontrer que ce consentement a été donné par la personne concernée aux fins dudit traitement. La suite de l'article 7 fixe les conditions relatives à un consentement valide. Ces conditions sont les suivantes:

- Art 7(2): Le consentement à un traitement, contenu dans une déclaration écrite produite par le responsable du traitement, doit être dissociable des autres questions évoquées dans cette déclaration, sous une forme compréhensible aisément accessible, et formulée dans des termes clairs et simples. Le considérant 42 cite la Directive relative aux clauses abusives dans les contrats conclus avec les consommateurs (Directive 93/13/CEE) comme source d'inspiration de ces obligations. En pratique, cela exigera que le consentement au traitement soit clairement dissociable de contrats ou accords plus globaux.

  Le considérant 42 énonce également que le consentement ne sera considéré comme éclairé qu'à condition que la personne concernée ait connaissance (au minimum) de l'identité du responsable du traitement, ainsi que des finalités visées par un tel traitement;

- Art 7(3): Les personnes concernées doivent avoir le droit de retirer leur consentement à tout moment, et cela doit être aussi facile de retirer son consentement que de le donner. En pratique, cela est susceptible d'obliger au minimum les organisations à permettre aux personnes concernées de retirer leur consentement en utilisant le même support (ex : site Internet, courrier électronique, SMS) que le support utilisé pour obtenir le consentement. Le GDPR énonce que le retrait du consentement ne rend pas rétroactivement illicite le traitement, mais exige du responsable du traitement que celui-ci fournisse cette information aux personnes concernées avant que le consentement ne soit donné; et

- Art 7(4): Lorsque l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement à un traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat, cela est susceptible de remettre en cause la mesure dans laquelle le consentement peut être considéré comme librement donné.

Le considérant 43 indique que le consentement sera présumé ne pas avoir été donné librement si :

- malgré son adéquation aux circonstances, aucune disposition ne permet de donner un consentement distinct pour des opérations de traitement distinctes ; ou si
- *"l'exécution d'un contrat, y compris la prestation d'un service... est subordonnée au consentement, malgré que celui-ci ne soit pas nécessaire à une telle exécution."*

Par conséquent, la fourniture d'un service ne doit pas être subordonnée au consentement d'une personne au traitement des données la concernant, pour des finalités qui ne seraient pas nécessaires à la fourniture du service.

Mineurs et recherches scientifiques

Des conditions particulières s'appliquent concernant la validité du consentement donné par des mineurs pour les services de la société de l'information, notamment certaines exigences d'obtention et de vérification du consentement parental en dessous de certaines limites d'âge (pour plus d'informations, veuillez-vous reporter à la section relative aux mineurs).

Le considérant 33 du GDPR traite du consentement à obtenir à des fins de recherche scientifique. Il reconnaît qu'il est *"bien souvent impossible d'identifier pleinement la finalité d'un traitement de données à des fins de recherche scientifique au moment où ces données sont collectées"*, et énonce que:

- les personnes concernées doivent être en mesure de donner leur consentement pour certains domaines de la recherche scientifique, lorsque cela répond à des *"normes éthiques reconnues"* pour de telles recherches ; et que
- les personnes concernées doivent être en mesure de ne donner leur consentement que pour *"certains domaines... ou certaines parties des projets de recherche, dans la mesure permise par la finalité visée."*

Langue du consentement

- Le GDPR impose que le consentement soit compréhensible, éclairé et univoque, etc. Il est peu probable que le consentement remplisse ces exigences si le consentement est requis dans une langue étrangère incompréhensible pour la personne concernée. Lorsque les responsables du traitement déterminent dans quelle langue de l'UE le consentement est requis, il est probable que les règles du GDPR relatives au ciblage dans le contexte du champ d'application territorial soit susceptible de s'appliquer (veuillez-vous reporter à la section relative au champ d'application matériel et territorial). Si une organisation "cible" une juridiction particulière de l'UE, il semble raisonnable de penser que le consentement devra être traduit dans la langue de ladite juridiction. Toutefois, le GDPR n'est pas clair sur ce point ; par exemple le fait de ne pas cibler une juridiction en particulier n'exclut pas nécessairement l'application des obligations relatives à l'obtention du consentement dans la langue de cette juridiction.

Où puis-je trouver ces dispositions?

Articles 4(11), 6(1)(a),7 ,8 et 9(2(a)),
Considérants 32, 33, 42 43

Mineurs

En bref

- Le GDPR contient plusieurs dispositions spécifiques aux mineurs, particulièrement concernant les bases juridiques du traitement et des notices d'information.
- Les mineurs y sont considérés comme des *"personnes vulnérables"*, qui méritent une *"protection particulière."*
- Le GDPR relève que le traitement de données relatives aux mineurs présente certains risques, et des restrictions supplémentaires sont susceptibles d'être imposées au moyen de codes de conduite.
- Le GDPR ne précise pas l'âge auquel un individu est considéré comme un enfant.
- Lorsque des services en ligne sont fournis à un enfant, et que la licéité du traitement de ses données à caractère personnel repose sur le consentement, celui-ci doit être donné ou autorisé par une personne exerçant l'autorité parentale sur cet enfant. Cette exigence s'applique aux mineurs de moins de 16 ans (sauf disposition d'un État membre prévoyant une limite d'âge inférieure, qui ne peut toutefois pas être inférieure à 13 ans).

Degré de changement

A faire

- ☐ Déterminez si les règles applicables aux enfants sont susceptibles de vous affecter.
- ☐ Si votre organisation propose des services de la société de l'information directement à des mineurs, déterminez quelles règles nationales sont susceptibles de s'appliquer, et assurez-vous que des mécanismes appropriés d'obtention du consentement parental soient mis en place, y compris des processus de vérification.
- ☐ Restez attentif à la législation nationale relative au traitement de données hors ligne concernant des mineurs.
- ☐ Lorsque des services sont proposés directement à un mineur, veillez à ce que des notices soient rédigées clairement et puissent être comprises par celui-ci.
- ☐ Veillez à ce que toute invocation d' *"intérêts légitimes"* pour justifier le traitement de données relatives à des mineurs soit appuyée par une analyse consciencieuse et documentée concernant la question de savoir si les intérêts de l'enfant prévalent sur ceux de votre organisation.
- ☐ Restez vigilants sur les codes de conduite applicables, susceptibles d'affecter tout groupe ou association auquel (à laquelle) pourrait participer votre organisation.

Commentaire

L'importance de la protection des enfants est mentionnée à plusieurs reprises dans le GDPR. En pratique, le texte final ne présente pas de nouvelle harmonisation significative et il faut s'attendre à ce que les restrictions les plus conséquentes émanent de lois nationales ou de codes de conduite existants ou à venir. (Veuillez-vous reporter à la section relative aux codes de conduite et aux certifications pour plus d'informations).

Consentement parental

La Directive 95/46/CE (la "Directive sur la protection des données") ne prévoit aucune restriction particulière concernant le traitement des données relatives aux mineurs, et les règles régissant la capacité des enfants à donner leur consentement sont issues des lois nationales. Le GDPR ne présente pas d'harmonisation significative. La principale disposition relative aux enfants est énoncée à l'article 8, et impose l'obtention d'un consentement parental pour les services de la société de l'information proposés directement à un enfant de moins de 16 ans, bien que ce plafond puisse être réduit à 13 ans par un État membre, et qu'il s'applique uniquement lorsque le traitement repose sur le consentement de l'enfant. En revanche, la question de savoir si cette exigence de consentement s'appliquera si les données à caractère personnel d'un enfant ou adolescent sont collectées en ligne de manière non intentionnelle n'est pas claire. Les recommandations initiales fournies par l'autorité de protection des données britannique semblaient suggérer que pour que cette exigence s'applique, les services en ligne doivent être destinés aux enfants.

Le responsable du traitement est également dans l'obligation, conformément à l'article 8(2) du GDPR, de fournir des *"efforts raisonnables"* pour vérifier que le consentement a été donné ou autorisé par le dépositaire de l'autorité parentale au regard des technologies disponibles.

Cette exigence ne concerne que certaines données en ligne, les données hors ligne resteront soumises aux règles habituelles des États membres relatives à la capacité à consentir. De même, l'article 8(1) ne doit pas être considéré comme affectant le droit général des contrats des États membres concernant la validité, la création ou l'effet d'un contrat conclu avec un mineur. Les organisations devront continuer à se référer à leur droit local dans ce domaine.

Les notices d'information adressées aux mineurs doivent être adaptées aux mineurs.

L'article 12 du GDPR prévoit que les obligations consistant à s'assurer que les informations fournies aux personnes concernées soient concises, transparentes et formulées en des termes simples, doivent être respectées "particulièrement pour toutes les informations à fournir spécifiquement à un enfant". Le considérant 58 ajoute :

"Les enfants méritant une protection spécifique, toute information et communication, lorsque le traitement des données les concerne, devra être rédigée en des termes clairs et simples que l'enfant peut aisément comprendre."

Le terme *"enfant"* n'est pas défini par le GDPR. Les responsables du traitement doivent par conséquent se préparer à répondre à ces exigences pour les notices d'information adressées à des adolescents et à de jeunes adultes.

Dispositions diverses - assistance, codes de conduite et activités des autorités de contrôle

L'article 6 (1) (f) du GDPR énonce que les droits et libertés d'une personne concernée pourraient *"en particulier"* prévaloir sur les intérêts du responsable du traitement ou d'un tiers lorsque la personne concernée est un enfant. Les responsables du traitement doivent s'assurer qu'une documentation soit conservée démontrant que les intérêts opposés en présence ont été dûment considérés au moment de se fonder sur des intérêts légitimes comme base juridique pour le traitement de données concernant des enfants.

Le considérant 38 énonce que l'utilisation de données relatives à des enfants à des fins de marketing ou de profilage, ou à des fins de fourniture de services à des enfants, constitue un domaine qui exige une protection particulière en vertu du GDPR. Ce considérant énonce également que le consentement parental ne saurait être exigé dans le cadre de services de prévention et/ou de sensibilisation adressés directement à un enfant, bien que cette suggestion ne soit pas reflétée dans le texte même du GDPR.

Le considérant 75 considère que les enfants sont des *"personnes physiques vulnérables"*, et que le traitement de données concernant des enfants constitue une activité susceptible d'engendrer un risque d'une *"probabilité et d'une gravité variables"*.

L'article 40 impose aux États membres, aux autorités de contrôle, au Comité Européen de Protection des Données et à la Commission d'encourager la création de codes de conduite, notamment dans le domaine de la protection des enfants et concernant la manière dont le consentement peut être recueilli auprès du dépositaire de l'autorité parentale concerné. Les organisations procédant au traitement de données à caractère personnel concernant des enfants doivent surveiller la mise en place de tels codes de conduites susceptibles d'imposer des contraintes supplémentaires particulières.

Enfin, les autorités de contrôle, dans le cadre de leurs démarches de sensibilisation et de compréhension par le public des risques, règles, garanties et droits liés au traitement des données à caractère personnel, conformément à l'obligation que leur impose l'article 57(1)(b), sont tenues de prêter une *"attention particulière"* aux activités qui s'adressent à des enfants.

Où puis-je trouver ces dispositions?

Articles 6(1) (f), 8,12(1) ,40(2) (g), 57(1) (b)
Considérants 38, 58,75

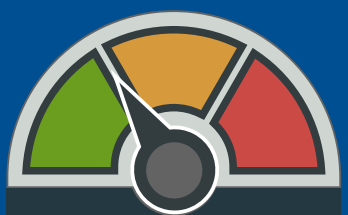
Données sensibles et licéité du traitement de données à caractère personnel

En bref

- Les *"catégories particulières de données à caractère personnel"* (données sensibles) incluent désormais explicitement les *"données génétiques"* et les *"données biométriques"* lorsque ces données sont traitées "afin d'identifier une personne physique de manière unique".
- Les fondements du traitement de données sensibles en vertu du GDPR sont globalement les mêmes que ceux énoncés dans la Directive sur la protection des données, bien qu'ils soient élargis en matière de gestion de la santé et des soins de santé.
- Le GDPR prévoit également une large capacité des États membres leur permettant de fixer des conditions supplémentaires (y compris des restrictions) concernant le traitement de données génétiques, biométriques, et de santé.

A faire

- ☐ Déterminez les bases juridiques sur lesquelles le traitement de données sensibles repose au sein de votre organisation, et vérifiez que ces fondements demeureront applicables en vertu du GDPR;
- ☐ Lorsque le traitement de données sensibles repose sur le consentement, veillez à ce que la qualité du consentement réponde aux nouvelles obligations relatives à l'obtention du consentement (veuillez-vous reporter à la section relative au consentement);
- ☐ Déterminez si les règles applicables aux données à caractère personnel d'enfants sont susceptibles de vous affecter. Dans l'affirmative, déterminez à quelles règles nationales votre organisation devra se conformer lors de l'obtention de leur consentement (pour plus d'informations, veuillez-vous reporter à la section relative aux mineurs);
- ☐ Si vous traitez des quantités importantes de données génétiques, biométriques ou de santé, veillez à vous tenir au fait des évolutions nationales, dans la mesure où les États membres disposent d'un droit étendu leur permettant d'imposer des conditions supplémentaires, y compris des restrictions - en application des principes énoncés dans le GDPR.



Degré de changement

Commentaire

L'article 9(2) énonce les circonstances dans lesquelles il est possible de procéder au traitement de données à caractère personnel sensibles, qui, dans les autres cas, est interdit. Les catégories suivantes de données sont considérées comme *"sensibles"*, tel qu'énoncé à l'article 9(1) :

- origine raciale ou ethnique ;
- opinions politiques ;
- convictions religieuses ou philosophiques ;
- appartenance syndicale ;
- données relatives à la santé, à la vie sexuelle et à l'orientation sexuelle ;
- données génétiques *(nouveauté)*; et
- données biométriques lorsqu'elles sont traitées aux fins d'identifier une personne physique de manière unique *(nouveauté)*.

Notez que le considérant 51 suggère que le traitement de photographies ne sera pas automatiquement considéré comme un traitement sensible (comme c'est le cas à ce jour dans certains États membres); les photographies seront concernées uniquement dans la mesure où elles permettront l'identification ou l'authentification d'une personne, de manière unique, en tant que données biométriques (ex: lorsqu'elles sont utilisées dans le cadre d'un passeport électronique).

Les fondements relatifs au traitement de données sensibles sont globalement les mêmes que ceux prévus par la Directive sur la protection des données. Ces fondements sont les suivants :

9(2) (a) - Consentement explicite de la personne concernée, sauf interdiction de recourir au consentement pour le traitement de données par le droit de l'UE ou d'un État membre

Aucun changement n'intervient ici, bien que de nouvelles conditions concernant le consentement doivent être prises en considération (veuillez-vous reporter à la section relative au consentement).

9(2) (b) - Traitement nécessaire aux fins de l'exécution des obligations en vertu du droit du travail, du droit relatif à la sécurité sociale ou à la protection sociale, ou en vertu d'une convention collective

Ceci vient légèrement élargir la formulation énoncée par la Directive sur la protection des données, en faisant explicitement référence à une nécessaire conformité aux conventions collectives, ainsi qu'au droit relatif à la sécurité sociale et à la protection sociale.

9(2) (c) - Traitement nécessaire à la sauvegarde des intérêts vitaux d'une personne concernée se trouvant dans l'incapacité physique ou juridique de donner son consentement

Ceci reproduit une disposition énoncée dans la Directive sur la protection des données.

9(2) (d) - Traitement effectué par une organisation à but non lucratif pour des finalités politiques, philosophiques, religieuses ou syndicales, à condition que le traitement concerne exclusivement des membres ou anciens membres (ou des personnes entretenant des contacts réguliers avec ces membres, ou participant à ces finalités), et à condition qu'aucune divulgation ne puisse avoir lieu sans le consentement

Ceci reproduit une disposition énoncée dans la Directive sur la protection des données.

9(2) (e) - Données manifestement rendues publiques par la personne concernée

Ceci reproduit une disposition énoncée dans la Directive sur la protection des données.

9(2) (f) - Traitement nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice, ou lorsque les tribunaux exercent leur fonction juridictionnelle

Le traitement de données par des tribunaux exerçant leur fonction juridictionnelle est ajouté à une disposition équivalente dans la Directive sur la protection des données.

9(2)(g) - Traitement nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre proportionnel à l'objectif poursuivi et contenant des mesures de sauvegarde des droits fondamentaux appropriées.

Ceci permet aux États membres d'élargir légalement les circonstances dans lesquelles des données sensibles peuvent être traitées à des fins d'intérêt public.

9(2)(h) - Traitement nécessaire aux fins de la médecine préventive et de la médecine du travail, dans l'appréciation de la capacité de travail des employés, des diagnostics médicaux, de la prise en charge sanitaire et sociale, ou de la gestion des systèmes et services de soins de santé ou de protection sociale, sur la base du droit de l'Union ou du droit d'un État membre, ou en vertu d'un contrat conclu auprès d'un professionnel de la santé

ET

9(2)(i) - Traitement nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé, des médicaments et des dispositifs médicaux

Ces deux dispositions élargissent la disposition équivalente énoncée dans la Directive sur la protection des données, et viennent combler certains manques reconnus dans cette Directive, par exemple en apportant une justification légale et formelle des utilisations règlementaires de données de santé dans le secteur de la santé et pharmaceutique, et en régissant le partage de données de santé avec des prestataires d'aides sociales.

Ces deux conditions imposent que des obligations de confidentialité soient instaurées au moyen de garanties supplémentaires.

9(2) (j) - Traitement nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherches scientifiques, de recherches historiques, ou à des fins statistiques, conformément à l'article 89(1)

Ceci introduit une nouvelle disposition concernant le traitement de données à caractère personnel sensibles à des fins archivistique, de recherche, statistiques, sous réserve d'une conformité aux garanties appropriées, parmi lesquelles des garanties permettant d'assurer le respect des principes de minimisation des données (pour plus d'informations, veuillez-vous reporter à la section relative aux dérogations et conditions particulières).

Données génétiques, biométriques ou de santé

En vertu de l'article 9(4) du GDPR, les États membres sont en droit de maintenir les conditions existantes ou d'imposer des conditions supplémentaires (y compris des restrictions) concernant les données génétiques, biométriques ou de santé. Par conséquent, les divergences d'approche existant autour de ces sujets sont susceptibles d'être maintenues, et il est susceptible que de nouvelles divergences apparaissent. Les organisations procédant au traitement de ces catégories de données ont tout intérêt à se tenir au fait des évolutions du droit national applicable en la matière, et de déterminer la nécessité d'exercer davantage d'influence dans ce domaine.

Condamnations et infractions pénales

Les données relatives aux condamnations et infractions pénales n'entrent pas dans la catégorie des données *"sensibles"* aux fins du GDPR. Il ne s'agit pour autant pas d'un changement, dans la mesure où (bien que la Loi britannique sur la protection des données traite les données relatives à des procédures et condamnations pénales comme des données sensibles) les données de ce type n'étaient pas considérées comme des données sensibles dans la Directive sur la protection des données.

Les règles énoncées par le GDPR concernant les données relatives à des condamnations et infractions pénales reproduisent les règles appliquées en vertu de la Directive sur la protection des données. L'article 10 prévoit que de telles données ne peuvent être traitées que sous le contrôle d'une autorité officielle, ou dès lors qu'un tel traitement est autorisé par le droit de l'Union ou le droit d'un État membre et prévoit des garanties suffisantes. Il faut s'attendre à ce que cette disposition continue de susciter des divergences au sein de l'UE.

Où puis-je trouver ces dispositions?

Articles 9
Considérants 51-56

Notices d'information

En bref

- Les responsables du traitement sont tenus de fournir des notices d'information afin de garantir la transparence du traitement.
- Des informations spécifiées par le GDPR doivent être fournies, et il existe également une obligation générale de transparence.
- La plupart des informations supplémentaires ne devraient pas être difficiles à fournir. C'est la longueur de la liste des informations à fournir qui peut présenter des difficultés. En outre il peut être difficile pour les organisations de fournir des informations quant aux durées de conservation des données. Cette obligation d'information sur les durées de conservation est toutefois déjà prescrite en droit français par la Loi Informatique et Libertés depuis sa modification par la Loi pour une République Numérique du 7 octobre 2016.
- L'accent est placé sur la nécessité de fournir des notices d'information claires et concises

A faire

- ☐ Examinez, révisez et actualisez vos notices d'information existantes.
- ☐ S'agissant des données collectées de manière indirecte, veillez à ce que la notice d'information soit fournie au moment approprié.
- ☐ Travaillez avec vos partenaires susceptibles de collecter des données pour le compte de votre organisation afin d'attribuer la responsabilité de l'examen, de l'actualisation et de la validation des notices d'information.

Commentaire

Le principe du traitement *"loyal et transparent"* exige que le responsable du traitement doive fournir des informations aux personnes concernées concernant le traitement de leurs données, à moins que ces informations aient déjà été fournies à ces personnes. Les informations à fournir sont précisées par le GDPR et sont énumérées ci-dessous. Le responsable du traitement peut également être tenu de fournir des informations supplémentaires si, compte tenu de circonstances et d'un contexte spécifiques, cela est nécessaire afin de s'assurer que le traitement des données est loyal et transparent. Les informations doivent être fournies de manière concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples (en particulier lorsque la personne concernée est un enfant).

Quelles sont les informations que doit communiquer le responsable du traitement aux personnes concernées ?

Le GDPR impose que soient fournies des informations plus complètes que ce qui était prévu par la Directive sur la protection des données – bien que la communication de la plupart de ces informations supplémentaires soit d'ores et déjà exigée dans certains États membres.

Les informations non mentionnées dans la Directive sur la protection des données apparaissent ici en italique.

- Identité et coordonnées du responsable du traitement (ou de son représentant si le responsable du traitement n'est pas établi dans l'UE); *coordonnées du Délégué à la Protection des Données.*
- Finalités du traitement et base juridique du traitement – y compris l' *"intérêt légitime" poursuivi par le responsable du traitement (ou un tiers) lorsque cet intérêt légitime est invoqué en tant que base juridique.*
- Destinataires, ou catégories de destinataires.
- *Détails relatifs aux transferts de données en-dehors de l'UE, notamment:*
  - *la manière dont les données seront protégées (ex: le destinataire est un État pour lequel une décision d'adéquation a été rendue par la Commission, des règles d'entreprise contraignantes sont appliquées (BCR), etc.); et*
  - *la manière dont les personnes peuvent obtenir une copie des BCR ou d'autres garanties, ou le l'endroit où de telles garanties ont été mises à disposition.*
- *La durée de conservation des données – en cas d'impossibilité, le critère utilisé pour déterminer cette durée.*

NB: Cette obligation d'information sur les durées de conservation est toutefois déjà prescrite en droit français par la Loi Informatique et Libertés depuis sa modification par la Loi pour une République Numérique du 7 octobre 2016.

- Le fait que la personne a un droit d'accès un droit à la *portabilité de ses données, un droit de rectifier, d'effacer et de limiter ses données à caractère personnel, un droit de s'opposer au traitement de ses données, et, en cas de traitement reposant sur le consentement, le droit de retirer son consentement.*
- *Le fait que la personne a le droit d'introduire une réclamation auprès d'une autorité de contrôle.*
- *L'existence ou non d'une contrainte réglementaire ou contractuelle imposant de fournir les données, ainsi que les conséquences de l'absence de fourniture des données.*
- L'existence ou non d'une prise de décision automatisée – ainsi que les informations concernant la logique sous-jacente, la signification et les conséquences du traitement pour la personne.

À quel moment le responsable du traitement est-il tenu de fournir ces informations ?

Si le responsable du traitement obtient directement les informations auprès de la personne

- Au moment où les données sont collectées.

Le responsable du traitement est également tenu d'indiquer aux personnes les informations qui doivent obligatoirement être communiquées, ainsi que les conséquences de l'absence de communication desdites informations.

Si le responsable du traitement ne les obtient pas directement auprès de la personne

- Dans un délai raisonnable après avoir obtenu les données (délai maximum d'un mois) ; ou
- Si les données sont utilisées pour communiquer avec la personne, au plus tard lors de la première communication à ladite personne ; ou
- S'il est envisagé de communiquer les informations à un autre destinataire, au plus tard avant que les données ne soient communiquées.

Le responsable du traitement est également tenu d'informer les personnes des catégories d'informations ainsi que de la (des) source(s) des informations, y compris du fait que ces informations proviennent de source publiquement accessibles.

- Le responsable du traitement n'est pas tenu de fournir ces informations à la personne dans les cas où cela serait impossible ou nécessiterait un effort disproportionné. Dans de tels cas, des mesures appropriées doivent être prises afin de protéger les intérêts des personnes, et les notices d'information doivent être mises à disposition du public.

  Il n'y a pas d'obligation de fournir des notices d'information:

  - si le droit de l'UE ou le droit d'un État membre prévoit l'obligation pour le responsable du traitement d'obtenir/ de communiquer l'information ; ou
  - si l'information doit demeurer confidentielle en raison d'obligations de secret professionnel ou réglementaires, obligations réglementées par le droit de l'UE ou le droit d'un État membre.

Si le responsable du traitement procède à un traitement ultérieur visant une nouvelle finalité non envisagée dans la notice d'information initiale, il sera alors tenu de fournir une nouvelle notice d'information incluant ce nouveau traitement.

Le fait de devoir fournir toutes ces informations est difficilement conciliable avec l'exigence de concision et de clarté énoncée par le GDPR.

Afin d'aider à atteindre cet objectif, il est prévu que la Commission puisse introduire des icônes normalisées via des actes délégués. Si elles sont introduites, ces icônes devront également être communiquées aux personnes.

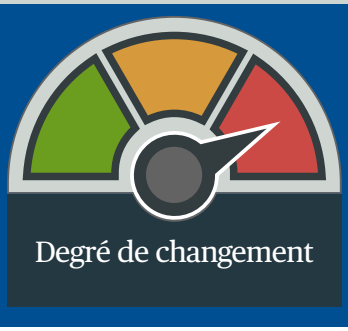
Où puis-je trouver ces dispositions?

Articles 12-14
Considérants 58, 60, 61 et 62

Droit d'accès, de rectification et de portabilité des données à caractère personnel pour les personnes

En bref

- Sur demande, les responsables du traitement sont tenus de :
  - confirmer s'ils procèdent au traitement des données à caractère personnel d'un individu ;
  - fournir une copie des données (dans de nombreux cas, sous une forme électronique d'usage courant) ; et de
  - fournir des documents justificatifs d'explication (détaillés).
- Les personnes concernées peuvent également demander à ce que leurs données à caractère personnel leurs soient restituées, ou soient transférées à un nouveau prestataire, sous format lisible par une machine, à condition que les données en questions aient été : 1) fournies par la personne concernée au responsable du traitement (interprété largement) ; 2) traitées automatiquement ; et
- 3) traitées sur la base du consentement ou de l'exécution d'un contrat.
- Cette demande doit être satisfaite dans un délai d'un mois (certains cas autorisant une extension de ce délai), et toute intention de ne pas y satisfaire doit être expliquée à la personne concernée.
- Les droits d'accès ont pour objectif de permettre aux personnes de vérifier la licéité du traitement, et le droit d'obtenir une copie ne saurait porter atteinte aux droits d'autrui.



A faire

☐	Examinez et révisez les processus, les procédures et la formation des équipes en contact avec le client – sont-elles suffisantes pour satisfaire aux règles relatives au droit d'accès et à la portabilité énoncées par le GDPR?
☐	Élaborez des courriers de réponse type afin de vous assurer que toutes les informations nécessaires soient fournies.
☐	Évaluez la capacité de votre organisation à fournir des données en conformité avec les obligations de format énoncées par le GDPR. Il sera éventuellement nécessaire de développer des capacités de formatage afin de satisfaire aux exigences relatives aux demandes d'accès.
☐	Si la portabilité s'applique, déterminez quels sont vos fichiers concernés. Déterminez si les données (et métadonnées associées) pourront être facilement exportées dans des formats structurés, lisibles par des machines. Tenez-vous au fait des initiatives technologiques visant à développer des formats interopérables.
☐	Songez à développer des portails d'accès pour les personnes concernées afin de permettre l'exercice direct du droit d'accès de ces personnes.

Droit à l'information et droit d'accès

Une personne dispose des droits suivants qu'elle peut exercer auprès du responsable de traitement :

- droit d'obtenir la confirmation que ses données à caractère personnel font l'objet d'un traitement ;
- droit d'accéder à ses données (par exemple, au moyen d'une copie) ; et
- droit d'obtenir des informations supplémentaires concernant le traitement.

Comme pour tous les droits des personnes concernées, le responsable du traitement est tenu d'y répondre *"sans retard injustifié"* et *"dans un délai maximum d'un mois",* bien que ce délai puisse dans certains cas être prolongé.

Le responsable du traitement est également tenu d'employer tous les moyens raisonnables pour vérifier l'identité de la personne effectuant la demande, mais ne doit pas conserver ou collecter des données dans le seul but de pouvoir répondre aux demandes d'accès. Ces aspects revêtent une importance particulière en matière de services en ligne.

Droit d'accès aux données

Le responsable du traitement est tenu de fournir *"une copie des données à caractère personnel faisant l'objet d'un traitement".* Cette copie doit être fournie gratuitement (changement pour les responsables du traitement basés au Royaume-Uni), bien que le responsable du traitement soit en droit d'exiger le paiement de frais administratifs raisonnables en cas de demande de copies supplémentaires.

Lorsque la personne concernée fait la demande sous format électronique, les informations doivent être fournies sous une forme électronique d'usage courant (à moins que la personne concernée ne demande qu'il en soit autrement). Cela est susceptible d'engendrer des coûts pour les responsables du traitement recourant à des formats spéciaux ou tenant des registres papier.

Le considérant 63 suggère également aux responsables du traitement d'utiliser, lorsque cela est possible, un système sécurisé susceptible de permettre aux personnes concernées d'accéder directement à leurs données. Il semble s'agir davantage d'une incitation que d'une exigence.

Informations supplémentaires

Le responsable du traitement est également tenu de fournir les informations suivantes (les éléments en italique ne sont actuellement pas exigés par la Directive sur la protection des données – bien qu'elles soient exigées par le droit de certains États Membres en application de la Directive sur la protection des données):

- les finalités du traitement ;
- les catégories de données traitées ;
- les destinataires, ou les catégories de destinataires *(en particulier les détails concernant la communication à des destinataires établis dans des pays tiers ou à des organisations internationales* (entités régies par le droit international public ou mises en place par des accords entre les pays)
- *la durée de conservation des données à caractère personnel prévue ou, en cas d'impossibilité, les critères utilisés pour déterminer cette durée;*
- *le droit pour les personnes de rectifier, d'effacer, de limiter le traitement, de s'opposer au traitement, et d'introduire une réclamation auprès d'une autorité de contrôle;*
- *les informations relatives à la source des données (si elles ne sont pas collectées auprès de la personne concernée);* et
- l'existence d'une prise de décision automatisée (c.-à-d. des décisions uniquement prises de manière automatique et ayant des effets juridiques ou similaires, ainsi que la prise de décision automatisée impliquant des données sensibles) – y compris les informations relatives à la logique sous-jacente ainsi qu'à l'importance et *aux conséquences prévues du traitement pour la personne concernée.*

Si le responsable du traitement n'entend pas satisfaire cette demande, il est tenu de justifier son refus.

Exemptions

Le GDPR reconnaît que le droit d'accès des personnes concernées est susceptible de porter atteinte aux droits d'autrui, et énonce que le droit d'obtenir une copie des données ne saurait porter atteinte aux droits d'autrui. Le considérant 63 énonce que ceci pourrait s'étendre à la protection des droits de propriété intellectuelle et au secret des affaires (par exemple, si la diffusion de la logique sous-jacente d'une prise de décision automatisée impliquerait la divulgation de telles informations). Néanmoins, ce considérant énonce également qu'un responsable du traitement ne saurait refuser de fournir *toutes* les informations au motif qu'un tel accès risquerait de porter atteinte aux droits d'autrui.

Le considérant 63 énonce également deux restrictions utiles :

- si le responsable du traitement détient une importante quantité de données, il est en droit de demander à la personne concernée que celle-ci lui précise spécifiquement les informations ou les activités de traitement sur lesquelles porte sa demande. (Toutefois, ce considérant n'évoque pas la possibilité d'une exemption justifiée par l'important volume des données en question: la limitation semble concerner davantage la spécificité de la demande plutôt que le temps et les efforts nécessaires à fournir par le responsable du traitement – bien que les deux aspects puissent être liés);

- ce droit dont jouit la personne concernée consiste à lui permettre d' *"avoir connaissance et de vérifier la licéité du traitement"*. Ceci vient confirmer les commentaires formulés par la CJUE dans l'affaire YS c. Minister voor Immigratie, Integratie en Asiel (Affaire C-141/12), selon lesquels l'objectif de la demande d'accès formulée par la personne concernée consiste à permettre à la personne concernée de confirmer l'exactitude des données ainsi que la licéité du traitement, et à lui permettre d'exercer, le cas échéant, ses droits de rectification, d'opposition, etc. Autrement dit, cet objectif est lié aux droits des personnes en vertu de la législation sur la protection des données: les demandes formulées à des fins autres que celles relatives à la protection des données semblent pouvoir être rejetées.

Rectification

Les personnes sont en droit de demander à un responsable du traitement que celui-ci rectifie les inexactitudes des données à caractère personnel les concernant. Dans certains cas, si les données à caractère personnel sont incomplètes, une personne peut demander au responsable du traitement de compléter ces données, ou d'enregistrer une déclaration supplémentaire.

Portabilité

Le droit d'accès aux données dont jouissent les personnes concernées en vertu du GDPR confère aux personnes le droit de demander à ce que leurs données leur soient fournies sous une forme d'usage courant.

La portabilité des données s'étend au-delà de ce droit, et exige du responsable du traitement qu'il fournisse ces informations dans un format structuré, communément utilisé, et lisible par une machine. De plus, le responsable du traitement peut être tenu de transmettre ces données directement à un autre responsable du traitement. Le GDPR encourage les responsables du traitement à développer des formats interopérables.

Alors que le droit d'accès des personnes présente un caractère large, le droit à la portabilité revêt un caractère plus restreint. La portabilité s'applique:

- aux données à caractère personnel traitées par des moyens automatisés (absence de registres papier) ;

- aux données à caractère personnel qui ont été fournies au responsable du traitement par la personne concernée ; et

- exclusivement lorsque le traitement repose sur le consentement, ou lorsque les données sont traitées aux fins d'exécution d'un contrat de mise en œuvre ou de mesures précontractuelles.

Les données que les personnes concernées "ont fourni" sont interprétées largement. Ceci n'est pas limité aux formulaires complétés par les personnes concernées mais aux informations collectées par le responsable du traitement au cours de ces opérations avec la personne concernée. Par exemple, les données collectées au moyen d'un compteur intelligent seront concernées ainsi que des emails envoyés à la personne concernée.

La portabilité des données est sans préjudice des droits des autres individus. Toutefois, selon les autorités de protection des données à caractère personnel, le responsable du traitement originaire n'a pas l'obligation de vérifier l'éventuel préjudice.

Au contraire, toute organisation recevant des données doit s'assurer que son utilisation des données à caractère personnel est licite. Il existe des exemptions à la portabilité – par exemple, lorsque cela risquerait de porter atteinte aux droits de propriété intellectuelle ou au secret des affaires. Les autorités de protection considèrent que cela n'empêche pas toute conformité avec ce droit.

Où puis-je trouver ces dispositions?

Accès des personnes	*Article 15*	*Considérants 59, 63, 64*
Rectification	*Article 16*	*–*
Portabilité	*Article 18*	*Considérant 68 et Avis G29 242*

Droits d'opposition

En bref

- Les personnes disposent du droit de s'opposer à certains types de traitement spécifiques :
  - Prospection;
  - Profilage (veuillez-vous reporter à la section relative au droit d'opposition au profilage);
  - Traitement justifié par des intérêts légitimes ou par l'exécution d'une mission visant l'intérêt public/l'exercice de l'autorité publique; et
  - Traitement à des fins de recherche ou de statistiques.
- Seul le droit de s'opposer à un traitement effectué à des fins de prospection est absolu (c.-à-d. nul besoin d'invoquer des motifs pour justifier l'opposition, aucune exemption ne permet de poursuivre un tel traitement).
- Certaines obligations imposent d'informer les personnes des droits dont ils disposent à un stade précoce, de manière claire et distincte de toute autre information.
- Les services en ligne sont tenus de proposer une méthode automatisée permettant d'exercer le droit d'opposition.

A faire

- ☐ Examinez vos notices d'information et politiques relatives à la protection des données, afin de veiller à ce que les personnes soient informées de leur droit d'opposition, de manière claire et distincte, ce, dès la "première communication";
- ☐ Pour les services en ligne, veillez à ce que soit mis en place un mécanisme automatisé permettant d'exercer ce droit; et
- ☐ Examinez vos listes et processus de suppression marketing (y compris les listes et processus opérés pour le compte de votre organisation par des partenaires et prestataires de services) afin de vous assurer qu'ils sont en capacité d'opérer en conformité avec le GDPR.

Droits d'opposition

Le GDPR prévoit trois droits d'opposition. Ces trois droits concernent les traitements de données effectués pour des finalités particulières ou qui ont une base juridique particulière.

Il n'existe pas de droit permettant à une personne de s'opposer à tout traitement de manière générale.

Ces droits peuvent permettre à une personne de s'opposer aux traitements suivants :

Traitement à des fins de prospection

Il s'agit d'un droit absolu ; dès lors qu'une personne exerce ce droit d'opposition, ses données ne doivent plus être traitées à des fins de prospection.

Traitement à des fins de recherches scientifiques, historiques ou statistiques

Ce droit n'est pas aussi absolu que le droit de s'opposer à un traitement à des fins de prospection. Il doit exister des *"raisons tenant à la situation particulière [de la personne concernée]".*

Une exception existe lorsque ce traitement est nécessaire à l'exécution d'une mission d'intérêt public.

Il n'existe pas d'équivalent à cette disposition dans la Directive sur la protection des données.

Autres traitements basés sur deux fondements particuliers:

Ici encore, le droit d'opposition peut être exercé pour des motifs liés à la situation particulière de la personne concernée, ce qui signifie que la personne concernée devra invoquer des motifs permettant de justifier son opposition. En outre, ce droit d'opposition ne pourra s'exercer que si:

1. Le traitement est fondé sur l'intérêt légitime du responsable du traitement (i.e. Art. 6(1) (f)) ; ou
2. Le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public/l'exercice de l'autorité publique (i.e. Art. 6(1) (e))

Le responsable du traitement est alors tenu de cesser le traitement des données à caractère personnel, excepté :

- s'il parvient à démontrer que des motifs légitimes et impérieux prévalent sur les intérêts de la personne concernée ; ou
- si le traitement est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice.

Ainsi, dès lors qu'une personne exerce son droit d'opposition sur la base de sa situation particulière, la charge de la preuve repose sur le responsable du traitement qui doit prouver en quoi, en dépit de la situation particulière de cette personne, il doit rester en capacité de traiter les données à caractère personnel de cette personne sur ce fondement.

Les règles énoncées par la Directive sur la protection des données sont ici renforcées. Dans la disposition équivalente, c'est à la personne concernée que revient la charge de démontrer des "motifs légitimes et impérieux" qui fondent son opposition, et le traitement ne doit cesser que si cette opposition est justifiée.

Notification de leurs droits aux personnes concernées

En cas de traitement à des fins de prospection, et en cas de traitement fondé sur l'intérêt public ou sur l'intérêt légitime du responsable de traitement, le droit d'opposition doit être explicitement porté à l'attention de la personne concernée, au plus tard au moment de la première communication avec cette personne. Cette information doit être présentée de manière claire et distincte par rapport aux autres informations.

Cette exigence d'information des personnes ne s'applique pas aux traitements de données à des fins statistiques/de recherche.

Dans le cas des services en ligne, la personne doit pouvoir exercer son droit d'opposition par des moyens automatisés.

Où puis-je trouver ces dispositions?

Article 21 *Considérants 69 et 70*

Droit d'opposition au profilage

En bref

- Les personnes disposent du droit de s'opposer à un traitement de leurs données à caractère personnel et peuvent exercer ce droit, à tout moment, pour des raisons tenant à leur situation particulière.
- Les personnes peuvent également s'opposer à un profilage lorsqu'il est réalisé à des fins de prospection. Il s'agit d'une véritable nouveauté prévue par le GDPR.

  Dans ce cas, la personne concernée n'aura pas besoin d'invoquer des motifs pour justifier son opposition au traitement de ses données, aucune exemption ne permettant de poursuivre le traitement.
- L'existence de ce droit d'opposition a pour conséquence d'imposer aux responsables de traitement une obligation d'informer les personnes de leurs droits d'opposition, de manière claire et distincte.
- Les services de la société de l'information auront l'obligation de mettre en place des méthodes automatisées permettant d'exercer le droit d'opposition ainsi que des moyens techniques permettant d'arrêter le profilage dès lors qu'un droit d'opposition en ce sens est exercé.

A faire

- ☐ Examinez vos notices d'information et politiques relatives à la protection des données, afin de veiller à ce que les personnes soient informées de leur droit d'opposition, de manière claire et distincte, ce, dès la "première communication";
- ☐ Pour les services de la société de l'information, veillez à ce que soit mis en place un mécanisme automatisé permettant aux personnes concernées d'exercer ce droit ; et
- ☐ Vérifiez que vous disposez de moyens techniques permettant d'arrêter un traitement de données consistant à profil les personnes, dès lors qu'une personne exerce son droit d'opposition.

Degré de changement

Le profilage

Le profilage se définit comme *"toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects 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".*

Le droit d'opposition au profilage

L'article 21 du GDPR prévoit plusieurs droits d'opposition et notamment :

1. Le droit de s'opposer à tout moment, pour des raisons tenant à la situation particulière de la personne concernée, à un traitement de ses données à caractère personnel, y compris un profilage, sous réserve que :

   - Le traitement soit nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique (Art 6(1) (e) ;

   - Le traitement soit nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts et droits fondamentaux de la personne concernée (Art 6(1) (f).

     Cela signifie que la personne concernée devra invoquer des motifs lui permettant de justifier son opposition.

     Le responsable du traitement sera alors tenu de cesser le traitement des données à caractère personnel, excepté :

   - s'il parvient à démontrer que des motifs légitimes et impérieux prévalent sur les intérêts de la personne concernée ; ou

   - si le traitement est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice.

2. Le droit de s'opposer à un traitement de ses données à caractère personnel à des fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection.

En outre, le GDPR confère aux personnes concernées un droit absolu de s'opposer au profilage à des fins de prospection sans que les personnes concernées n'aient besoin d'invoquer un motif au soutien de leur demande.

Il est important de noter que, par conséquent, le responsable de traitement n'aura plus seulement l'obligation d'arrêter la prospection de la personne de concernée. Il devra également arrêter le traitement consistant à utiliser les données à caractère personnel de la personne concernée afin de réaliser un profilage de celle-ci à des fins de prospection.

Où puis-je trouver ces dispositions?

Article 21 *Considérants 69 et 70*

Droit à l'effacement des données et droit à la limitation du traitement

En bref

- De nouveaux droits aux contours encore flous sont introduits: un "droit à l'oubli" (désormais qualifié de droit à l'effacement) et un droit à la limitation du traitement des données.
- Les personnes peuvent exiger que leurs données soient "effacées", lorsqu'un problème concernant la légalité du traitement apparait, ou lorsqu'elles retirent leur consentement (sur lequel le traitement est fondé).
- Une personne peut exiger que le responsable du traitement "limite" le traitement de ses données le temps nécessaire à la prise en compte de sa réclamation (par exemple concernant l'exactitude des données), ou lorsque le traitement est illicite mais que la personne s'oppose à l'effacement de ses données.
- Lorsque le responsable du traitement a rendu publiques des données qui font par la suite l'objet d'une demande d'effacement, celui-ci est tenu d'informer les autres responsables du traitement de ces données de l'existence et du contenu de cette demande. Il s'agit là d'une nouvelle obligation large et problématique

A faire

- ☐ Veillez à ce que le personnel et les fournisseurs susceptibles de recevoir des demandes d'effacement de données soient en mesure de les identifier et sachent comment les traiter
- ☐ Évaluez la possibilité que vous opériez dans un secteur au sein duquel le fait de répondre favorablement aux demandes d'effacement s'avèrerait si déraisonnable, et infondé, qu'il faille recourir à des exemptions prévues par les États membres.
- ☐ Évaluez si vos systèmes vous permettent de satisfaire aux exigences visant à limiter le traitement de certaines données le temps nécessaire à la prise en compte des réclamations: entreprenez au besoin les développements nécessaires.

Degré de changement

Droit à l'oubli

Les personnes peuvent demander à ce que leurs données soient "effacées" dans certains cas spécifiques ; pour l'essentiel lorsque le traitement échoue à satisfaire aux exigences du GDPR. Ce droit peut être exercé à l'encontre de responsables du traitement, qui sont alors tenus d'y répondre dans les meilleurs délais (et, en toute hypothèse, dans un délai maximum d'un mois, bien que ce délai puisse être prolongé dans certains cas complexes).

Quand ce droit s'applique-t-il ?

- Lorsque les données ne sont plus nécessaires au regard de la finalité pour laquelle elles ont été collectées ou traitées.
- Lorsque la personne concernée retire son consentement au traitement (et qu'il n'existe aucun autre fondement au traitement).
  - L'exercice de ce droit est également possible en cas de retrait du consentement précédemment donné par un enfant dans le cadre de services en ligne. Néanmoins, il semble qu'aucune nouveauté ne soit ajoutée au principe général selon lequel le consentement peut être retiré et que lorsque c'est le cas, la personne concernée est en droit d'exiger que ses données soient effacées.
- Pour les traitements fondés sur des motifs légitimes, lorsque la personne concernée s'oppose au traitement, et que le responsable du traitement ne peut démontrer l'existence de motifs légitimes impérieux prévalant pour un tel traitement.
- Lorsque les données feraient l'objet d'un traitement illicite (i.e. elles seraient traitées en violation des dispositions du GDPR).
- Lorsque les données doivent être effacées pour respecter une obligation légale prévue par le droit de l'Union ou d'un Etat membre à laquelle le responsable du traitement est soumis.

Cette dernière hypothèse surviendrait par exemple si une personne considérait qu'un responsable du traitement conserve ses données à caractère personnel alors même que la législation énonce que de telles données (par exemple, une vérification liée à l'emploi) doivent être effacées à l'issue d'une période déterminée.

Cette disposition générale, en vertu de laquelle des demandes d'effacement peuvent être formulées lorsque les données font l'objet d'un traitement *"illicite"* pourrait poser des difficultés : nombreux sont les cas dans lesquels les données pourraient faire l'objet d'un traitement illicite au regard du GDPR (éventuelle inexactitude des données, non communication d'un élément d'information obligatoire auprès de la personne concernée). Toutefois, rien n'indique clairement que ceci vienne fonder le droit d'exiger l'effacement de données. La disposition équivalente figurant dans la Directive sur la protection des données autorisait à davantage de discrétion, en exigeant un effacement "selon le cas". Il conviendra d'observer la manière dont les exemptions seront rédigées par les États membres.

Données rendues publiques

Lorsque le responsable du traitement a rendu publiques des données à caractère personnel, et qu'il doit procéder à leur effacement, ce dernier est alors tenu d'informer les autres responsables du traitement qui traitent ces données du fait que la personne concernée a exigé que ses données soient effacées. Cette obligation vise à renforcer les droits des personnes au sein de l'environnement en ligne.

Cette obligation impose de prendre des *mesures raisonnables*, et de prendre en compte les technologies disponibles et le coût de mise en œuvre. Néanmoins, cette obligation pourrait revêtir une portée extrêmement large, et se révéler très difficile à mettre en œuvre : par exemple, dans la mesure où les données sont devenues publiques, se pose la question de savoir comment le responsable du traitement initial pourra identifier les responsables du traitement qu'il doit informer.

Autres obligations de notification auprès des destinataires

Lorsque le responsable du traitement est dans l'obligation d'effacer des données à caractère personnel, il est alors tenu de le notifier à tous ceux auxquels il a transmis ces données, à moins que cette communication soit impossible ou implique des efforts disproportionnés.

Exemptions

Cette obligation ne s'applique pas lorsque le traitement est nécessaire;

- à l'exercice du droit à la liberté d'expression et d'information;
- au respect d'une obligation légale prévue par le droit de l'Union ou d'un État membre;
- à l'exécution d'une mission d'intérêt public, ou relevant de l'exercice de l'autorité publique;
- à des fins de santé publique;
- à des fins archivistique, de recherches ou statistiques (si les conditions régissant ce type de traitement sont satisfaites); ou
- à la constatation, à l'exercice ou à la défense de droits en justice.

Veuillez-vous reporter à la section relative aux dérogations et conditions particulières pour les autres situations dans lesquelles des exemptions peuvent s'appliquer, si ces exemptions sont prévues par le droit de l'Union ou la législation d'un État membre.

Droit à la limitation du traitement

Ce pan vient remplacer les dispositions de la Directive sur la protection des données relatives à la notion de "verrouillage". Dans certains cas, ce droit donne à la personne concernée une alternative à la demande d'effacement des données. Dans d'autres, il permet à la personne concernée de demander à ce que ses données soient conservées le temps que d'autres questions soient traitées.

En quoi consiste la limitation du traitement ?

Dès lors que des données à caractère personnel font l'objet d'une "limitation", le responsable du traitement est seulement autorisé à conserver ces données. Il ne pourra dès lors plus traiter ces données, excepté :

- si la personne concernée y consent; ou
- si ce traitement est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ; à la protection des droits d'une autre personne physique ou morale ; pour des motifs importants d'intérêt public (de l'Union ou d'un État membre).

Lorsque les données sont traitées automatiquement, la limitation du traitement doit être assurée par des moyens techniques, et être indiquée de manière claire dans les systèmes informatiques du responsable du traitement. Ceci pourrait nécessiter de déplacer des données vers un système distinct, de verrouiller les données sur un site Web, ou de rendre ces données indisponibles d'une autre manière.

Lorsque des données ont été communiquées auprès d'autres destinataires, le responsable du traitement est tenu d'informer ces autres destinataires de la limitation de traitement dont font l'objet ces données (sauf si cela est impossible ou nécessite un effort disproportionné).

Le responsable du traitement est tenu d'informer la personne concernée avant de lever une limitation de traitement.

Quand cette limitation s'applique-t-elle ?

- Lorsqu'une personne conteste l'exactitude de certaines données à caractère personnel, celles-ci devront alors faire l'objet d'un traitement limité, le temps qu'elles soient vérifiées ;
- Lorsqu'une personne s'est opposée au traitement (et que ce traitement se fonde sur des intérêts légitimes), elle pourra demander que les données fassent l'objet d'un traitement limité, le temps que le responsable du traitement vérifie les bases juridiques du traitement ;
- Lorsque le traitement est illicite, mais que la personne s'oppose à l'effacement des données et qu'elle préfère demander que leur traitement soit limité ; et
- Lorsque le responsable du traitement n'a plus besoin des données, mais que celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de ses droits en justice.

Cette dernière hypothèse pourrait par exemple nécessiter que les responsables du traitement mettent en œuvre des solutions de stockage de données pour d'anciens clients, dans le cas où ces données seraient utiles à des procédures dans lesquelles la personne est impliquée.

Où puis-je trouver ces dispositions?

Droit à l'effacement des données
Article 17 et 19,
Considérants 65, 66, 73

Droit à la limitation du traitement
Article 18 et 19,
Considérants 67 et 73

Prise de décision automatisée

En bref

- Les règles relatives à la prise de décision automatisée sont similaires aux règles équivalentes prévues dans la Directive sur la protection des données.
- Les règles concernent les décisions :
  - prises uniquement sur la base d'un traitement automatisé ; et
  - qui produisent des effets juridiques ou d'autres effets significatifs similaires.
- Dès lors que la décision est :
  - nécessaire à la conclusion ou à l'exécution d'un contrat ; ou
  - autorisée par le droit de l'Union ou d'un État membre auquel le responsable du traitement est soumis ; ou
  - fondée sur le consentement explicite de la personne,
- le recours au traitement automatisé est alors autorisé. Néanmoins, des mesures appropriées destinées à protéger les intérêts de la personne doivent être mises en œuvre.
- Des restrictions supplémentaires interviennent lorsque la décision individuelle automatisée se fonde sur des données sensibles, qui nécessitent un consentement explicite, ou doivent être autorisées par le droit de l'Union ou d'un État membre s'agissant de motifs importants d'intérêt public.

A faire

- Vérifiez quels types de prise de décision automatisée sont utilisés. Identifiez toutes les décisions fondées sur
  - le consentement;
  - une autorisation légale;
  - ou qui concernent des données sensibles ou des enfants
- Si une décision individuelle automatisée est fondée sur le consentement, veillez à ce qu'il s'agisse d'un consentement explicite.
- Si la prise de décision automatisée est autorisée par la loi, vérifiez s'il s'agit du droit de l'Union ou de celui d'un État membre ; restez vigilants quant à la question de savoir si les États membres tenteront d'apporter des modifications à la loi afin de s'aligner sur le GDPR.
- Si une décision individuelle automatisée est fondée sur des données sensibles :
  - Vérifiez si vous pouvez obtenir un consentement explicite ;
  - Si ce n'est pas possible, vous devrez exercer une influence afin d'obtenir le soutien juridique de l'État membre (ou de l'Union) pour effectuer ce traitement.
- Si la prise de décision automatisée implique des enfants, sollicitez les conseils de juristes. Il s'agit d'une activité soumise à des restrictions.

Restrictions relatives à la prise de décision automatisée ayant des conséquences significatives

Les restrictions relatives aux décisions uniquement fondées sur un traitement automatisé (qui peuvent inclure le profilage), s'appliquent dès lors que les décisions produisent des effets juridiques concernant la personne en question ou qu'elles l'affectent de façon similaire et de manière significative. Le considérant 71 donne l'exemple des demandes de crédit en ligne et des pratiques de recrutement en ligne ; il énonce également clairement que l'élément répréhensible dans ces hypothèses n'est autre que l'absence d'intervention humaine.

Les personnes sont en droit de ne pas être soumises à de telles décisions. (Ceci peut être interprété soit comme l'interdiction d'un tel traitement, soit comme le fait que le traitement puisse avoir lieu mais que les personnes soient en droit de s'y opposer. Cette ambiguïté se retrouve également dans la Directive sur la protection des données, et les États membres ont des approches différentes à cet égard.)

Ce type de traitement automatisé significatif peut être utilisé à condition que celui-ci soit :

- nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;
- autorisé par le droit de l'Union ou d'un État membre ; ou
- fondé sur le consentement explicite de la personne concernée.

Décision individuelle automatisée fondée sur le consentement explicite ou l'exécution contractuelle

Dans le premier et le troisième cas (exécution du contrat et consentement), le responsable du traitement doit mettre en œuvre des mesures appropriées afin de protéger la personne concernée. Ceci doit inclure au minimum le droit d'obtenir une intervention humaine afin que la personne concernée soit en mesure d'exprimer son point de vue et de contester la décision.

Les dispositions équivalentes énoncées dans la Directive sur la protection des données indiquaient que ceci n'était pas nécessaire si l'effet de la décision consistait à faire droit à la demande de la personne.

Ces dispositions ne figurent pas dans le GDPR, dans la mesure où dans des contextes tels que celui de la finance ou de l'assurance, lorsqu'un contrat est proposé (même à des conditions difficiles), le responsable du traitement pourrait affirmer que la demande de la personne a été accordée, évitant ainsi la finalité des dispositions.

Le considérant 71 indique que des techniques statistiques appropriées doivent être utilisées ; que la transparence doit être garantie ; que des mesures doivent être mises en place afin de corriger les inexactitudes et les risques d'erreur ; que la sécurité doit être assurée et les effets discriminatoires évités.

Le considérant 71 indique également que ces mesures ne sauraient concerner les enfants.

Autorisation légale

Dans le deuxième cas (autorisation légale), la loi elle-même doit prévoir des mesures appropriées afin de sauvegarder les intérêts des personnes. Le considérant 71 indique que la prise de décision automatisée permettant de garantir la sécurité et la fiabilité des services, ou encore de contrôler et prévenir la fraude et l'évasion fiscale sont des types de décisions automatisées susceptibles d'être justifiées par le droit de l'Union ou d'un État membre.

Données sensibles

La prise de décision automatisée fondée sur des données sensibles est plus limitée. Les décisions fondées sur ce type de données peuvent uniquement être prises:

- sur la base d'un consentement explicite; ou
- lorsque le traitement est nécessaire pour un motif important d'intérêt public et conformément au droit de l'Union ou d'un Etat membre, qui doit intégrer des mesures destinées à protéger les intérêts des personnes concernées.

Où puis-je trouver ces dispositions?

Article 4 (4) et 22
Considérants 71 et 72

Obligations en matière de gouvernance des données

En bref

- Le GDPR impose à toutes les organisations de mettre en œuvre une large gamme de mesures afin de réduire les risques de violation du GDPR, et de prouver qu'elles prennent au sérieux la question de la gouvernance des données.
- Ceci inclut des mesures de responsabilité telles que: des études d'impact sur la vie privée, des audits, la révision des politiques relatives aux données personnelles, des rapports d'activité et (éventuellement) la désignation d'un délégué à la protection des données (DPO).
- Pour les organisations n'ayant pas encore attribué les responsabilités et défini un budget pour la mise en conformité aux règles relatives à la protection des données, ces obligations engendreront une lourde charge.

A faire

- ☐ Attribuez les responsabilités et un budget visant la mise en conformité aux règles relatives à la protection des données au sein de votre organisation. Que vous décidiez ou non de désigner un DPO (ou que vous en ayez l'obligation), la longue liste des mesures en matière de gouvernance des données prévue par le GDPR nécessite d'assumer les responsabilités afin de permettre la répartition des mesures à adopter.

A faire (suite)

- ☐ Identifiez clairement parmi les personnes auxquelles vous attribuez des responsabilités si celles-ci doivent être considérées comme des DPO (aux fins prévues par le GDPR) ou non, compte tenu des règles relatives aux conflits d'intérêt et aux protections accordées aux DPO par le GDPR.
- ☐ Prenez en considération les rapports hiérarchiques – les autorités de contrôle exigeront un accès direct à la Direction – et la description de poste pour les personnes désignées ayant la charge des responsabilités en matière de protection des données
- ☐ Veillez à ce qu'un programme complet de conformité soit établi pour votre organisation, et que celui-ci comprenne des éléments tels que : études d'impact sur la vie privée, audits réguliers, examens et mises à jour des politiques RH, programmes de formation et de sensibilisation.
- ☐ Auditez les accords existants conclus avec les fournisseurs, et mettez à jour les modèles de DP et les contrats d'approvisionnement afin de tenir compte des obligations des sous-traitants prévues par le GDPR.
- ☐ Surveillez les publications des autorités de contrôle/de l'UE, ainsi que les conditions et codes de bonne pratique des fournisseurs publiés par le secteur afin de vérifier s'ils sont appropriés à une utilisation au sein de votre organisation. Si vous êtes fournisseur, examinez l'impact des dispositions du GDPR sur votre structure de coûts, ainsi que sur votre responsabilité dans l'approbation de la légalité des activités de vos clients.
- ☐ Instaurez des mesures visant à préparer les registres des activités de traitement de votre organisation. Si vous êtes fournisseur, développez votre stratégie afin de traiter les demandes clients consistant à fournir une aide à la préparation de ce type de registres.

Le GDPR entérine plusieurs concepts de "gouvernance des données", dont les avantages ont été mis en évidence depuis un certain temps par les législateurs et les autorités de contrôle. Ces concepts créeront de nouvelles obligations et de nouveaux coûts opérationnels significatifs pour de nombreuses organisations publiques et privées.

Les responsables du traitement ont une obligation générale d'adopter des mesures techniques et organisationnelles visant à satisfaire aux obligations du GDPR (et doivent être capable de le démontrer). Le fait de gérer un programme d'audit régulier, en parallèle des autres mesures énoncées ci-dessous (notamment les études d'impact sur la vie privée), sera probablement accueilli positivement par les autorités de contrôle en charge de faire appliquer les obligations du GDPR.

Figurent parmi les obligations clés :

Protection des données dès la conception - "Privacy by Design"

Les organisations doivent mettre en œuvre des mesures techniques et organisationnelles visant à prouver qu'elles ont pris en considération et intégré, dans leurs activités de traitement, des mesures permettant de respecter les règles en matière de protection des données.

L'adoption de politiques du personnel appropriées est expressément mentionnée, tout comme le recours à la pseudonymisation (afin de garantir le respect du principe de minimisation des données).

Etudes d'Impacts sur la Vie Privée "EIVP" ("Privacy Impact Assessment" - PIA)

Une EIVP est une évaluation destinée à identifier et à minimiser les risques de non-conformité. Bien que ce concept ne soit pas nouveau, les directives actuelles des régulateurs recommandent son utilisation, et Bird & Bird a réalisé des EIVP pour plusieurs de ses clients, le GDPR formalise l'obligation de réaliser des EIVP.

Plus précisément, les responsables du traitement doivent veiller à ce qu'une EIVP ait été effectuée avant toute activité de traitement susceptible d'engendrer un *"risqué élevé"* pour les droits et libertés des personnes physiques.

Le traitement *"à grande échelle"* de données sensibles, ou les activités de profilage, sont cités (de manière non exhaustive) à titre d'exemples de traitement à risque élevé. Les autorités de contrôle publieront des informations complémentaires contenant davantage d'exemples et de recommandations.

Au minimum, le GDPR exige qu'une EIVP contienne:

- Une description: des activités de traitement et de leur finalité;
- Une évaluation: de la nécessité et de la proportionnalité du traitement, des risques en découlant et des mesures adoptées pour atténuer ces risques, notamment les garanties et les mesures de sécurité destinées à protéger les données à caractère personnel et à se conformer au GDPR.

Si un DPO a été nommé (voir ci-dessous), son avis sur l'élaboration de l'EIVP doit être sollicité.

Une autorité de contrôle doit être consultée avant de démarrer un traitement lorsque l'EIVP a identifié que celui-ci présente un niveau élevé de risques non atténués. Dans une telle situation, le GDPR indique la marche à suivre.

Dans le cadre de la conduite d'une EIVP, les responsables du traitement doivent solliciter l'avis des personnes concernées *"ou de leurs représentants"*, le cas échéant. Dans le cadre du traitement de données RH, ceci sera probablement interprété comme une obligation de consulter les instances représentatives du personnel.

Délégué à la protection des données ("Data Protection Officer" - DPO)

Les responsables du traitement et les sous-traitants sont libres de désigner un DPO, sachant toutefois que les acteurs suivants en ont l'obligation:

- Les autorités publiques (avec quelques exceptions mineures);
- Toute organisation dont les activités de base nécessitent:
  - *un "suivi régulier et systématique" des personnes « à grande échelle";* ou
  - *un traitement "à grande échelle" de données sensibles ou de données relatives à des condamnations pénales ou infractions;* et
- Les acteurs étant contraints de le faire en vertu de la législation locale (les États comme l'Allemagne entreront probablement dans cette catégorie).

Les lignes directrices du G29 publiées en décembre 2016 ont pour objectif d'aider les organisations à interpréter le terme d' "activités de base", "suivi régulier et systématique" et de "grande échelle". Elles incluent les points suivants:

- *"Activités de base":* sont citées les activités qui font "partie intégrante" de la poursuite des objectifs du responsable du traitement ou du sous-traitant. Ces recommandations confirment, de manière rassurante, que le traitement par une organisation de données à caractère personnel de ses employés (qui est grandement susceptible d'inclure des données sensibles) est accessoire à ses activités et ne constitue pas une activité de base. Les exemples d'activités de base incluent notamment la surveillance de la sécurité d'une entreprise dès lors qu'elle est embauchée pour protéger un espace public, le traitement effectué par un hôpital de données relatives à la santé de patients et le traitement d'un prestataire externe de services de santé des données clients de ses employés.

- *"Suivi régulier et systématique":* toutes les formes de suivi et de profilage en ligne sont citées comme exemples par le G29, y compris pour des finalités de publicité comportementale et d'email de "reciblage" dit retargeting. Les autres exemples cités incluent le profilage et l'évaluation (par exemple, l'évaluation des crédits, la prévention de la fraude ou la mise en place d'assurance premiums) ; suivi de localisation ; suivi des données relatives à l'aptitude physique et à la sante ; système de vidéosurveillance et le traitement de données par des objets connectés (compteurs intelligents, voitures intelligentes, etc.).

- *"Grande échelle":* Dans ses lignes directrices, le G29 indique qu'il ne souhaite pas que des chiffres précis soient utilisés comme références pour ce terme mais qu'il est sur le point de publier des seuils pour l'avenir. A la place, les recommandations de décembre 2016 listent quelques facteurs généraux évidents à prendre en compte pour définir la notion de grande échelle (par exemple, le nombre de personnes concernées et l'étendue géographique du traitement). Des exemples de traitement à grande échelle cités comprennent : le traitement de données clients par une banque ou entreprise d'assurance ; le traitement par une chaine de fast-food internationale des données de géolocalisation des clients en temps réel à des fins statistiques réalisé par un responsable de traitement spécialisé.

Les lignes directrices du G29 confirme que dès lors qu'un DPO est désigné volontairement, les mêmes obligations, telles que prévues par le GDPR pour les DPO devant être désignés obligatoirement, seront applicables (notamment les points résumés ci-dessous). De manière intéressante, le G29 recommande également qu'une organisation qui décide de ne pas désigner volontairement un DPO documente les raisons pour lesquelles cette organisation estime qu'elle n'est pas soumise à l'obligation de désigner un DPO (tel que résumé ci-dessous).

Si la désignation d'un DPO n'est pas obligatoire et qu'un DPO n'est pas désigné volontairement, un membre du personnel ou un consultant peut être désigné pour effectuer des tâches similaires. Néanmoins, le G29 indique que pour éviter toute confusion, cette personne ne devra pas être nommée DPO.

Si un DPO est désigné, il doit l'être en fonction de ses qualités professionnelles et de son expertise (qui doivent être obligatoirement entretenues avec l'aide de son employeur). Les lignes directrices du G29 indiquent que plus les activités de traitement de données à caractère personnel sont sensibles ou complexes, plus il est attendu du DPO un haut niveau d'expertise.

Les organisations doivent s'assurer que la finalité première de leur DPO soit de garantir la conformité au GDPR. Ses missions doivent inclure au minimum : le conseil auprès de ses collègues et la surveillance de la conformité de son organisation au GDPR, au droit de la protection des données personnelles et aux règles internes, y compris via la formation et la sensibilisation, la réalisation d'audits, le conseil sur les EIVP, ainsi que la coopération avec les autorités de contrôle. Les recommandations du G29 mentionnées ci-dessus insistent sur le fait que les DPO ne seront pas tenus personnellement responsable du manquement de leur organisation à se mettre en conformité avec le GDPR. La responsabilité incombe à l'organisation, notamment si celle-ci entrave ou échoue à soutenir le DPO dans la réalisation des objectifs premiers de celui-ci.

Des ressources appropriées doivent être fournies afin que le DPO puisse remplir ses obligations conformément au GDPR, et il doit directement reporter au niveau le plus élevé de la direction.

Les groupes d'entreprises peuvent désigner un seul DPO. Un DPO peut être soit un membre du personnel, soit un prestataire extérieur. Les lignes directrices du G29 indiquent que les principales caractéristiques des compétences d'un DPO incluent qu'ils doivent être bien informés de l'organisation qu'ils représentent et qu'ils doivent être accessibles, en ce compris qu'ils doivent être capable de communiquer aisément avec les autorités de contrôle et les personnes concernées (par exemple, les clients et le personnel) dans les pays dans lesquels l'organisation opère. Il semblerait que le G29 s'attende à ce que les DPO soient à la fois multilingues et expert en matière de protection des données personnelles ou qu'ils aient accès facilement à des services de traduction.

Les responsables du traitement et les sous-traitants doivent s'assurer que leur DPO soit impliqué dans toutes les problématiques relatives à la protection des données personnelles (y compris, selon les lignes directrices du G29, à la suite d'une violation des donnée), qu'il soit en mesure d'agir indépendamment et ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions, et qu'il ne soit pas relevé ou pénalisé pour l'exercice de celles-ci. Reste à savoir la manière dont le droit du travail interprétera cette disposition.

Les recommandations du G29 indiquent également que si la direction d'une organisation n'est pas d'accord avec les recommandations du DPO et décide de ne pas les suivre, elle doit formellement enregistrer cette décision et en expliquer les raisons. Les lignes directrices avertissent également qu'il ne peut être donné d'instructions au DPO concernant la manière dont il gère une problématique, les résultats qui doivent être atteints ou s'il doit consulter ou non une

autorité de contrôle, ce qui est susceptible de donner lieu à des échanges potentiellement intéressants à la suite d'une violation des données.

Le GDPR n'interdit pas les DPO à exercer d'autres fonctions mais exige expressément que les organisations s'assurent que ces autres fonctions ne donnent pas lieu à un conflit d'intérêts pour le DPO. Les lignes directrices du G29 vont plus loin. Elles indiquent qu'un DPO ne peut pas exercer une position qui le conduirait à déterminer les finalités et les moyens d'un traitement de données à caractère personnel. Il reste à voir si les régulateurs estimeront que les RSSI peuvent également exercer le rôle de DPO mais ces recommandations mettent en doute leur capacité à cumuler ces fonctions.

Les coordonnées du DPO doivent être publiées et communiquées à l'autorité de contrôle dans la mesure où le DPO constitue le point de contact s'agissant des questions relatives au respect des règles en matière de protection des données.

Recours à des prestataires de services (sous-traitants)

Le GDPR impose aux responsables du traitement un lourd devoir de vigilance lors du choix de leurs prestataires de services de traitement de données à caractère personnel, ce qui impliquera une évaluation régulière des processus d'approvisionnement et des demandes de dossiers d'appel d'offre.

Des contrats devront être établis avec les prestataires de services et contenir un certain nombre d'informations (ex: les données traitées et la durée du traitement) et obligations (ex: l'assistance lors de la survenance d'une violation de sécurité, les mesures techniques et organisationnelles devant être prises, et les obligations d'assistance en matière d'audits). Ces mêmes obligations s'appliquent dès lors qu'un prestataire de services a lui-même recours à un sous-traitant.

La Commission et les autorités de contrôle publieront probablement une version approuvée des clauses contractuelles relatives aux prestataires de services. Il faut s'attendre à ce que cela s'avère onéreux du point de vue des prestataires de services. L'approche de ces derniers en matière de tarification des prestations devra ainsi être revue.

Registre des activités de traitement

Les organisations sont dans l'obligation de tenir un registre de leurs activités de traitement (type de données traitées, finalités de leur utilisation, etc.) similaire aux enregistrements auxquels les responsables du traitement doivent procéder en vertu des législations actuelles, auprès des autorités de contrôle.

Les sous-traitants sont également tenus de tenir un tel registre relatif aux données à caractère personnel que les responsables du traitement les chargent de traiter, une obligation qui constituera un véritable défi pour de nombreux prestataires de services de cloud et de communications.

Bien qu'une exemption des obligations mentionnées ci-dessus s'applique aux organisations employant moins de 250 personnes, cette exemption ne saurait s'appliquer dans le cadre de traitement de données sensibles, ce qui devrait probablement anéantir l'utilité d'une telle exemption.

Où puis-je trouver ces dispositions?

Protection des données dès la conception
Article 25
Considérants 74-78

EIVP
Articles 35-36
Considérants 89 - 94

DPO
Articles 37-39
Considérant 97, Avis G29 243

Recours aux sous-traitants
Article 28 et 29
Considérant 81

Registre des activités de traitement
Article 30
Considérant 82

Violations de données à caractère personnel et notification

En bref

- Les responsables du traitement et sous-traitants sont désormais soumis à un régime général de notification des violations de données à caractère personnel.
- Les sous-traitants sont tenus de déclarer auprès des responsables du traitement toute violation de données à caractère personnel.
- Les responsables du traitement sont tenus de déclarer toute violation de données à caractère personnel auprès de leur autorité de contrôle, et dans certains cas, auprès des personnes concernées, en respectant dans chaque cas des dispositions spécifiques prévues par le GDPR.
- Les responsables du traitement doivent tenir un registre interne des violations.
- Tout manquement est susceptible d'entraîner une amende administrative pouvant atteindre 10 000 000 €, ou dans le cas d'une entreprise, 2 % de son chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé devant être retenu.
- En l'état actuel des choses, le régime spécifique de notification des violations applicable aux fournisseurs de services de communications, énoncé dans le Règlement 611/2013, demeure applicable.

A faire

- ☐ Conformément au principe de responsabilité – "accountability" - énoncé par le GDPR, les responsables du traitement et les sous-traitants doivent développer et mettre à jour leurs procédures internes de notification des violations, notamment leurs systèmes d'identification des incidents et leurs plans de réponse aux incidents.
- ☐ Ces procédures devront être régulièrement testées et réexaminées.
- ☐ Travaillez aux côtés de vos équipes IT/SI et assurez-vous qu'elles mettent en œuvre les mesures techniques et organisationnelles appropriées afin de rendre les données inintelligibles en cas d'accès non autorisé.
- ☐ Les polices d'assurance doivent être revues afin d'évaluer l'étendue de leur couverture en cas de violations.
- ☐ Les modèles de clauses MSA/de protection des données et de dossiers d'appel d'offre doivent être actualisés par les clients, notamment: (i) pour exiger des prestataires qu'ils leur notifient de manière proactive les violations; et afin de (ii) mettre tout particulièrement l'accent sur l'obligation de coopérer entre les parties concernées.

Degré de changement

Incidents déclenchant une notification

En cas d'incident défini comme *"une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données"*, le nouveau régime de notification des violations prévu par le GDPR s'appliquera comme suit :

1. Obligation imposant aux sous-traitants de notifier les responsables du traitement

Délais:

Dans les meilleurs délais après en avoir eu connaissance.

Exemption:

Aucune exemption prévue par le GDPR (sachant toutefois que le CEPD a été chargé d'émettre des directives concernant les *"circonstances particulières dans lesquelles un responsable du traitement ou un sous-traitant est tenu de notifier la violation de données à caractère personnel").*

Observations :

- Toutes les violations devront être déclarées.
- Le CEPD publiera des lignes directrices afin de clarifier la notion de "dans les meilleurs délais" ainsi que les circonstances particulières dans lesquelles un sous-traitant sera tenu de notifier une violation de données à caractère personnel.

2. Obligation imposant aux responsables du traitement de notifier l'autorité de contrôle

Délais:

Dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance.

Exemption:

Pas de notification si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Observations:

- Dès lors que le délai de notification n'est pas respecté, les motifs de ce retard devront être fournis à l'autorité de contrôle (ex : demande de la part d'une autorité répressive)
- Le CEPD publiera des lignes directrices afin de clarifier la notion de "dans les meilleurs délais" ainsi que les circonstances particulières dans lesquelles un responsable du traitement sera tenu de notifier une violation de données à caractère personnel

3. Obligation imposant aux responsables du traitement de notifier les personnes concernées

Si le responsable du traitement ne l'a pas encore fait, l'autorité de contrôle pourra imposer au responsable du traitement de notifier les personnes concernées, à moins que l'une des trois exemptions soit satisfaite.

Délais:

Dans les meilleurs délais: la nécessité d'atténuer un risque immédiat de dommage exigerait la notification sans délai des personnes concernées, étant toutefois entendu que la nécessité de mettre en œuvre des mesures appropriées contre les violations de données continues ou similaires est susceptible de justifier un plus long délai.

Exemption:

Aucune communication si:

- La violation de données à caractère personnel n'est pas susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques;
- Des mesures appropriées de protection techniques et organisationnelles étaient en place au moment de l'incident (ex., données chiffrées); ou
- Cette communication impliquerait des efforts disproportionnés (dans ce cas, une campagne publique d'information ou une "mesure similaire" devra être envisagée afin que les personnes concernées puissent être informées de manière efficace)

Obligations en matière de documentation

- Registre des violations internes: obligation incombant au responsable du traitement de documenter tout incident *"en indiquant les faits concernant la violation de données personnelles, ses effets et les mesures prises pour y remédier".* Il peut être demandé à l'autorité de contrôle d'évaluer la manière dont les responsables du traitement se conforment à leurs obligations de notification de violations de données.

- Plusieurs exigences prescrites doivent également être respectées dans le cadre des communications à l'autorité de contrôle (ex: description de la nature de la violation de données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif d'enregistrements de données concernés, etc.) ainsi que des communications auprès des personnes concernées (ex: décrire en des termes clairs et simples la nature de la violation de données à caractère personnel, et fournir au minimum les informations suivantes: (i) le nom et les coordonnées du Délégué à la Protection des Données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues; (ii) les conséquences probables de la violation de données à caractère personnel; et (iii) les mesures proposées ou prises par le responsable du traitement afin de remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives).

Sanctions en cas de non-conformité

Le non-respect des obligations décrites ci-dessus expose l'organisation à une amende administrative pouvant atteindre 10 000 000 €, ou dans le cas d'une entreprise, 2 % de son chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Qu'en est-il de l'autre régime européen de notification des violations relatif aux fournisseurs de services de communication?

En l'état actuel des choses, le Règlement 611/2013, qui détaille la procédure spécifique applicable aux notifications de violations (énoncée dans la Directive 2002/58/CE, la "Directive vie privée et communications électroniques", telle qu'amendée) demeure applicable aux fournisseurs de services de communications électroniques au public (ex: sociétés de télécommunications, FAI et fournisseurs de messagerie électronique). Toutefois, la Commission européenne a publié le 10 janvier 2017 une proposition de Règlement visant à remplacer la Directive vie privée et communications électronique.

Le fait que ce nouveau Règlement entrera en vigueur à la même date que le GDPR, soit le 25 mai 2018, symbolise l'intention d'une relation harmonieuse entre ces deux Règlements. Le texte remplace la Directive vie privée et communications électroniques mais contient une formulation très similaire à celle applicable en matière de notification des violations en vertu de cette Directive. Cela étant dit, le texte de ce nouveau Règlement ne remplace pas le Règlement 611/2013. Par conséquent, techniquement, les fournisseurs de services de télécommunications devront notifier les violations de données à l'autorité de protection des données compétente en application du régime établi par le Règlement 611/2013 et non celui prévu par le GDPR. Toutefois, nous estimons qu'à un certain moment, le Règlement 611/2013 sera remplacé par le régime prévu par le GDPR.

Où puis-je trouver ces dispositions?

Articles 33, 34, 70, 83 et 84 *Considérants 85 - 88*

Codes de conduite et certifications

En bref

Le GDPR prévoit des dispositions relatives à l'approbation de codes de conduites ("Codes") et à l'octroi de certifications, de marques et de labels destinés à aider les responsables du traitement et les sous-traitants à prouver leur conformité et leurs bonnes pratiques.

Codes de conduite :

- Les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent préparer des Codes qui seront soumis à l'approbation, à l'enregistrement et à la publication par une autorité de contrôle ou, par le Comité Européen de Protection des Données ("CEPD") si des activités de traitement sont menées dans plusieurs Etats membres. La Commission européenne peut décider que les Codes qui lui ont été soumis par le CEPD seront d'application générale au sein de l'UE.
- Les Codes pourraient être approuvés dans un large éventail de domaines, et l'application de ces Codes contribuera à aider les responsables du traitement et les sous-traitants à prouver leur conformité aux obligations prévues par le GDPR.
- Le respect des Codes fera l'objet d'un contrôle, qui sera effectué par des organismes agréés disposant d'un niveau d'expertise approprié. Les responsables du traitement et les sous-traitants dont on détermine qu'ils ont violé un code applicable pourront être suspendus de l'application du Code et signalés à l'autorité de contrôle.

En bref (suite)

Certifications, marques et labels :

- L'élaboration de mécanismes de certification en matière de protection des données, ainsi que de marques et labels doit être encouragée.
- Des certifications seront délivrées par des organismes de certification agréés (qu'il reste encore à établir).
- La certification est volontaire, mais elle permettra aux responsables du traitement et aux sous-traitants de prouver leur conformité avec le GDPR.
- Les certifications seront valables pour une durée de trois ans renouvelable.
- Le CEPD tiendra un registre accessible au public, qui contiendra tous les mécanismes de certification, les marques et les labels

A faire

Codes de conduite

- Afin de prendre une longueur d'avance sur les procédures d'accréditation qui seront établies par les autorités de contrôle, les sous-traitants (tels que les prestataires de services cloud) et les responsables du traitement évoluant dans des secteurs spécifiques ont tout intérêt à identifier, ou à créer, des associations ou autres organismes représentatifs susceptibles d'élaborer des Codes, qui seront soumis à l'approbation des autorités de contrôle.

Certifications, marques et labels

- Les sous-traitants et responsables du traitement ont tout intérêt à suivre les avancées relatives à l'accréditation des organismes de certification, et à déterminer s'ils souhaiteront ou non déposer une demande de certification en temps voulu.

- Dès lors que les programmes de certification auront été établis, les responsables du traitement devront se familiariser avec les programmes en question et prendre en considération les certifications, marques et labels au moment de choisir leurs sous-traitants/prestataires de services

Codes de conduite

Les Codes constituent un aspect important de l'élargissement et l'adaptation des outils de conformité en matière de protection des données sur lesquels pourront s'appuyer les responsables du traitement et les sous-traitants, via un mécanisme *"semi-auto-régulé"*.

Les Codes devraient fournir des directives faisant autorité dans certains domaines clés, parmi lesquels:

- l'intérêt légitime dans des contextes spécifiques;
- la pseudonymisation;
- l'exercice des droits des personnes;
- la protection des mineurs et les modalités du consentement parental;
- la mise en œuvre appropriée des principes de "privacy by design" (protection de la vie privée dès la conception) et de "privacy by default" (protection de la vie privée par défaut), et de mesures de sécurité;
- la notification des violations de sécurité; et
- la résolution des litiges entre les responsables du traitement et les personnes concernées.

L'élaboration et l'approbation des Codes devraient offrir un certain nombre d'avantages, parmi lesquels:

- l'établissement et l'actualisation des bonnes pratiques en matière de conformité dans des contextes spécifiques de traitement;
- permettre aux responsables du traitement et aux sous-traitants de s'engager à respecter les normes et pratiques officielles, et d'en être à cet égard reconnus;
- l'application des Codes peut prouver que les importateurs de données (responsables du traitement et sous-traitants) basés en dehors de l'UE/EEE ont mis en place des garanties appropriées à fin d'autoriser les transferts prévus par l'article 46. Les transferts effectués sur la base d'un code de conduite approuvé et assorti de l'engagement contraignant et exécutoire pris par l'importateur de données d'appliquer les garanties appropriées, pourront avoir lieu sans autorisation spécifique de la part d'une autorité de contrôle. Les Codes feraient ainsi office de mécanisme alternatif destiné à la gestion des transferts internationaux, en s'inscrivant au même niveau que les clauses contractuelles types et les BCR (règles d'entreprise contraignantes).

Approbation des Codes

Les Codes proposés par les associations ou autres organismes représentatifs en lien avec des activités de traitement de données concernant uniquement un État membre devront être soumis à l'autorité de contrôle compétente pour avis et, sous réserve d'éventuelles modifications ou prorogations, approbation. Si un Code couvre des activités de traitement menées dans plusieurs États membres, il devra être soumis à l'avis du CEPD. Sous réserve d'éventuelles modifications ou prorogations, le Code et l'avis du CEPD pourront ensuite être présentés à la Commission européenne qui, à l'issue d'un examen officiel, pourra se prononcer sur son applicabilité générale.

Les Codes sont conservés et mis à disposition dans des registres accessibles au public.

Contrôle du respect des Codes

Le contrôle du respect des Codes sera mené exclusivement par les organismes agréés par l'autorité de contrôle compétente.

Afin d'être agréés, ces organismes devront prouver:

- leur indépendance et leur expertise;
- qu'ils ont établi des procédures destinées à évaluer la capacité des responsables du traitement et des sous-traitants à appliquer le Code, à en contrôler le respect, ainsi qu'à réviser le Code de manière régulière;
- leur capacité à gérer les réclamations relatives aux violations; et
- qu'ils ont mis en œuvre des processus destinés à éviter les conflits d'intérêt.

Les agréments sont révocables si les conditions d'agrément ne sont plus remplies.

Certifications, marques et labels

Le concept de certification des activités de traitement de données constitue une avancée significative dans la création d'un cadre fiable et contrôlable pour les activités de traitement de données. Ceci devrait s'avérer particulièrement pertinent dans le cadre du Cloud computing et d'autres formes de services à localisations multiples, pour lesquels les audits individuels ne sont généralement pas faisables en pratique.

Les États membres, les autorités de contrôle, le CEPD et la Commission sont tous encouragés à établir des mécanismes de certification en matière de protection des données ainsi que des marques et des labels pour des activités de traitement spécifiques.

Les certifications sont volontaires. L'autorité de contrôle compétente et le CEPD approuveront les critères relatifs aux certifications. Le CEPD pourra élaborer des critères pour une certification commune : le "Label Européen de Protection des Données".

Ces certifications présentent deux avantages clés:

1. les responsables du traitement et les sous-traitants seront en mesure de prouver leur conformité, notamment concernant la mise en œuvre de mesures techniques et organisationnelles.

2. les certifications peuvent prouver que les importateurs de données (responsables du traitement et sous-traitants) basés en dehors de l'UE/EEE ont mis en place des garanties appropriées aux fins de l'article 46. Les transferts effectués sur la base d'un mécanisme de certification approuvé et assorti de l'engagement contraignant et exécutoire pris par l'importateur de données d'appliquer les garanties appropriées pourront avoir lieu sans autorisation spécifique de la part d'une autorité de contrôle. Les Certificats offriront ainsi un mécanisme alternatif destiné à la gestion des transferts internationaux, en s'inscrivant au même niveau que les clauses contractuelles types et les BCR (règles d'entreprise contraignantes).

Les certifications des opérations de traitement de données à caractère personnel seront délivrées pour une période de trois ans, et pourront être renouvelées ou retirées si les conditions d'octroi des certifications ne sont plus remplies.

Le CEPD tient un registre accessible au public, qui contient tous les mécanismes de certification, tous les labels et toutes les marques en matière de protection des données.

Les certifications peuvent être délivrées par des organismes de certification agréés, publics ou privés. Les organismes nationaux d'accréditation et/ou les autorités de contrôle pourront agréer les organismes de certification (afin qu'ils puissent délivrer des certifications, des labels et des marques) qui, notamment:

- possèdent l'expertise requise et sont indépendants au regard de l'objet de la certification;
- disposent de procédures permettant d'examiner périodiquement et de retirer les certifications, les marques et les labels;
- sont capables de gérer les réclamations relatives aux violations des certifications; et
- disposent de règles visant à gérer les conflits d'intérêt.

Les critères d'agrément seront élaborés par les autorités de contrôle ou le CEPD, et seront accessibles au public.

Les agréments des organismes de certification seront délivrés pour une durée maximum de cinq ans, et pourront être renouvelés ou retirés si les conditions d'octroi de l'agrément ne sont plus remplies.

Où puis-je trouver ces dispositions?

Codes de conduite
Articles 24, 28(5), 32, 40, 41, 57, 58, 64, 70, 83
Considérants 77, 81, 98, 99, 148, 168.

Certifications, marques et labels
Articles 24, 25, 28, 32, 42, 43
Considérants 77, 81, 100, 166 et 168

Transferts de données à caractère personnel

En bref

- Les transferts de données à caractère personnel vers des destinataires situés dans des “pays tiers” (c.-à-d. en dehors de l’Espace économique européen (“EEE”)) demeurent réglementés et restreints dans certains cas.
- Les obligations du GDPR sont globalement similaires à celles imposées par la Directive sur la protection des données, et prévoient certaines améliorations, notamment la suppression de l’obligation de notifier les clauses contractuelles types auprès des autorités de contrôle, et l’encouragement de l’élaboration de codes de pratique adéquats en matière de transferts et de schémas de certification.
- Le respect des obligations en matière de transfert des données demeurera une question importante pour les organisations multinationales, ainsi que pour toutes celles recourant à des chaînes logistiques traitant des données à caractère personnel en dehors de l’EEE.
- La violation des dispositions du GDPR en matière de transfert de données figure dans la liste des domaines de non-conformité, pour lesquels le niveau maximum d’amende peut être imposé (jusqu’à 4 % du chiffre d’affaires annuel mondial).
- En cas de manquement, des poursuites peuvent être engagées à l’encontre des responsables du traitement et/ou des sous-traitants.

A faire

- ☐ Examinez et cartographiez les principaux flux internationaux de données.
- ☐ Examinez les mécanismes de transfert de données que vous avez mis en place et déterminez si ceux-ci demeureront appropriés.
- ☐ Examinez les contrats standards de fournitures de services et les clauses contractuelles afin de vous assurer que les informations relatives au transfert de données à caractère personnel de votre fournisseur, dont vous êtes responsable, sont appréhendées et gérées de manière conforme.
- ☐ Si vous-même ou vos fournisseurs recouriez/recouraient précédemment à la certification *Safe Harbor* pour garantir la légalité des transferts, cette démarche n’est désormais plus valide. Cela étant dit, vous pouvez envisagez d’obtenir une certification en vertu du “Privacy Shield”, également appelé le “bouclier de protection des données UE – Etats-Unis”. En toute hypothèse, il vous faudra revoir vos relations avec vos prestataires de services et/ou clients afin d’établir une nouvelle base juridique qui justifiera les transferts de données transatlantiques en cours.
- ☐ S’agissant des transferts de données au sein d’un groupe, déterminez si les BCR pourraient constituer une option viable.
- ☐ Si vous transférez des données à caractère personnel en dehors de l’EEE pour fournir des biens ou des services, préparez-vous à recevoir des questions de la part de vos clients s’agissant de votre approche (ou de l’approche de vos prestataires) en matière de transferts.
- ☐ Surveillez les avancées relatives aux codes de conduite approuvés et aux schémas de certification appliqués dans le cadre des activités d’une organisation.

Commentaire

Les transferts de données à caractère personnel vers des "pays tiers" (c.-à-d. situés en dehors de l'EEE) continuent d'être soumis à des restrictions en vertu du GDPR. Ceci demeurera une question importante pour toutes les organisations multinationales. Néanmoins, les exigences actuelles demeureront globalement en place, avec quelques améliorations.

La principale amélioration réside dans le fait que le processus actuel, au titre duquel les transferts basés sur des clauses contractuelles types doivent être notifiés ou approuvés par les autorités de protection des données, est supprimé.

La Commission aura le pouvoir de déterminer quels sont les pays, territoires, secteurs spécifiques ou organisations internationales qui offrent un niveau de protection adéquat en matière de transferts de données. La liste existante de pays ayant précédemment été approuvés par la Commission comme offrant un niveau de protection adéquat restera applicable, à savoir: l'Andorre, l'Argentine, le Canada (où la LPRPDE s'applique), la Suisse, les îles Féroé, Guernesey, Israël, l'île de Man, Jersey, la République orientale de l'Uruguay, et la Nouvelle-Zélande. Les pays qui seront ajoutés ou retirés de cette liste seront publiés au Journal Officiel.

Précédemment approuvé par la Commission, le régime américain de Safe Harbor n'est désormais plus valide. Toutefois, le 12 juillet 2016, seulement 9 mois après l'invalidation du Safe Harbor, la Commission Européenne a formellement adopté une décision d'adéquation visant à reconnaitre au mécanisme de "Privacy Shield UE-Etats-Unis" un niveau de protection équivalent aux exigences européennes. Les organisations américaines peuvent adhérer aux standards prévus par le *Privacy Shield* depuis le 1er août 2016. Le *Privacy Shield* donne à la Commission Européenne la possibilité d'effectuer des révisions périodiques afin d'évaluer le niveau de protection prévu par le *Privacy Shield* à la suite de l'entrée en vigueur du GDPR. Il n'est pas fait mention du *Privacy Shield* dans le GDPR, bien que celui-ci inclut les exigences essentielles permettant d'évaluer le caractère adéquat telles qu'énoncées dans la décision *Schrems.*

Le GDPR est plus précis quant aux procédures et critères particuliers que la Commission doit prendre en considération lorsqu'elle évalue le caractère adéquat, et en particulier la nécessité que le pays tiers offre des garanties pour assurer un niveau adéquat de protection *"essentiellement équivalent à celui qui est garanti dans l'Union"*, et qu'il offre aux personnes concernées des droits effectifs et opposables ainsi que des voies de recours. La Commission doit consulter le CEPD lors de l'évaluation des niveaux de protection, et garantir qu'il existe un contrôle et une révision continus de toutes les décisions d'adéquation prises (au moins tous les quatre ans). La Commission a également le pouvoir d'abroger, de modifier ou de suspendre toute décision d'adéquation.

D'autres mécanismes de transfert des données à caractère personnel demeurent reconnus: les clauses contractuelles types (adoptées par la Commission, ou adoptées par une autorité de contrôle puis approuvées par la Commission) demeureront une option, et les ensembles existants de clauses approuvées demeureront en vigueur.

L'utilisation d'autres garanties appropriées, telles que les règles d'entreprise contraignantes (BCR) et les instruments juridiquement contraignants et exécutoires entre des autorités publiques, sera également acceptée.

Aspect significatif, les transferts seront autorisés dès lors qu'un code de conduite approuvé (conformément au nouveau régime énoncé à l'article 40) ou qu'un mécanisme de certification approuvé (conformément au nouveau régime énoncé à l'article 42) sera utilisé, sous réserve que des engagements contraignants et exécutoires soient pris, par le responsable du traitement ou le sous-traitant dans le pays tiers, d'appliquer les garanties appropriées, notamment à l'égard des droits des personnes concernées. Il sera également convenu d'autres dispositions relatives aux garanties ad hoc, sous réserve de l'autorisation de l'autorité de contrôle compétente.

S'agissant des BCR, le GDPR inscrit dans la loi les obligations actuelles relatives aux BCR à l'égard des responsables du traitement et des sous-traitants. Elles seront toujours soumises à l'approbation de l'autorité de contrôle compétente, mais conformément à un mécanisme de contrôle de la cohérence. Ceci se révélera utile dans les quelques États membres qui ne sont toujours pas en mesure d'accepter les BCR.

Un certain nombre de dérogations persiste concernant l'autorisation des transferts de données à caractère personnel dans des circonstances limitées, qui sont similaires aux dérogations existantes, et comprennent : le consentement explicite, la nécessité contractuelle, les motifs importants d'intérêt public, les actions en justice, les intérêts vitaux, ainsi que les données de registres publics. Une nouvelle dérogation (limitée) est prévue concernant les transferts non répétitifs impliquant un nombre limité de personnes concernées, lorsque le transfert est nécessaire aux fins des intérêts légitimes impérieux poursuivis par les responsables du traitement (qui ne prévalent pas sur les intérêts ou les droits de la personne concernée) et si le responsable du traitement a évalué (et documenté) toutes les circonstances entourant le transfert de données, et a conclu à l'existence d'une adéquation. Le responsable du traitement doit informer l'autorité de contrôle et les personnes concernées dès lors qu'il s'appuie sur cette dérogation.

Disposition très attendue, le GDPR établit enfin clairement le caractère illégal du transfert de données à caractère personnel en dehors de l'EEE en réponse à une exigence légale émanant d'un pays tiers, à moins que cette exigence soit fondée sur un contrat international ou si un autre fondement pour le transfert s'applique.

Où puis-je trouver ces dispositions?

Articles 40-45
Considérants 78-91

Désignation des Autorités de contrôle

En bref

- Les autorités nationales de protection des données continueront d'exister.
- Elles doivent coopérer ensemble et avec la Commission européenne afin de contrôler l'application du GDPR.
- Elles doivent exercer en toute indépendance.
- Les membres des autorités de contrôle doivent être nommés suivant une procédure transparente pour le public et posséder les compétences nécessaires en matière de protection des données.

A faire

Aucune action n'est requise (à moins que vous soyez membre d'une autorité de protection des données existante ou que vous fassiez partie du personnel de cette autorité!)

Degré de changement

Commentaire

Les autorités nationales de protection des données (autorités de contrôle) continueront d'exister. Leur mission consiste à surveiller l'application du GDPR afin de préserver les droits fondamentaux en lien avec le traitement de données à caractère personnel et de faciliter la libre circulation des données à caractère personnel au sein de l'UE.

Elles doivent coopérer ensemble et avec la Commission européenne afin de contribuer à l'application cohérente du GDPR.

Bien que les États, à l'instar de l'Allemagne, puissent conserver plus d'une autorité de contrôle, l'une de ces autorités doit être désignée en tant que représentante auprès du nouveau Comité Européen de Protection des Données ("CEPD").

Chaque Etat membre doit notifier à la Commission européenne les dispositions légales qu'il adopte concernant l'établissement et la désignation de l'autorité de contrôle.

Les autorités de contrôle doivent exercer en toute indépendance (mais soumises à des contrôles financiers et à une surveillance judiciaire). Les membres des autorités de contrôle doivent demeurer libres de toute influence extérieure, et ne solliciter ni n'accepter d'instructions de quiconque. Ils doivent s'abstenir de tout acte incompatible avec leurs fonctions et, pendant toute la durée de leur mandat, ne pas exercer d'activités professionnelles incompatibles, rémunérées ou non.

Les États membres doivent fournir à leurs autorités de contrôle l'ensemble des ressources humaines, techniques, financières et autres ressources nécessaires à l'exercice effectif de leurs missions et de leurs pouvoirs.

Chaque autorité de contrôle choisit son propre personnel, qui est soumis à sa seule direction. Le budget d'une autorité de contrôle est public et identifié de manière distincte, même si celui-ci fait partie du budget national.

La législation des États membres doit prévoir la création des autorités de contrôle et définir les règles relatives à leurs membres, à leurs qualifications ainsi qu'à leur éligibilité. La durée de leur mandat ne doit pas être inférieure à quatre ans, sachant que les États membres peuvent décider du caractère renouvelable de ce mandat. Les devoirs d'indépendance des membres énoncés ci-dessus doivent être incorporés dans le droit national. Les membres des autorités de contrôle et leur personnel sont soumis à une obligation de *"secret professionnel"*, à la fois pendant leur mandat et à l'issue de celui-ci.

Les dispositions relatives à l'établissement des autorités de contrôle constituent une élaboration plus détaillée des dispositions de l'article 28 de l'ancien cadre posé par la Directive sur la protection des données 95/46/CE. Les nouvelles règles ne présentent aucun élément manifestement inhabituel. Certains aspects nécessitent néanmoins quelques remarques : la spécificité de la durée du mandat, l'accent placé sur l'indépendance, l'insistance autour de la disposition relative aux ressources adéquates pour chaque autorité de contrôle, ainsi que l'obligation prévoyant que *"chaque membre [d'une autorité de contrôle] a les qualifications, l'expérience et les compétences nécessaires, notamment dans le domaine de la protection des données à caractère personnel, pour l'exercice de ses fonctions et de ses pouvoirs".*

Il est probable que surviennent des litiges sur la question de savoir si les autorités de contrôle sont financées de manière adéquate, notamment dans des États comme le Royaume-Uni au sein duquel la source traditionnelle de financement issue des frais d'enregistrement/de déclaration cessera d'exister.

Où puis-je trouver ces dispositions?

Articles 51 à 54
Considérants 117 à 123, Chapitre VI section ,

Compétence, missions et pouvoirs

En bref

- Les autorités de contrôle bénéficient d'une compétence spécifique leur permettant d'agir sur leur propre territoire.
- Une autorité de contrôle chef de file est compétente pour les traitements transfrontaliers (pour plus d'informations, veuillez-vous reporter à la section sur la coopération et la cohérence entre les autorités de contrôle).
- Une longue liste de pouvoirs et de missions spécifiques est attribuée aux autorités de contrôle.

A faire

- ☐ Familiarisez-vous avec l'ensemble des pouvoirs et des missions des autorités de contrôle.
- ☐ Si vous exercez des activités de traitement transfrontalier, veillez à avoir une bonne compréhension du système relatif à l'autorité chef de file (veuillez-vous reporter à la section sur la coopération et la cohérence entre les autorités de contrôle).
- ☐ Vous pourriez envisager de parvenir à une mise en conformité grâce à un Code de conduite ou à une Certification reconnu(e), qui exigera l'approbation de l'autorité de contrôle.

Degré de changement

Compétence

Les autorités de contrôle (couramment appelées “Autorités de protection des données” ou “DPA”) bénéficient d’une compétence pour *“exercer les missions et les pouvoirs”* décrits dans le GDPR sur le territoire national dont elles relèvent. Le considérant 122 indique que cette compétence inclut le *“traitement affectant des personnes concernées sur le territoire de l’Etat membre dont elle relève, ou encore le traitement effectué par un responsable du traitement ou un sous-traitant qui n’est pas établi dans l’Union lorsque ce traitement vise des personnes concernées résidant sur le territoire de l’Etat membre dont elle relève”.*

Dans les cas où la base juridique du traitement, effectué par un organisme privé ou une autorité publique, constitue une obligation légale, agissant dans l’intérêt public ou relevant de l’exercice de l’autorité publique, l’autorité “concernée” est compétente et le système d’autorité chef de file transfrontière ne s’applique pas. Tandis que cette disposition manque de clarté, le considérant 128 précise qu’une autorité de contrôle bénéficie d’une compétence exclusive sur les autorités publiques et les organismes privés agissant dans l’intérêt public qui, dans les deux cas, sont établis sur le territoire de l’autorité de contrôle. Reste à éclaircir la question de savoir si cette disposition concerne les établissements multiples et constitue un moyen d’exclure le guichet unique, ou si celle-ci confère une compétence exclusive à l’autorité de contrôle du pays d’origine même si le traitement a lieu dans un autre État de l’UE. Ceci pourrait engendrer une application étendue aux organismes du secteur privé, par exemples pour les institutions financières exerçant des activités de lutte contre le blanchiment d’argent en lien avec des clients basés dans un autre État de l’UE.

Les autorités de contrôle ne sont pas compétentes pour contrôler les opérations de traitement effectuées par des juridictions dans l’exercice de leur fonction juridictionnelle. Le terme “juridiction” n’est pas défini, et il reste à éclaircir la question de savoir jusqu’où cette règle s’appliquera dans la hiérarchie judiciaire.

Un système d’autorité chef de file est établi afin de gérer les traitements transfrontaliers (pour plus d’informations relatives à ce dispositif complexe, veuillez-vous reporter à la section sur la coopération et la cohérence entre les autorités de contrôle).

Missions

Conformément à l’article 57 du GDPR, une liste très détaillée de missions est attribuée aux autorités de contrôle. Il n’est pas nécessaire de toutes les énumérer, dans la mesure où la dernière mission figurant sur la liste est la suivante: *“s’acquitte de toute autre mission relative à la protection des données à caractère personnel”.* Les autorités de contrôle sont par conséquent tenues de prendre toutes les mesures qui peuvent raisonnablement être considérées comme étant en lien avec la *“protection des données à caractère personnel”.*

Certaines missions nécessitent d’être soulignées. Les autorités de contrôle doivent contrôler et faire respecter l’ *“application”* du GDPR, et favoriser la sensibilisation du public, des responsables du traitement et des sous-traitants.

Elles doivent conseiller le gouvernement et le parlement national sur les nouvelles propositions de loi.

Les démarches consistant à aider les personnes concernées, à traiter et à examiner les réclamations introduites par des personnes ou des organismes représentatifs, à mener des enquêtes et plus particulièrement à coopérer avec les autres autorités de contrôle sont toutes expressément mentionnées, tout comme le fait de surveiller les évolutions pertinentes dans le domaine des technologies de l’information et de la communication et des pratiques commerciales.

Les autorités de contrôle doivent encourager l’élaboration de Codes de Conduite et la mise en place de mécanismes de Certification, et *“procède à l’agrément”* des organismes de certification ainsi que des organisations chargés du suivi des codes de conduite.

Les autorités de contrôle ne sont pas autorisées à facturer les personnes concernées ou les délégués à la protection des données pour les services qu’elles délivrent; le GDPR reste néanmoins silencieux sur la question de savoir si les responsables du traitement et les sous-traitants pourraient être facturés pour les services qu’ils reçoivent de la part des autorités de contrôle.

Où puis-je trouver ces dispositions?

Articles 55-59
Considérants 117-123, chapitre VI section 2; Avis G29 244

Pouvoirs

L'article 58 du GDPR énumère les pouvoirs des autorités de contrôle, qui peuvent être complétés par les États membres s'ils le souhaitent. La plupart des pouvoirs correspondent aux missions spécifiques énumérées dans l'article 57 et ne nécessitent pas d'être répétés.

Les pouvoirs qu'il convient de souligner sont les suivants: ordonner à un responsable du traitement ou à un sous-traitant de lui communiquer des informations; mener des enquêtes sous la forme d'audits; obtenir l'accès aux locaux et aux données, émettre des avertissements et des sanctions, et imposer des amendes; ordonner à des responsables du traitement et à des sous-traitants de se conformer au GDPR et de respecter les droits des personnes concernées; interdire le traitement et les flux de données transfrontaliers en dehors de l'UE; approuver les clauses contractuelles types et les règles d'entreprise contraignantes. L'exercice des pouvoirs d'une autorité de contrôle doit être soumis à des garanties et à un recours juridictionnel.

Les États membres doivent conférer aux autorités de contrôle le droit de porter des affaires à l'attention des autorités judiciaires et *"le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire appliquer les dispositions du présent Règlement".* Vraisemblablement, les écarts de pouvoirs existants persisteront au regard du droit national et des procédures nationales.

Enfin, les autorités de contrôle doivent produire des rapports annuels. En résumé, la compétence, les pouvoirs et les missions des autorités de contrôle sont intégrés dans une liste détaillée de tout ce qu'elles doivent faire ou peuvent faire. Il s'agit principalement du rapprochement prévisible entre les pratiques existantes et certaines innovations émanant des États membres.

Coopération et cohérence entre les autorités de contrôle

En bref

Pour les traitements transfrontaliers au sein de l'UE, la Commission européenne a proposé un guichet unique au titre duquel l'autorité de contrôle de l'établissement principal du responsable du traitement serait seule compétente pour contrôler et garantir le respect de ses obligations par ce responsable du traitement au sein de l'UE. Face à une forte opposition, cette proposition a été assouplie.

Il existera désormais une autorité chef de file dans le cas d'établissements multiples ou de traitement transfrontalier au sein de l'UE, qui sera l'autorité de contrôle de l'établissement principal, étant toutefois entendu que les autorités de contrôle situées dans d'autres États au sein desquels le responsable du traitement est établi, ou au sein desquels les personnes concernées sont sensiblement affectées, ou au sein desquels une réclamation a été introduite, peuvent être impliquées, et l'autorité chef de file devra coopérer avec celles-ci. Les autorités non chef de file peuvent également gérer les affaires purement locales impliquant un responsable du traitement transfrontalier.

A faire

- ☐ Si vous exercez des activités au sein d'un seul État membre – (comme cela est encore le cas pour la majorité des entreprises), le système de l'autorité chef de file ne vous concerne pas, et le mécanisme de résolution des litiges ne vous affectera qu'à condition que le CEPD retarde ou s'oppose à une proposition de Code de conduite ou de système de Certification.
- ☐ Si vous exercez des activités dans plus de deux États membres, renseignez-vous sur l'autorité chef de file dont vous dépendez (en prenant en compte les recommandations établies par le G29 relatives aux autorités de contrôle) et rapprochez-vous de celle-ci avant toute mise en œuvre, en accédant par exemple aux formations et aux recommandations qu'elle met à disposition.

Degré de changement

Commentaire

Compétence de l'autorité chef de file

Si un responsable du traitement ou un sous-traitant mène des activités de traitement transfrontalier, que ce soit via des établissements multiples au sein de l'UE ou via seulement un établissement unique, l'autorité de contrôle de l'établissement principal ou unique agira en tant qu'autorité chef de file de cette activité de traitement transfrontalière.

Le G29 a adopté le 13 décembre 2016 des lignes directrices ainsi que des FAQ permettant d'identifier une autorité chef de file. Dès lors qu'une organisation a de multiples établissements, la compétence de l'autorité chef de file est déterminée en fonction du lieu à partir duquel les décisions relatives aux finalités et à la manière de procéder au traitement de données ont été prises – cela peut être le lieu de l'administration centrale de l'organisation, si les décisions sont effectivement prises dans un établissement situé en dehors de l'UE, l'autorité de contrôle de ce lieu sera alors l'autorité chef de file. Il est reconnu dans ces lignes directrices qu'il peut exister des situations dans lesquelles plusieurs autorités chef de file compétentes peuvent être identifiées, c.-à-d. dans des hypothèses où une entreprise multinationale décide d'avoir des centres de prises de décision distincts, situés dans différents pays, pour différentes activités de traitement. Ces directives énoncent également que « le GDPR ne permet de "forum shopping"; il doit exister un exercice réel et effectif des activités de direction au sein de l'Etat Membre identifié comme étant le lieu de l'établissement principal de l'organisation. Les organisations doivent être en capacité de démontrer aux autorités de contrôle que les décisions relatives au traitement de données à caractère personnel sont effectivement prises et mises en œuvre, dans la mesure où elles seront susceptibles de devoir fournir des preuves à l'appui de leur position. Il est également énoncé au sein de ces directives que les responsables du traitement n'ayant aucun établissement dans l'Union Européenne ne peuvent pas bénéficier du mécanisme de guichet unique. Ils doivent se rapprocher, à travers leur représentant local, des autorités de contrôle nationales dans chaque Etat Membre dans lesquels ils ont une activité.

Chaque autorité de contrôle demeure compétente pour exercer ses pouvoirs si une réclamation a été introduite auprès d'elle ou si une violation se produit dans l'Etat dont elle relève, et si l'objet de cette réclamation ou de cette violation concerne uniquement un établissement dans l'Etat membre dont elle relève, ou affecte sensiblement des personnes concernées dans cet État uniquement. Le comité européen de la protection des données ("CEPD") peut donner des directives sur ce que signifie affecter *"sensiblement"* les personnes concernées dans plus d'un État membre. Les lignes directrices du G29 citées ci-dessus contiennent des précisions sur ce que signifie affecter "sensiblement" les personnes concernées.

Ces affaires locales doivent être notifiées à l'autorité chef de file, qui a trois semaines pour décider d'intervenir ou non (en prenant en considération le fait qu'il y ait ou non un établissement dans un autre État), et appliquer ensuite la procédure de coopération. Les autorités non chef de file peuvent soumettre à l'autorité chef de file des projets de décision.

Si l'autorité chef de file n'intervient pas, l'autorité locale gérera l'affaire en recourant, le cas échéant, à l'assistance mutuelle et aux pouvoirs d'enquêtes conjointes.

Procédure de coopération

L'autorité de contrôle chef de file doit coopérer avec les autres autorités de contrôle "concernées". Elles doivent échanger des informations et tenter de parvenir à un consensus.

L'autorité chef de file doit fournir des informations aux autres autorités de contrôle, et peut solliciter l'assistance mutuelle auprès de celles-ci et mener des enquêtes conjointes sur leurs territoires. L'autorité chef de file doit soumettre sans tarder un projet de décision aux autorités concernées, qui disposent de quatre semaines pour s'y opposer. Peut intervenir un autre cycle de présentation des projets de décision, qui est soumis à une période d'objection de deux semaines. Si l'autorité chef de file ne souhaite pas suivre les avis des autorités concernées, elle devra se soumettre à la procédure de cohérence supervisée par le CEPD.

Bien qu'il existe des règles détaillées permettant de déterminer quelle autorité de contrôle doit prendre la décision officielle et notifier le responsable du traitement, l'autorité chef de file est tenue de garantir, conformément à une décision officielle, que des mesures de conformité sont prises par le responsable du traitement dans tous ses établissements.

Une autorité chef de file peut toutefois de manière exceptionnelle prendre des mesures temporaires d'urgence sans attendre l'achèvement de la procédure de cohérence.

Le système d'autorité chef de file revêt un certain nombre de lacunes apparentes, et pourrait être affaibli dès lors que des autorités non chef de file seront en mesure de s'imposer en arguant du fait que des personnes concernées basées dans leur juridiction sont sensiblement affectées par le traitement effectué par un responsable du traitement dont l'établissement principal se situe sur un autre territoire ; son succès reposera en grande partie sur le consensus et la bonne volonté des autorités de contrôle.

Assistance mutuelle, opérations conjointes et cohérence

Les autorités de contrôle sont tenues de se prêter mutuellement assistance en se communiquant des informations ou en effectuant des *"demandes d'autorisation et de consultations préalable, inspections et enquêtes".* La Commission européenne peut spécifier la forme et les procédures de l'assistance mutuelle.

Les autorités de contrôle peuvent mener des enquêtes conjointes et des opérations répressives. Une autorité de contrôle est en droit de participer à ce type d'opérations si un responsable du traitement dispose d'un établissement sur le territoire de l'Etat membre dont elle relève, ou si un nombre important de personnes concernées sont susceptibles d'être sensiblement affectées. Si le droit local l'autorise, une autorité de contrôle d'accueil peut conférer des pouvoirs d'enquête à du personnel détaché de l'autorité de contrôle d'origine. Dans la mesure où les autorités de contrôle ont mené des enquêtes conjointes en vertu du droit existant, le GDPR devrait simplement développer et renforcer ces arrangements dans la pratique.

Dans le cas où des autorités de contrôle prendraient certaines mesures officielles, désapprouveraient, ou souhaiteraient qu'une autre autorité de contrôle prenne des mesures, le GDPR prévoit un mécanisme de cohérence et de résolution des litiges. Dans ses recommandations, le G29 insiste sur la coopération entre l'autorité chef de file et les autorités de contrôle concernées afin de parvenir à un plan d'action mutuellement acceptable tout en énonçant que le mécanisme formel de cohérence devra uniquement être invoqué dans les hypothèses où la coopération n'aboutirait pas à un résultat mutuellement acceptable.

Le CEPD doit se prononcer sur plusieurs propositions soumises par les autorités de contrôle, et doit notamment approuver les règles d'entreprise contraignantes, les critères de certification et les codes de conduite. Si l'autorité de contrôle désapprouve l'avis du CEPD, l'affaire est renvoyée à la procédure de résolution des litiges.

Cette procédure s'applique également aux litiges entre autorité chef de file et autorité concernée. Dans tous les cas, la décision du CEPD est contraignante et votée à la majorité des deux tiers. En l'absence de cette majorité et à l'issue d'un certain délai, une majorité simple suffit. Les autorités de contrôle impliquées sont tenues de se conformer à la décision du CEPD, et les décisions officielles devront être émises conformément à la décision du CEPD

Où puis-je trouver ces dispositions?

Considérants 124-138 chapitre VII, sections 1 et 2

Comité Européen de la Protection des Données

En bref

- L'ancien groupe de travail de l'article 29, dont les membres étaient les autorités nationales de contrôle de l'UE, le contrôleur européen de la protection des données et la Commission européenne, a été remplacé par le "comité européen de la protection des données" ("CEPD"), avec une composition similaire mais avec un Secrétariat indépendant.
- Le CEPD bénéficie du statut d'un organe de l'UE doté de la personnalité juridique et de pouvoirs étendus afin de statuer sur les litiges entre les autorités nationales de contrôle, de fournir des conseils et des directives, ainsi que d'approuver les codes et certifications à l'échelle de l'UE.

A faire

☒ Il n'est pas nécessaire de prendre des mesures immédiates – à moins que vous soyez membre d'une autorité nationale de contrôle.

☐ Néanmoins, le CEPD exercera une influence majeure sur le droit et les pratiques en matière de protection des données au sein de l'UE, et vous pourriez souhaiter en savoir plus sur la manière d'influencer ou de contester ses décisions.

Degré de changement

Commentaire

Le groupe de travail de l'article 29, établi par la Directive 95/46/CE (la "Directive sur la protection des données") et composé des représentants des autorités de contrôle des États membres de l'UE ainsi que de la Commission et du contrôleur européen de la protection des données, sera supprimé par le GDPR. Il sera remplacé par le CEPD, qui sera de la même manière composé des responsables des autorités de contrôle nationales (ou de leurs représentants) et du contrôleur européen de la protection des données.

Le représentant de la Commission auprès du CEPD est un membre non votant, et dans les États (tels que l'Allemagne) qui disposent de plusieurs autorités de contrôle, le droit national doit prévoir la désignation d'un représentant commun. Dans les cas de résolution de litiges impliquant l'adoption d'une décision contraignante, les droits de vote du contrôleur européen de la protection des données sont restreints aux décisions concernant des principes qui seraient applicables aux institutions européennes.

Le CEPD bénéficie d'un statut largement renforcé. Il ne s'agit pas simplement d'un comité consultatif, mais d'un organe indépendant de l'Union européenne qui dispose de sa propre personnalité juridique.

Il est officiellement représenté par son président, qui a pour rôle principal d'organiser les travaux du CEPD et plus particulièrement d'administrer la procédure de conciliation relative aux litiges entre les autorités nationales de contrôle. Le président et les deux vice-présidents sont élus parmi les membres du CEPD, et occupent leurs fonctions pour une période de cinq ans renouvelable une fois.

Bien que le CEPD se prononce généralement à la majorité simple, le règlement intérieur et les décisions contraignantes (en première instance) sont votés à la majorité des deux tiers.

Le CEPD adopte son propre règlement intérieur et organise ses propres affaires. L'indépendance du CEPD est mise en avant. Il semble qu'il soit suggéré implicitement que la Commission ait exercé une trop grande influence sur le groupe de travail de l'article 29 par le passé, et qu'elle ait tenté de consolider ce pouvoir.

Le Secrétaire de l'ancien groupe de travail de l'article 29 était un fonctionnaire de la Commission. Le nouveau CEPD disposera de son propre Secrétariat assuré par le Contrôleur européen de la protection des données, qui accomplira ses tâches sous l'autorité exclusive du président du CEPD.

Bien que le CEPD se voie conférer une liste de missions longue et détaillée, son rôle principal consiste à veiller à l'application cohérente du GDPR au sein de l'Union. Il conseille la Commission, notamment sur le niveau de protection offert par les pays tiers ou les organisations internationales, et promeut la coopération entre les autorités de contrôle nationales. Il publie des lignes directrices, des recommandations et des bonnes pratiques : par exemple dès lors qu'une violation des données est susceptible d' *"engendrer un risque élevé pour les droits et les libertés"* des personnes, ou sur des questions relatives aux obligations concernant les règles d'entreprise contraignantes. Il encourage les Codes de conduite et la Certification, qui aideront les responsables du traitement et les sous-traitants à démontrer leur conformité au GDPR.

Bien qu'une grande partie des missions figurant dans cette liste consiste en la description ou la formalisation de l'activité de l'actuel groupe de travail de l'article 29, les avis et les activités du CEPD bénéficieront d'une force exécutoire plus importante.

La caractéristique la plus distinctive du nouveau rôle du CEPD réside dans le fait qu'il est chargé de la conciliation et de la résolution des litiges entre les autorités de contrôle nationales. Pour en savoir plus sur cette activité, veuillez consulter la section intitulée compétence, missions et pouvoirs. Il a souvent été reproché à l'ancien groupe de travail de l'article 29 de ne pas engager de processus de consultation adéquat avant de prendre des décisions. Le nouveau CEPD doit consulter les parties intéressées *"le cas échéant"*. Nonobstant la qualification de "sortie", il s'agit d'un avantage majeur pour les parties susceptibles d'être affectées par les avis, les directives, les conseils et les propositions de bonnes pratiques.

Lorsque le comité le juge nécessaire *"ses débats sont confidentiels, comme le prévoit son règlement intérieur"*. Ceci suggère que les réunions et les débats seront en principe publics, sauf décision contraire.

Enfin, le CEPD doit préparer un Rapport Annuel.

Où puis-je trouver ces dispositions?

Considérants 139 et 140, et chapitre VII section 3

Voies de recours et responsabilités

En bref

- Les personnes peuvent faire valoir les droits suivants (contre les responsables du traitement et les sous-traitants):
  - droit d'introduire une réclamation auprès des autorités de contrôle dès lors que leurs données ont été traitées de manière non conforme aux dispositions du GDPR;
  - droit à un recours juridictionnel effectif dès lors qu'une autorité de contrôle compétente n'a pas traité de manière appropriée une réclamation;
  - droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant concerné; et
  - droit à réparation de la part du responsable du traitement ou du sous-traitant concerné pour tout dommage matériel ou moral résultant de la violation du GDPR.
- Les personnes physiques et morales peuvent former un recours auprès des juridictions nationales contre toute décision juridiquement contraignante les concernant et prononcée par une autorité de contrôle.
- Les personnes peuvent introduire une réclamation pour perte financière, et pas seulement pour réparation. La possibilité pour un groupe de former un recours est facilitée.

A faire

- ☐ Les responsables du traitement et leurs sous-traitants doivent s'assurer que les accords relatifs au traitement des données et à la gestion des contrats indiquent clairement le champ d'application des responsabilités du sous-traitant, et doivent prévoir les mécanismes de résolution des litiges à l'égard de leurs obligations respectives afin de régler les demandes en réparation.
- ☐ Les responsables du traitement et les sous-traitants doivent s'engager à informer les autres responsables du traitement et sous-traitants impliqués dans le même traitement de toutes les violations de conformité pertinentes ainsi que de toute réclamation ou demande reçue de la part des personnes concernées.
- ☐ Les responsables conjoints du traitement, et les responsables du traitement impliqués dans les mêmes opérations de traitement, doivent s'entendre sur leurs obligations respectives en matière de conformité des données, sur leurs responsabilités respectives s'agissant des violations de protection des données, et sur les mécanismes de résolution des litiges relatifs à leurs responsabilités respectives s'agissant de régler les demandes en réparation.

Degré de changement

Réclamations auprès des autorités de contrôle

Les droits des personnes concernées d'introduire des réclamations auprès des autorités de contrôle sont légèrement renforcés par rapport à la Directive sur la protection des données. La Directive oblige les autorités de contrôle à entendre les réclamations introduites par les personnes concernées, afin de vérifier la licéité du traitement des données, et informer les personnes concernées qu'une vérification a été menée.

Conformément au GDPR, les personnes concernées dont les données à caractère personnel ont été traitées de manière non conforme aux dispositions du GDPR bénéficient d'un droit spécifique leur permettant d'introduire une réclamation auprès des autorités de contrôle, et l'autorité de contrôle doit informer les personnes concernées sur les avancées et l'issue des réclamations introduites.

Recours judiciaires contre des décisions prononcées par les autorités de contrôle

Les personnes concernées et les autres parties affectées bénéficient d'un droit de recours judiciaire effectif à l'égard de certains actes et décisions des autorités de contrôle.

- Toute personne bénéficie d'un droit de recours judiciaire effectif contre toute décision juridiquement contraignante les concernant, et prononcée par une autorité de contrôle.
- Les personnes concernées bénéficient d'un droit de recours judiciaire effectif dès lors qu'une autorité de contrôle échoue à traiter une réclamation ou échoue à informer dans les 3 mois la personne concernée sur les avancées ou l'issue de sa réclamation.

Le considérant 143 précise que les décisions et actions susceptibles d'être contestées auprès des tribunaux comprennent l'exercice des pouvoirs d'enquête, rectificatifs et d'autorisation de l'autorité de contrôle, ou le renvoi ou le rejet des réclamations. Ce droit n'englobe pas les autres mesures prises par les autorités de contrôle qui ne sont pas juridiquement contraignantes, telles que les avis émis ou les conseils fournis par les autorités de contrôle.

Recours judiciaires à l'encontre des responsables du traitement et des sous-traitants

Les personnes concernées dont les droits ont été violés bénéficient d'un droit de recours judiciaire effectif à l'encontre du responsable du traitement ou du sous-traitant responsable de la violation présumée. Cette disposition va au-delà de la disposition équivalente énoncée dans la Directive sur la protection des données, qui prévoit un recours judiciaire uniquement à l'encontre des responsables du traitement, et non à l'encontre des sous-traitants de données.

Responsabilité en matière d'indemnisation

Toute personne ayant subi un dommage résultant de la violation du GDPR est en droit de percevoir une indemnisation de la part du responsable du traitement ou du sous-traitant. Conformément à la Directive sur la protection des données, la responsabilité en matière d'indemnisation s'applique exclusivement aux responsables du traitement.

La disposition suivante est formulée à l'égard de la répartition des responsabilités en matière d'indemnisation entre les responsables du traitement et les sous-traitants :

- les responsables du traitement sont responsables des dommages causés par un traitement qui n'est pas conforme au GDPR ;
- les sous-traitants sont uniquement responsables des dommages causés par un traitement qui n'a pas respecté les obligations prévues par le GDPR qui incombent spécifiquement aux sous-traitants ou par un traitement mis en œuvre indépendamment des instructions licites du responsable de traitement ou contrairement à celles-ci; et
- afin de garantir aux personnes concernées une réparation effective, les responsables du traitement et les sous-traitants impliqués dans le même traitement sont responsables de tout dommage causé et chacun est tenu responsable du dommage dans sa totalité. Toutefois, un responsable du traitement ou un sous-traitant qui est tenu de verser une indemnisation sur cette base est en droit de réclamer auprès de toutes les parties concernées la part de la réparation correspondant à leur part de responsabilité dans le dommage.

Tandis que la Directive sur la protection des données ne fait référence au droit d'indemnisation qu'en cas de *"dommage"*, le GDPR précise clairement que l'indemnisation peut être recouvrée pour des pertes à la fois pécuniaires et non pécuniaires. Cette clarification est néanmoins cohérente avec l'interprétation judiciaire actuelle autour de la signification du dommage dans le centre de demandes d'indemnisation en vertu de la Directive sur la protection des données (voir Google Inc. c. Vidal-Hall & Others [2015] EWCA Civ 311).

Le GDPR précise que les responsables du traitement ou les sous-traitants sont exonérés de cette responsabilité s'ils *"ne sont en aucune manière responsables de l'événement ayant provoqué le dommage"*. Cette exemption semble légèrement plus réductrice que l'exemption pouvant être revendiquée en vertu de la Directive sur la protection des données par un responsable du traitement qui peut prouver *"qu'il n'est pas responsable de l'événement ayant provoqué le dommage"*.

Instances représentatives

Le GDPR autorise les instances représentatives, agissant pour le compte des personnes concernées, à introduire des réclamations auprès des autorités de contrôle, et à former des recours judiciaires contre des décisions prononcées par les autorités de contrôle ou contre les responsables du traitement ou les sous-traitants. Cette disposition s'applique à toute instance représentative qui:a not-for-profit body, organisation or association;

- est valablement constituée conformément à la législation de l'État membre ;
- exerce une activité non lucrative ;
- présente des objectifs statutaires s'inscrivant dans l'intérêt public ; et
- est active dans le domaine de la protection des données.

Les personnes concernées peuvent également mandater ces instances afin de faire valoir en leur nom leur droit de recouvrer une indemnisation de la part des responsables du traitement ou des sous-traitants, sous réserve que la législation de l'État membre l'autorise.

Si la législation de l'État membre le permet, ces instances représentatives pourront, indépendamment du mandat de la personne concernée, introduire des réclamations auprès des autorités de contrôle et former un recours judiciaire contre les décisions de l'autorité de contrôle, ou contre les responsables du traitement ou sous-traitants.

Il n'existe aucune disposition équivalente dans la Directive sur la protection des données.

Où puis-je trouver ces dispositions?

Articles 77-82
Considérants 141 - 147

Amendes administratives

En bref

- Les autorités de contrôle sont autorisées à imposer des amendes administratives à la fois aux responsables du traitement et aux sous-traitants.
- Les amendes peuvent être imposées à la place, ou en parallèle de mesures susceptibles d'être imposées par les autorités de contrôle. Elles peuvent être imposées pour un large éventail d'infractions, y compris des violations purement procédurales.
- Les amendes administratives sont discrétionnaires et non obligatoires ; elles doivent être imposées au cas par cas, et revêtir un caractère *"effectif, proportionné et dissuasif".*
- Il existe deux catégories d'amendes administratives:
  - Certaines infractions feront l'objet d'amendes administratives pouvant s'élever jusqu'à 10 000 000 €, ou dans le cas d'une entreprise, à 2 % du chiffre d'affaires total, le montant le plus élevé étant retenu.
  - D'autres infractions seront soumises à des amendes administratives pouvant s'élever jusqu'à 20 000 000 €, ou dans le cas d'une entreprise, à 4 % du chiffre d'affaires total, le montant le plus élevé étant retenu.
- Les États membres peuvent déterminer si, et dans quelle mesure, les autorités publiques doivent être soumises à des amendes administratives.

A faire

☐	Effectuez une analyse de conformité au GDPR afin d'identifier les domaines présentant la non-conformité la plus importante, et de prioriser les mesures permettant d'atténuer les risques, notamment s'agissant des activités de traitement à risque élevé.
☐	Actualisez vos registres de risque.
☐	Évaluez les risques que votre responsabilité soit engagée au sein de vos accords existants avec des clients, fournisseurs et/ou partenaires, notamment en examinant les clauses de limitation et d'exclusion de responsabilité prévues par ces contrats.
☐	Examinez vos contrats d'assurance.

Considérations générales

Les amendes administratives ne sont pas appliquées de manière automatique, et sont prononcées au cas par cas. Le considérant 148 précise que dans le cas d'une violation mineure, ou lorsqu'une amende infligerait une charge disproportionnée à une personne physique, un rappel à l'ordre pourra être émis plutôt qu'une amende.

Il existe actuellement un degré élevé de variation entre les États membres s'agissant de l'imposition de sanctions financières par les autorités de contrôle. Bien que les accords en vertu du GDPR prévoient des sanctions maximales et confèrent aux autorités de contrôle une certaine marge de manœuvre lorsqu'elles prononcent des sanctions, le considérant 150 indique que le mécanisme de contrôle de la cohérence doit être utilisé pour promouvoir une application cohérente des amendes administratives.

Chaque État membre doit néanmoins établir des règles sur la question de savoir si, et dans quelle mesure, des amendes administratives doivent être prononcées à l'encontre des autorités publiques et des instances établies dans cet État membre.

Amendes administratives maximales

Le GDPR prévoit deux groupes de plafonds maximaux pour des amendes administratives qui peuvent être imposées pour les violations correspondantes.

Dans chaque cas, l'amende maximale est exprimée en € ou, dans le cas des entreprises, en pourcentage du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Le considérant 150 confirme que dans ce contexte, *"une entreprise"* revêt la signification énoncée dans les articles 101 et 102 du Traité sur le fonctionnement de l'Union européenne ("TFUE") (c.-à-d. d'une manière générale, les entités exerçant une activité économique).

La violation des dispositions suivantes prévues par le GDPR est passible d'amendes administratives pouvant s'élever jusqu'à 20 000 000 €, ou dans le cas d'une entreprise, à 4 % du chiffre d'affaires total, le montant le plus élevé étant retenu:

- principes de base relatifs au traitement de données à caractère personnel, y compris les conditions relatives au consentement (Articles 5, 6, 7 et 9);
- droits des personnes concernées (Articles 12-22);
- transferts internationaux (Articles 44-49);
- obligations issues du droit des États membres adoptés en application du chapitre IX; et
- non-respect d'une ordonnance imposée par les autorités de contrôle (tel qu'indiqué dans l'article 58(2) ou refus de se soumettre aux demandes d'une autorité de contrôle dans le cadre d'une enquête réalisée en vertu de l'article 58(1).

Les autres violations sont passibles d'amendes administratives pouvant s'élever jusqu'à 10 000 000 €, ou dans le cas d'une entreprise, à 2 % du chiffre d'affaires total, le montant le plus élevé sera retenu. Les infractions soumises à ces amendes maximales sont susceptibles d'être constituée en cas de violation des obligations suivantes:

- obligation d'obtenir un consentement pour les traitements de données à caractère personnel relatives aux enfants (Article 8) ;
- obligation de mettre en place des mesures techniques et organisationnelles afin de garantir la protection des données dès la conception et par défaut (Article 25) ;
- obligation pour les co-responsables du traitement d'accepter leurs obligations de conformité respectives (Article 26) ;
- obligation pour les responsables du traitement et les sous-traitants basés en dehors de l'UE de désigner des représentants (Article 27) ;
- obligation des responsables du traitement lorsqu'ils recourent à des sous-traitants (Article 28) ;
- obligation pour les sous-traitants de sous-traiter uniquement avec le consentement préalable du responsable du traitement, et de traiter les données que sur instruction du responsable du traitement (Articles 28-29);
- obligation de conserver des registres des activités de traitement (Article 30) ;
- obligation pour les responsables du traitement et les sous-traitants de coopérer avec les autorités de contrôle (Article 31) ;
- obligation de mettre en œuvre des mesures techniques et organisationnelles (Article 32) ;
- obligation de notifier les violations dès lors que le GDPR l'exige (Articles 33 et 34) ;
- obligations relatives à la conduite d'étude d'impact relative à la vie privée (Articles 35 et 36) ;
- obligations relatives à la nomination des Délégués à la protection des données (Articles 37-39) ;

- obligations imposées aux organismes de certification (Article 42) ; et
- obligations imposant aux organismes de surveillance de prendre des mesures en cas de violation des codes de conduite (Article 41).

Dans les cas où le même traitement, ou un traitement connexe, implique la violation de plusieurs dispositions du GDPR, les amendes n'excèderont pas le montant prévu pour l'infraction la plus grave.

Facteurs à prendre en compte

L'article 83(2) du GDPR énumère les facteurs à prendre en compte pour déterminer s'il y a lieu d'imposer une amende administrative, et pour décider du montant de l'amende à imposer. Ces facteurs comprennent:

- la nature, la gravité, et la durée de l'infraction au vu de la nature, du champ d'application ou des finalités du traitement en question, ainsi que le nombre de personnes concernées et le niveau de dommage subi par celles-ci ;
- s'il s'agit d'une violation intentionnelle ou commise par négligence ;
- les mesures prises par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;
- le degré de responsabilité du responsable du traitement ou du sous-traitant ;
- toutes les autres violations antérieures pertinentes ;
- le degré de coopération avec l'autorité de contrôle ;
- les catégories de données à caractère personnel affectées ;
- si la violation a été notifiée auprès de l'autorité de contrôle par le responsable du traitement ou le sous-traitant ;
- tout antécédent d'action coercitive ;
- le respect des codes de conduite approuvés conformément à l'article 40 ou des mécanismes de certification approuvés conformément à l'article 42 ; et
- tout autre facteur aggravant ou atténuant applicable dans ces circonstances, ex : avantages financiers obtenus ou pertes évitées découlant directement ou indirectement de l'infraction.

Dès lors que des amendes sont imposées à des personnes autres que des entreprises, l'autorité de contrôle devra prendre en considération la situation économique de la personne et le niveau général de revenus au sein de l'État membre.

Où puis-je trouver ces dispositions?

Article 83
Considérants 148-152

Dérogations et conditions particulières

En bref

Les États membres conservent la capacité d'introduire des dérogations dès lors que celles-ci sont requises à des fins de sécurité nationale, de prévention et de détection des activités criminelles, ainsi que dans certains autres cas. Conformément à la jurisprudence de la Cour de justice de l'Union européenne, une telle dérogation doit respecter *"l'essence"* du droit à la protection des données, et constituer une mesure nécessaire et proportionnée.

S'agissant de ces finalités particulières, le GDPR impose aux États membres de, ou les autorise à, introduire des législations supplémentaires. S'agissant des cas de recherche historique ou scientifique, de traitement statistique, ou archivistique, cela peut même fournir une base juridique au traitement des données sensibles.

Il existe d'autres sujets particuliers pour lesquels des modifications législatives au sein des États membres sont prévues, notamment le traitement des données des employés, le traitement en lien avec la liberté d'expression et le secret professionnel (qui prévoit des restrictions en matière de droit d'audit des autorités de contrôle).

Les responsables du traitement (et, dans certains cas, les sous-traitants) devront surveiller et s'adapter aux différentes approches des États membres dans ces domaines

A faire

- ☐ Déterminez si certaines activités de traitement que vous mettez en place sont soumises à des dérogations ou à des conditions particulières en vertu du GDPR
- ☐ Dès lors qu'une dérogation ou une condition particulière s'applique à votre traitement, définissez les juridictions au sein desquelles ce traitement a lieu.
- ☐ Envisagez d'exercer une influence supplémentaire dans les pays au sein desquels votre organisation pourrait être concernée par l'introduction de restrictions locales.
- ☐ Dès lors que des règles de secret professionnel s'appliquent aux données à caractère personnel reçues ou obtenues par un responsable du traitement ou un sous-traitant, assurez-vous que celles-ci soient labellisées de manière appropriée afin qu'elles puissent être protégées contre toute communication aux autorités de contrôle.

Degré de changement

Inconnu: La plupart des mêmes catégories de dérogation et de conditions particulières s'appliquent tel que prévu par la Directive 95/46 EC (la Directive relative à la protection des données) mais il existe une difficulté concernant l'anticipation de la conformité à de telles dérogations et conditions particulières dans la mesure où elles dépendront de la manière dont les Etats membres introduiront ou maintiendront les lois et règles en la matière.

Commentaire

Cas particuliers

Le GDPR prévoit d'importantes dérogations et exemptions dans deux domaines principaux : (1) au chapitre III section 5, s'agissant des *"restrictions"* relatives aux obligations et aux droits à la protection des données ; et (2) au chapitre IX, s'agissant des *"situations particulières de traitement des données".*

Article 23 - Limitations

L'article 23 du GDPR confère aux États membres le droit d'introduire des dérogations à la législation sur la protection des données dans certaines situations; c'est également le cas pour la Directive sur la protection des données. Les États membres peuvent mettre en place des dérogations aux obligations de transparence et aux droits des personnes concernées, mais uniquement si ces mesures *"respectent l'essence des libertés et des droits fondamentaux et soient... nécessaires et proportionnées... dans une société démocratique."*

Cette mesure doit garantir l'un des éléments suivants:

- la sécurité nationale;
- la défense;
- la sécurité publique;
- la prévention, l'investigation, la détection ou la poursuite des infractions pénales ou des manquements à la déontologie des professions réglementées;
- d'autres considérations importantes d'intérêt public, notamment les intérêts économiques ou financiers (ex: questions budgétaires ou fiscales);
- la protection de l'indépendance de la justice et des procédures judiciaires;
- l'exercice de l'autorité publique en matière de contrôle, d'inspection et de réglementation en relation avec l'exercice de l'autorité publique en matière de sécurité, défense, d'autres considérations importantes d'intérêt public, ou de la prévention de la criminalité/éthique;
- la protection de la personne concernée ou des droits et libertés d'autrui; ou
- l'application du droit civil.

Afin qu'une mesure soit acceptable, elle doit (conformément à l'article 23(2)) inclure des dispositions spécifiques énonçant:

- les finalités du traitement;
- les catégories de données concernées;
- le champ d'application des restrictions au GDPR introduit par la mesure;
- les garanties permettant de prévenir les abus, les accès ou transferts illicites;
- les responsables du traitement pouvant s'appuyer sur ces restrictions;
- les durées de conservation et les mesures de sécurité applicables;
- le risque pour les droits et libertés des personnes concernées; et
- le droit des personnes concernées à être informées de la restriction, sauf si cela porte préjudice aux finalités de la restriction.

Articles 85-91 : "Situations particulières de traitement des données"

Les dispositions du chapitre IX du GDPR prévoient un ensemble de dérogations, d'exemptions et de pouvoirs permettant d'imposer des exigences supplémentaires, au regard des obligations et des droits énoncés par le GDPR, pour des types de traitement particuliers. Ces différentes dispositions se fondent sur des situations de traitement particulières d'ores et déjà traitées par la Directive sur la protection des données.

Article 85 : Liberté d'expression et information

Cette disposition impose aux États membres, de mettre en place des exemptions au GDPR dès lors que cela est nécessaire pour *"concilier le droit à la protection des données à caractère personnel... et le droit à la liberté d'expression et d'information".* Bien que cet article ait un champ d'application plus large que l'article 9 de la Directive sur la protection des données, l'article 85(2) prévoit des dispositions spécifiques pour les traitements effectués à des fins journalistiques, ou à des fins d'expression universitaire, artistique ou littéraire. Les États membres devront informer la Commission sur la manière dont ils ont mis en place cette obligation, et devront l'informer de tout changement apporté à ces législations.

Article 86 : Droit d'accès du public aux documents officiels

Cette disposition vient compléter le considérant 72 de la Directive sur la protection des données, et permet la communication des données à caractère personnel contenues dans les documents officiels conformément aux législations de l'Union ou des États membres qui autorisent le droit d'accès du public aux documents administratifs. Cette disposition prévoit néanmoins des restrictions: ces législations devraient, conformément au considérant 154 du GDPR, *"concilier l'accès du public aux documents officiels... et le droit à la protection*

des données à caractère personnel". La Directive 2003/98/CE (la "Directive ISP") sur la *"réutilisation des informations du secteur public"* ne modifie ni les obligations des autorités, ni les droits des personnes, en vertu du GDPR.

Article 87 : Numéro d'identification national

Cet article énonce effectivement le droit des États membres de définir leurs propres conditions relatives au traitement des numéros d'identification nationaux en vertu de la Directive sur la protection des données. L'unique expansion vise à clarifier que ceci exige la mise en place de garanties appropriées.

Article 88 : Données des employés

Les États membres sont autorisés à établir (soit en vertu de la loi, soit en vertu d'accords collectifs) des règles plus spécifiques en matière de traitement des données à caractère personnel des employés, couvrant tous les principaux aspects du cycle d'emploi, du recrutement à la fin du contrat. Cela inclut la capacité de mettre en place des règles énonçant les situations dans lesquelles le consentement sera considéré valable dans le cadre d'une relation de travail. Ces règles doivent inclure des mesures spécifiques visant à garantir *"la dignité, les intérêts légitimes et les droits fondamentaux"* de la personne concernée. Le GDPR énonce que la transparence du traitement, les transferts au sein d'un groupe d'entreprises, et les systèmes de contrôle sont des domaines exigeant une attention particulière. Les États membres doivent notifier la Commission toute nouvelle législation introduite en vertu de cet article avant que le GDPR n'entre en vigueur, et doivent également la notifier de tout amendement.

Article 89(1) et (2) : A des fins de recherche scientifique et historique ou à des fins statistiques

L'article 89(1) reconnaît que les responsables de traitement peuvent traiter des données à de telles fins dès lors que des garanties appropriées sont appliquées (veuillez-vous reporter à la section sur la licéité du traitement et le traitement ultérieur et sur les données sensibles et la licéité du traitement). Dès que possible, les responsables du traitement sont tenus d'atteindre ces finalités avec des données qui ne permettent pas, ou ne permettent plus, l'identification des personnes concernées ; si l'anonymisation n'est pas possible, la pseudonymisation devra être utilisée, à moins qu'une telle pseudonymisation se révèle préjudiciable aux fins recherche ou du processus statistique.

L'article 89(2) autorise les États membres et l'UE à légiférer davantage afin de prévoir des dérogations aux droits d'accès, de rectification, de suppression, de restriction et d'opposition des personnes concernées (sous réserve des garanties énoncées dans l'article 89(1)) lorsque de tels droits "rendent impossible ou entravent sérieusement" la réalisation de ces finalités spécifiques, et que la dérogation est nécessaire pour atteindre ces finalités.

Les considérants fournissent davantage d'informations sur la manière dont les termes *"recherche scientifique", "recherche historique"* et *"fins statistiques"* doivent être interprétés. Le considérant 159 précise que la recherche scientifique devrait être *"interprétée au sens large"* et inclut la recherche financée par des fonds privés, ainsi que les études menées dans l'intérêt public. Afin que le traitement soit considéré comme étant de nature statistique, le considérant 162 précise que le résultat du traitement ne devrait pas constituer des *"données à caractère personnel, mais des données agrégées"*, et ne devrait pas être utilisé à l'appui de mesures ou des décisions relatives à une personne physique en particulier.

Article 89(1) et (3) : Archivage dans l'intérêt général

Les mêmes dérogations et garanties sont prévues à des fins *"archivistiques dans l'intérêt public"* comme indiqué ci-dessus s'agissant du traitement à des fins de recherche et statistiques, étant toutefois entendu que les dérogations peuvent également être accordées concernant le droit à la portabilité des données. Des informations supplémentaires sont fournies dans le considérant 158, qui suggère que cette disposition ne devrait être utilisée que par les organismes ou autorités qui ont l'obligation d'interagir avec des archives *"à conserver à titre définitif dans l'intérêt public général"* en vertu de la législation de l'État membre ou de l'Union.

Article 90 : Obligations de secret

Cet article permet aux États membres de mettre en place des règles spécifiques afin de sauvegarder l' *"obligation de secret professionnel"* ou les autres *"obligations de secret équivalentes"* dans le cadre desquelles les autorités de contrôle sont habilitées à accéder aux données à caractère personnel ou aux locaux. Ces règles doivent *"concilier le droit à la protection des données à caractère personnel et l'obligation de secret professionnel",* et s'appliquent exclusivement aux données reçues ou obtenues en vertu de cette obligation. Ici encore, les États membres doivent notifier la Commission de toute législation introduite conformément à cet article avant que le GDPR n'entre en vigueur, et doivent également l'informer de tout amendement.

Article 91 : Églises et associations religieuses

Cet article protège les règles existantes et *"complètes"* relatives aux églises, aux associations et aux communautés religieuses, qui sont alignées sur les dispositions du GDPR. Ces entités demeureront dans l'obligation de se soumettre au contrôle d'une autorité de contrôle indépendante conformément aux conditions du chapitre VI (se reporter à la section sur la coopération et la cohérence entre les autorités de contrôle).

Où puis-je trouver ces dispositions?

Dérogations
Article 23, Considérant 73

Conditions particulières
Articles 6(2), 6(3), 9(2)(a),85-91
Considérants 50, 53, 153-165

Actes délégués, actes d'exécution et dispositions finales

En bref

Les chapitres finaux du GDPR confirment que celui-ci entrera en vigueur le 25 mai 2018. Les relations prévues avec les autres instruments de protection des données de l'UE, notamment avec la directive 2002/58/CE (la "Directive vie privée et communications électroniques") sont également énoncés au sein de ces chapitres.

La Commission publiera régulièrement des rapports sur le GDPR dès son entrée en vigueur. Ces dispositions finales confèrent également à la Commission le pouvoir d'adopter certains actes délégués en vertu du GDPR (c.-à-d. à l'égard de l'utilisation des icônes et des mécanismes de certification).

A faire

- ☐ Notez que le GDPR entrera en vigueur le 25 mai 2018.
- ☐ Commencez à planifier les changements auxquels vous devrez procéder pour vous conformer aux nouvelles obligations. Consultez les points d'action énumérés dans les autres sections.
- ☐ Si cela concerne votre activité, surveillez de près les nouveaux développements en lien avec la Directive vie privée et communications électroniques. Le 10 janvier 2017, la Commission européenne a adopté une nouvelle proposition de Règlement visant à remplacer la Directive vie privée et communications électroniques.

Degré de changement

Commentaire

Le chapitre 10 du RGPD confère à la Commission le pouvoir d'adopter des actes délégués (tel qu'indiqué à l'article 12(8) relatif aux icônes normalisées, et dans l'article 43(8) relatif aux mécanismes de certification). Ces pouvoirs peuvent être révoqués à tout moment par le Parlement ou le Conseil. Les actes adoptés entreront en vigueur dans un délai de 3 mois, sous réserve que ni le Parlement ni le Conseil ne s'y oppose. Cette période peut être prolongée. La Commission sera assistée par un comité, conformément au Règlement 182/2011. Il est particulièrement important que la Commission procède aux consultations appropriées tout au long de son travail préparatoire, y compris au niveau des experts (considérant 166).

Des pouvoirs d'exécution sont également conférés à la Commission afin de garantir des conditions uniformes pour la mise en œuvre du GDPR, qui devront également être exercés conformément au Règlement 182/2011.

Le chapitre 11 du GDPR confirme que la Directive sur la protection des données sera abrogée dès l'entrée en vigueur du GDPR, qui aura lieu deux ans et vingt jours après sa publication au Journal officiel (soit le 25 mai 2018). Les références à la Directive sur la protection des données abrogée au sein d'autres lois devront désormais interprétées comme des références au GDPR et les références au G29 seront interprétées comme des références au Comité Européen de la Protection des Données.

La Commission transmettra régulièrement des rapports sur le GDPR au Parlement et au Conseil, en insistant particulièrement sur les dispositions relatives au transfert de données, ainsi que sur les dispositions relatives à la coopération et à la cohérence.
Le premier rapport sera présenté au plus tard 4 ans après l'entrée en vigueur du GDPR, et sera ensuite présenté tous les 4 ans. Les rapports seront accessibles au public.

Il est clairement précisé à l'article 95 que le GDPR n'impose pas d'obligations supplémentaires aux fournisseurs de services de communications électroniques accessibles au public au sein de l'Union sous réserve qu'ils soient soumis à des obligations spécifiques en vertu de la Directive vie privée et communications électroniques ayant les mêmes finalités. Le 10 janvier 2017, la Commission européenne a adopté une nouvelle proposition de Règlement visant à remplacer la Directive vie privée et communications électroniques.

Le considérant 171 clarifie le fait que lorsque le traitement est fondé sur le consentement, conformément à l'actuelle Directive sur la protection des données, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la manière dont le consentement a été donné est conforme aux conditions énoncées par le GDPR.

Où puis-je trouver ces dispositions?

Articles 92-99
Considérants 166-173

Glossaire terminologique

Accès des personnes
Il s'agit du droit des personnes concernées d'obtenir auprès du responsable du traitement, sur demande, certaines informations relatives au traitement de leurs données à caractère personnel, tel qu'indiqué dans la section 2 chapitre III du GDPR.

Autorité de contrôle/Autorité chef de file
Les autorités de contrôle sont des autorités nationales de protection des données, qui sont habilitées à faire appliquer le GDPR dans leur propre État membre. Concept du "guichet unique": dès lors qu'une entreprise est établie dans plus d'un État membre, elle sera rattachée à une "autorité chef de file", qui sera déterminée par le lieu de son "établissement principal" au sein de l'UE. Une autorité de contrôle qui n'est pas une autorité chef de file peut également disposer de pouvoirs d'action en tant qu'autorité de régulation, par exemple dans les hypothèses où le traitement a des conséquences sur des personnes concernées dans le pays au sein duquel cette autorité de contrôle est l'autorité nationale

Catégories particulières de données
Souvent désignées comme étant des "données sensibles". Le GDPR a étendu la définition afin d'inclure à la fois les données biométriques et les données génétiques.

CEPD
Le Comité Européen de la Protection des Données; il remplacera le groupe de travail institué par l'article 29, et ses fonctions consisteront à garantir la cohérence dans l'application du GDPR, à conseiller la Commission de l'UE, à publier des lignes directrices, des codes de pratique et des recommandations, à accréditer les organismes de certification, ainsi qu'à se émettre des avis sur les propositions de décision des autorités de contrôle.

Directive sur la protection des données
La directive européenne 95/46/CE régissait auparavant le traitement des données à caractère personnel au sein de l'UE, et sera désormais remplacée par le GDPR.

Données à caractère personnel
Il s'agit de toutes les informations relatives à une personne physique ("personne concernée") identifiée/identifiable. Une personne concernée est une personne physique qui peut être identifiée, ou identifiable, directement ou indirectement.

DPO
Délégué à la Protection des données (Data Protection Officer); il est obligatoire d'en désigner un en vertu du GDPR dès lors que: (i) le traitement est effectué par une autorité publique ou; (ii) les "activités de base" du responsable du traitement et du sous-traitant (a) consistent en un traitement "à grande échelle de catégories particulières de données" ou; (b) consistent en un traitement à grande échelle de catégories particulières de données ou de données relatives à des condamnations pénales et des infractions.

Droit à l'effacement des données/droit à l'oubli
Le droit à l'effacement des données à caractère personnel d'une personne concernée existant a été, dans certains cas, étendu à un nouveau "droit à l'effacement" dans les cas énoncés dans la section 3 chapitre III du GDPR.

EEE
L'Espace Economique Européen comprend l'ensemble des 28 États membres de l'UE ainsi que l'Islande, le Liechtenstein et la Norvège. L'EEE n'inclut pas la Suisse

EIVP ou PIA
Le GDPR impose une nouvelle obligation aux responsables du traitement et aux sous-traitants, d'effectuer une étude d'impact relative à la protection des données, ou EIVP (Privacy Impact Assessment ou PIA) avant d'entreprendre tout traitement présentant un risque spécifique pour la vie privée du fait de sa nature, de sa portée ou de ses finalités. La section 3 du chapitre IV énonce une liste non exhaustive des catégories de traitement relevant de cette disposition.

Entreprise
Ce terme est utilisé dans plusieurs contextes au sein du GDPR, le plus souvent pour désigner une entité juridique exerçant une "activité économique". Ce terme revêt une signification particulière dans le cadre des dispositions du GDPR relatives aux sanctions financières. Les entreprises sont susceptibles de faire l'objet de sanctions calculées en pourcentage de leur chiffre d'affaires annuel mondial. Dans ce contexte, le terme fait référence aux principes développés dans le cadre du droit européen de la concurrence

Le groupe de travail de l'article 29
Le groupe de travail de l'Article 29 (G29) est constitué de représentants des autorités nationales de contrôle de l'UE, du contrôleur européen de la protection des données et de la Commission européenne. Il a été remplacé dans le GDPR et s'appelle désormais le Comité Européen de la Protection des Données (CEPD) composé de manière similaire mais avec un Secrétariat indépendant (veuillez-vous reporter au chapitre relative au "Comité Européen de la Protection des Données").

Traitement
Ce large terme désigne toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel ou des ensembles de données à caractère personnel, via des moyens automatisés ou non. Figurent parmi les exemples de traitement la collecte, l'enregistrement, l'organisation, le stockage, l'utilisation et la destruction de données à caractère personnel.

Pseudonymisation
Technique de traitement des données à caractère personnel permettant que ces données à caractère personnel ne puissent plus être attribuées à un individu spécifique sans l'utilisation d'informations supplémentaires, et qui devront être conservées de manière distincte et soumises à des mesures techniques et organisationnelles afin de garantir la non-attribution.

Glossaire terminologique

Règlement Européen sur la Protection des Données Personnelles

Règlement européen 2016/679 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, et abrogeant la directive 95/46/CE (RGPD en français ou GDPR en anglais). Il entrera en application le 25 mai 2018.

Responsable du traitement

Tout personne ou tout organisme qui, seul(e) ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.

Sous-traitants

Toute entité ou personne qui traite des données à caractère personnel pour le compte du responsable du traitement.

Transfert

Transfert de données à caractère personnel vers des pays situés en dehors de l'EEE ou vers des organisations internationales, qui est soumis à des restrictions énoncées dans le chapitre V du GDPR. De manière identique aux dispositions de la Directive sur la protection des données, il n'est pas nécessaire que les données soient physiquement transportées pour être considérées comme juridiquement transférées. Le fait de consulter, depuis un pays situé hors de l'E.E.E, des données situées dans l'E.E.E est considéré comme un transfert au sens du GDPR.

Practice Co-heads

Ruth Boardman
Partner
+44 (0)20 7415 6018
ruth.boardman@twobirds.com

Ariane Mole
Partner
+33 (0)1 42 68 6304
ariane.mole@twobirds.com

Experts in every office

twobirds.com

Aarhus & Abu Dhabi & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Düsseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Stockholm & Sydney & Warsaw