Bird & Bird

Guide du Règlement Général sur la Protection des Données (RGPD)

Sommaire

Le règlement général sur la protection des données (« RGPD ») est la pierre angulaire de la législation de l'Union européenne (« UE ») en matière de protection des données. Il s'applique à la quasi-totalité des personnes au sein de l'UE et aux organisations poursuivant des opérations commerciales dans ou avec l'UE. L'« *effet Bruxelles* » signifie que de nombreuses juridictions en dehors de l'Union européenne suivent les concepts du RGPD. Il est donc important pour les entreprises du monde entier de comprendre le RGPD.

Le guide résume les principaux aspects du RGPD et met en avant les actions les plus importantes à mener pour s'y conformer.

Ce résumé a été divisé en plusieurs sections qui, pour l'essentiel, correspondent à celles utilisées par le RGPD, elles-mêmes subdivisées en thèmes. Chaque sous-section commence par un court résumé et une liste d'actions suggérées. Nous avons également inclus un onglet bleu dans chaque sous-section pour vous orienter vers les sources pertinentes au sein du RGPD, ainsi que des détails sur les principales lignes directrices publiées par les régulateurs européens formant le Comité européen de la protection des données (« *CEPD* ») (et son prédécesseur, le groupe de travail « Article 29 »).

Nous avons finalisé les mises à jour de ce guide en décembre 2023 - à cette date, nous avions pris connaissance d'un nombre important de décisions de la Cour de justice de l'Union européenne (« *CJUE* ») analysant le RGPD. Nous avons fait référence à ces décisions tout au long du guide.

L'Union européenne poursuit également un programme numérique ambitieux avec de nombreux nouveaux textes législatifs, qui complètent désormais le RGPD. Nous avons indiqué comment le règlement sur les marchés numériques (*Digital Markets Act*), le règlement sur les services numériques (*Digital Services Act*), le règlement sur les données (*Data Act*), le règlement sur la gouvernance des données (*Data Governance Act*) et la Directive NIS2 doivent être lus en parallèle du RGPD. Bien qu'un consensus politique ait été trouvé à propos du règlement sur l'Intelligence Artificielle (*AI Act*), à la date de rédaction de cette introduction, aucun texte n'a été définitivement convenu, nous n'avons donc pas (encore) inclus d'indications sur les chevauchements avec le règlement sur l'Intelligence Artificielle. Nous continuerons à mettre à jour ce guide pour tenir compte de nouvelles décisions, lignes directrices et législations. Si vous souhaitez recevoir des mises à jour de notre part, n'hésitez pas à nous le faire savoir. En attendant, nous espérons que ce guide vous sera utile.

Champ d'application matériel et territorial

En bref

Le RGPD a étendu la portée de la législation européenne en matière de protection des données :

- Un responsable du traitement ou un sous-traitant établi dans l'UE entre dans son champ d'application lorsque des données à caractère personnel sont traitées « *dans le cadre des activités* » de son « *établissement* ». L'expression « *dans le cadre de* » est interprétée au sens large et il est facile de répondre aux critères d'un « *établissement* ».

- En l'absence de présence dans l'UE, le RGPD s'appliquera lorsque : (1) des données à caractère personnel relatives à une personne concernée située dans l'UE sont traitées en relation avec des biens/services qui lui sont proposés, ou (2) le comportement de personnes situées dans l'UE est « *suivi* ».

Bien qu'il s'agisse d'un règlement, le RGPD permet aux États membres de légiférer dans de nombreux domaines. Cela a d'ailleurs remis en cause l'objectif de cohérence du RGPD dans des domaines tels que le traitement des données des employés.

Le RGPD ne s'applique pas à certaines activités - y compris les traitements couverts par la Directive « *Police-Justice* »[1], qui a été adoptée comme le 27 avril 2016 (UE 2016/680) à des fins de sécurité nationale, et le traitement effectué par des personnes physiques uniquement pour des activités personnelles/domestiques.

Le RGPD est en vigueur depuis le 25 mai 2018.

À faire

Les organisations (i) disposant d'un établissement dans l'UE ou (ii) ne disposant pas d'un établissement dans l'UE, mais qui suivent ou ciblent avec des biens/services des personnes situées dans l'UE doivent :

- comprendre l'impact du RGPD et la jurisprudence/les lignes directrices pertinentes qui ont clarifié son application territoriale ; et

- déterminer une démarche de conformité, et continuer de vérifier leurs programmes de conformité.

Les organisations travaillant dans des domaines où des règles « *spéciales* »/sectorielles s'appliquent devraient déterminer si elles sont tenues de se conformer à des lois supplémentaires spécifiques des États membres et établir/maintenir des programmes de conformité appropriés en conséquence.

Les organisations doivent être conscientes que leur traitement peut également être réglementé (ou bientôt réglementé) par les « *Big 5* », les nouvelles lois de l'UE sur les données (le règlement sur les services numériques, le règlement sur les marchés numériques, le règlement sur les données, le règlement sur la gouvernance des données et le règlement sur l'IA). Les « *Big 5* » peuvent s'appliquer aux données à caractère personnel, mais aussi aux « *données* » au sens large (y compris les données non personnelles). Les organisations devront développer leurs programmes de conformité en matière de réglementation numérique afin de couvrir ces obligations supplémentaires.

[1] Titre complet : directive 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données

Champ d'application territorial

Responsables du traitement ou sous-traitants « *établis* » dans l'UE

Conformément à l'Article 3(1), le RGPD s'applique aux organisations qui ont des « *établissement*[s] » dans l'UE, lorsque des données à caractère personnel sont traitées « *dans le cadre des activités* » d'un tel établissement. Si ce critère est rempli, le RGPD s'applique, que le traitement effectif des données ait lieu dans l'UE ou non.

La notion d'« *établissement* » a été examinée par la CJUE dans l'affaire *Weltimmo c. NAIH* (C230/14) en 2015. Elle a confirmé que l'établissement est une expression « *large* » et « *souple* » qui ne doit pas dépendre de la forme juridique de l'organisation. Celle-ci peut être « *établie* » lorsqu'elle exerce « *une activité réelle et effective, même minime* » - par le biais d'une « *installation stable* » dans l'UE. La présence d'un seul représentant peut suffire. En l'espèce, il a été considéré que Weltimmo était établi en Hongrie, bien qu'enregistré en Slovaquie.

Les lignes directrices 3/2018 relatives au champ d'application territorial du RGPD du CEPD (« Lignes Directrices Champ d'Application ») s'alignent sur la jurisprudence susmentionnée concernant le champ d'application territorial, estimant que « le seuil de l'« *installation stable* », (ou « *dispositif stable* » *selon la terminologie employée dans le RGPD*) *peut être assez bas lorsque les activités d'un responsable du traitement portent principalement sur la fourniture de services en ligne*». *Dans certains cas, « la présence d'un seul employé ou agent d'une entité d'un État tiers dans l'Union […] pour constituer une installation stable* » pourrait suffire. Le CEPD précise toutefois que la simple présence d'un employé dans l'UE n'est pas suffisante. En effet, le traitement doit également être effectué dans le cadre des activités de cet employé - le fait qu'une organisation emploie du personnel dans l'UE ne signifie donc pas que le traitement de données à caractère personnel sans lien avec l'activité en question sera soumis au RGPD.

Les organisations qui ont des bureaux de vente dans l'UE qui promeuvent ou vendent de la publicité ou du marketing ciblant les résidents de l'UE seront probablement soumises au RGPD - puisque le traitement associé des données à caractère personnel est considéré comme étant « *indissociablement lié* » et donc effectué « *dans le cadre des activités* » de ces établissements de l'UE (affaire *Google Spain SL, Google Inc. c. AEPD, Mario Costeja Gonzalez* (C-131/12). Les Lignes Directrices Champ d'Application donnent l'exemple d'un site de commerce électronique chinois disposant d'un bureau à Berlin et menant des campagnes de marketing commercial sur les marchés de l'UE. Le fait que le bureau de Berlin contribue à rendre l'activité de commerce électronique rentable dans l'UE suffit, selon le CEPD, à considérer que l'entreprise chinoise traite des données à caractère personnel dans le cadre de son établissement allemand.

En revanche, les Lignes Directrices Champ d'Application précisent que l'accessibilité d'un site internet ne constitue pas à elle seule un établissement dans l'UE. Cela reflète également la jurisprudence de la CJUE - *VKI c. Amazon* (C-191/15)- qui a précédemment estimé qu'un site internet n'était pas un établissement. Le CEPD donne l'exemple d'une chaîne hôtelière qui cible les consommateurs de l'UE, mais qui n'est pas présente dans l'UE. L'analyse correcte serait celle de l'Article 3(2) (les dispositions extraterritoriales), et non celle de l'Article 3(1). Les lignes directrices du CEPD confirment également que ce n'est pas parce qu'une organisation peut être considérée comme « *établie* » pour une activité que toutes ses activités sont soumises au RGPD.

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

Conformément à l'Article 3(2), les organisations établies en dehors de l'UE seront soumises au RGPD lorsqu'elles traitent des données à caractère personnel relatives à des personnes concernées dans l'UE dans le cadre :

- de l'« *offre de biens ou de services* » (le paiement n'est pas requis) ; ou
- du « *suivi* » de leur comportement au sein de l'UE.

Pour l'offre de biens et de services (mais pas pour le suivi), la simple accessibilité d'un site à partir de l'UE n'est pas suffisante. Il doit être évident que l'organisation « *envisage* » que les activités soient dirigées vers des personnes concernées dans l'UE. En d'autres termes, l'élément déterminant sera la preuve de l'intention. Selon les Lignes Directrices Champ d'Application, les éléments qui seront pris en compte incluent :

- les références à l'UE ou à un État membre dans les supports promotionnels ;
- le paiement d'un moteur de recherche pour faciliter l'accès à un site internet dans l'UE ou

le lancement d'une campagne marketing destinée à un public de l'UE ;

- la nature internationale de l'activité en cause, telle que certaines activités touristiques ;
- la fourniture de numéros de téléphone ou d'adresses locales en lien avec un produit ou un service ;
- l'utilisation de noms de domaine de premier niveau faisant référence à l'UE ou à un État membre (par exemple, « .eu » ou ». de ») ;
- la fourniture de conseils pour un voyage depuis un État membre ;
- le fait de mentionner une clientèle internationale ou de fournir des témoignages de clients dans les supports promotionnels, en particulier lorsque les clients sont situés dans l'UE ;
- l'utilisation d'une langue ou d'une monnaie de l'UE ; et
- la fourniture de services de livraison dans l'UE.

Il n'est pas indiqué dans les Lignes Directrices Champ d'Application qu'un ou que tous ces éléments doivent être présents pour que le RGPD s'applique, mais plutôt qu'il s'agit du type d'indicateurs que les autorités de contrôle examineront afin de déterminer s'il existe une intention suffisante de cibler des individus dans l'UE. Il n'est pas certain que les organisations non européennes qui offrent des biens et des services aux entreprises de l'UE (par opposition aux particuliers) entreront bien dans le champ d'application du critère « *offre de biens et de services* » de l'Article 3(2)(a).

Contrairement à l'offre de biens et de services, le suivi ne requiert pas spécifiquement une intention. Néanmoins, les Lignes Directrices Champ d'Application précisent que « *L'utilisation du terme « suivi » implique que le responsable du traitement poursuit un objectif spécifique en vue de la collecte et de la réutilisation ultérieure des données pertinentes relatives au comportement d'une personne au sein de l'Union* ». Le « *facteur important* » pour identifier le suivi est la présence du « *suivi des personnes physiques sur l'internet, y compris l'utilisation ultérieure éventuelle de techniques de profilage* ». Le profilage, tel que défini par le RGPD, nécessite un traitement automatisé et l'évaluation des « *aspects personnels relatifs à une personne physique* », tels que la prédiction de l'état de santé, des préférences personnelles, de la situation économique, des performances professionnelles, de la localisation ou des déplacements.

En d'autres termes, la collecte passive, au fil du temps, de données à caractère personnel concernant le comportement d'une personne dans l'UE ne suffit pas pour constituer un suivi - il doit y avoir un objectif d'évaluation. Les Lignes Directrices Champ d'Application fournissent une liste d'exemples :

- la publicité comportementale et les activités de géolocalisation (en particulier à des fins de commercialisation) ;
- le suivi en ligne au moyen de cookies et des prises d'empreinte digitale (*fingerprinting*) ;
- un service en ligne d'analyse personnalisée de l'alimentation et de la santé ;
- la vidéosurveillance :
- les études de marché et autres études comportementales basées sur des profils individuels ; et
- le suivi de ou l'établissement de rapports réguliers sur l'état de santé d'une personne.

Bien que les Lignes Directrices Champ d'Application précisent que la surveillance ne doit pas nécessairement s'effectuer en ligne (par exemple, les technologies portables et autres dispositifs intelligents sont clairement mentionnés par le CEPD), il est intéressant de constater que la plupart des exemples fournis sont des exemples de suivi en ligne. D'autres cas d'utilisation courants, tels que les contrôles de lutte contre le blanchiment d'argent, la surveillance du courrier électronique dans le cadre du travail et la prévention de la fraude, ne sont pas mentionnés.

Le concept de « *suivi* » est actuellement examiné dans le cadre d'enquêtes et de décisions concernant Clearview AI, qui a élaboré une base de données à partir de données faciales provenant d'internet. Plusieurs régulateurs européens ont soutenu que le RGPD s'applique à Clearview parce que la mise à disposition de sa base de données « *est liée* » au suivi des personnes concernées par ses clients.

Focus sur la France : Extension du champ d'application territorial du RGPD en France par la loi « SREN »

En France, l'Article 3 de la loi Informatique et Libertés tel que modifié par la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (« SREN ») étend le champ d'application territorial du RGPD dans son interprétation française « *aux traitements de données à caractère personnel de personnes qui se trouvent sur le territoire français par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union européenne lorsque ces traitements sont liés au suivi du comportement de ces personnes au sein de l'Union européenne,* ***notamment par la collecte de leurs données à caractère personnel en vue de leur rapprochement avec des données liées à leur activité en ligne*** **».** Ainsi, la définition par la loi française de l'Article 3 du RGPD va au-delà de la position du CEPD qui considère que la collecte de données sur des personnes situées dans l'UE ne s'analyse pas nécessairement comme un « *suivi* » au sens de l'Article 3 du RGPD. Si ces personnes se trouvent sur le territoire français et que leurs données sont collectées en vue de leur rapprochement avec des données liées à l'activité en ligne, alors le RGPD et la Loi Informatique et Libertés s'appliqueront.

En ce qui concerne les trois critères de l'Article 3 du RGPD (établissement, ciblage et suivi), un arrêt de la Cour d'appel britannique dans l'affaire *Soriano v Forensic News* ([2021] EWCA Civ 1952 – disponible en anglais uniquement) suggère que les critères peuvent être interprétés de manière plus large. La Cour a estimé qu'un groupe de journalistes américains associés au site internet Forensic News avait une « *probabilité raisonnable* » de remplir l'un des critères de l'Article 3 (ce qui signifie que l'affaire peut être entendue). La Cour a déclaré qu'une « *activité minimale* » d'abonnement à des publications dans l'UE pouvait constituer un établissement, que la production de contenus journalistiques pouvait constituer une « *offre* » de services et que la collecte et le tri de données journalistiques concernant un individu résidant dans l'UE pouvaient constituer un « *suivi* ». Toutefois, à la suite du Brexit, l'affaire pourrait avoir un impact plus limité dans l'UE qu'au Royaume-Uni, et elle n'a pas encore été entendue dans son intégralité par la Cour d'appel.

Les organisations soumises à l'Article 3(2) du RGPD doivent désigner un représentant dans l'un des États membres de l'UE où se trouvent les personnes dont les données sont traitées. Une obligation équivalente de désignation d'un représentant basé au Royaume-Uni existe également dans le cadre du RGPD britannique. Les Lignes Directrices Champ d'Application confirment que le RGPD n'établit pas de responsabilité substitutive pour les représentants : ils ne peuvent être tenus responsables que de leurs obligations directes en vertu du RGPD (c'est-à-dire en vertu des Articles 30 et 58(1)). Bird & Bird aide désormais les organisations non européennes et non britanniques à remplir cette obligation et peut être désigné comme représentant RGPD au Royaume-Uni et dans l'UE. Contactez Bird & Bird Privacy Solutions si vous souhaitez obtenir plus d'informations sur nos services.

Lorsque le droit d'un État membre de l'UE s'applique en vertu du droit international public

Le considérant 25 donne l'exemple d'une mission diplomatique ou d'un poste consulaire. Les Lignes Directrices Champ d'Application mentionnent également l'exemple d'un paquebot de croisière battant pavillon allemand (en raison de son enregistrement) dans les eaux internationales. Dans cet exemple, le navire de croisière sera soumis au RGPD, selon le CEPD. Une solution similaire pourrait être étendue aux avions.

Exclusions

Certaines activités ne relèvent pas du champ d'application du RGPD (énumérées ci-dessous).

En outre, le RGPD reconnaît que les droits relatifs à la protection des données ne sont pas absolus et doivent être mis en balance (proportionnellement) avec d'autres droits - y compris la « *liberté d'entreprendre* ». (Pour la capacité des États membres à introduire des exemptions, voir la section sur les dérogations et conditions particulières). Étant donné que le RGPD crée un régime strict dans de nombreux domaines de la protection des données, avec sans doute plus de bâtons que de carottes réglementaires, les entreprises peuvent trouver utile de se référer au considérant 4 lorsque le besoin s'en fait sentir.

Le RGPD ne s'applique pas aux traitements des données à caractère personnel (ces exemptions générales sont très similaires, dans les cas suivants, aux dispositions équivalentes incluses dans la directive sur la protection des données) :

- pour des activités qui ne relèvent pas du champ d'application de la législation de l'UE

(par exemple, les activités relatives à la sécurité nationale) ;

- dans le cadre de la politique étrangère et de sécurité commune de l'UE ;
- par les autorités compétentes à des fins de prévention, d'enquête, de détection ou de poursuite d'infractions pénales et de questions connexes (c'est-à-dire lorsque la Directive « Police-Justice » s'applique) ;
- par les institutions de l'UE, où un instrument juridique spécifique, le règlement (UE) 2018/1725 entré en vigueur le 11 décembre 2018, vise à aligner les règles applicables aux institutions de l'UE sur celles prévues par le RGPD. Les règles ne sont toutefois pas identiques ;
- par une personne physique ou dans le cadre d'une « ***activité exclusivement personnelle ou domestique*** ». Cela couvre la correspondance et la tenue de carnets d'adresses, mais aussi le réseautage social et les activités en ligne menées à des fins sociales et domestiques. Il s'agit d'une extension des principes énoncés dans l'affaire *Bodil Lindqvist* (C-101/01) avant l'avènement des réseaux sociaux. Dans cette affaire, la CJUE a noté que le partage de données avec l'internet au sens large « *de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes* » ne pouvait pas relever de cette exemption, qui, selon elle, devrait être limitée aux activités « *qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers* ». Le RGPD reste applicable aux responsables du traitement et aux sous-traitants qui « *fournissent les moyens de traiter* » qui relève de cette exemption.

Le RGPD est déclaré « *sans préjudice* » de l'application des règles de la directive sur le commerce électronique (2000/31/CE), en particulier celles concernant la responsabilité des « *prestataires intermédiaires* ». Ces exemptions de responsabilité ont été remplacées par des exemptions équivalentes (et actualisées) dans le règlement sur les services numériques (2022/2065), qui exempte les simples fournisseurs de services de transport, de mise en cache et d'hébergement de toute responsabilité dans certaines circonstances, mais impose également des obligations supplémentaires de vigilance raisonnable à ces fournisseurs de services. L'articulation entre le RGPD, la directive sur le commerce électronique, le règlement sur les services numériques et les autres nouvelles lois sur les données du « *Big 5* » (le règlement sur les services numériques, le règlement sur les marchés numériques, le règlement sur les données, le règlement sur la gouvernance des données et le règlement sur l'IA) n'est pas simple. Il est indiqué que les « *Big 5* » sont « *sans préjudice* » de l'application du RGPD et il est souligné par endroits que la protection des données à caractère personnel est « *régie exclusivement* » par la législation sur la protection des données. Toutefois, les « *Big 5* » contiennent également un certain nombre de dispositions qui concernent directement la protection des données (par exemple, l'interdiction par le règlement sur les services numériques du profilage à des fins publicitaires sur la base de données relatives à des mineurs ou à des catégories particulières de données dans certains scénarios) de sorte que, en pratique, plusieurs fondements juridiques peuvent être invoqués dans le cadre de l'application de la législation sur la protection des données. Dans d'autres domaines, cependant, la séparation est plus claire (par exemple, la responsabilité des fournisseurs d'accès à internet (« FAI ») eu égard aux contenus illégaux continuera probablement d'être retenue sur le fondement du règlement sur les services numériques, tel que cela était le cas sous l'empire de la directive sur le commerce électronique). Il convient de noter que les « *Big 5* » s'appliquent à la fois aux données à caractère personnel et non personnelles et qu'ils créent parfois des droits similaires à ceux dont les personnes concernées bénéficient en vertu du RGPD.

Les organisations doivent être prêtes à développer de façon considérable leurs programmes de conformité pour se mettre en conformité avec les « *Big 5* ».

Règlement et droit national

En tant que règlement, le RGPD est directement applicable dans les États membres sans qu'il soit nécessaire d'adopter de lois de transposition en droit national.

Toutefois, à de nombreuses occasions, le RGPD permet aux États membres de légiférer en matière de protection des données. Il s'agit notamment des cas où le traitement des données à caractère personnel est requis pour se conformer à une obligation légale, lié à une mission d'intérêt public ou effectué par un organe doté de l'autorité publique. De nombreux articles du RGPD indiquent également que leurs dispositions peuvent être précisées ou restreintes par le droit des États membres. Le traitement des données relatives aux employés est un autre domaine

important dans lequel les États membres sont susceptibles d'adopter des approches divergentes.

Les organisations travaillant dans des secteurs où des règles spéciales s'appliquent (par exemple, la santé et les services financiers) devraient (1) déterminer si elles bénéficient de ces « *règles spéciales* » dans la mesure où ces dispositions ont été introduites dans les juridictions concernées afin de préciser ou libéraliser le RGPD et (2) d'adapter leurs politiques en conséquence.

Où puis-je trouver ces dispositions ?

Champ d'application matériel, Article 2, considérants 15 à 21

Champ d'application territorial, Article 3, considérants 22 à 25

Concepts clés à connaître

En bref

Voici les concepts clés du RGPD qui devraient constituer la base de la structure des programmes de conformité des entreprises :

- Transparence et consentement - Les exigences strictes du RGPD relatives aux informations à fournir et aux autorisations requises de la part des personnes, notamment le fait que le consentement doit être univoque et ne doit pas être présumé, impliquent qu'il est nécessaire, en raison des nombreuses mentions d'information sur la protection des données, des formulaires de collecte du consentement et des bandeaux de consentement aux cookies, de fournir plus d'information ou d'obtenir des niveaux de consentement plus pointu que dans d'autres juridictions.

- Vie privée des enfants - étant donné l'importance accordée à la sécurité en ligne, un certain nombre de régulateurs européens ont publié des lignes directrices spécifiques sur la manière dont les services en ligne peuvent se conformer au RGPD, notamment en ce qui concerne le traitement des données relatives aux enfants, et plusieurs amendes importantes ont été prononcées dans ce domaine. En outre, lorsque les services en ligne/utilisant internet se fondent sur le consentement comme base juridique de traitement, ils doivent vérifier l'âge et recueillir le consentement d'un parent si l'âge de l'utilisateur est inférieur à l'âge précisé par la loi (l'« *âge minimum du consentement numérique* » - 16 ans par défaut, bien que certains États membres l'aient abaissé à 13, 14 ou 15 ans).

- Données réglementées - les définitions de « *données à caractère personnel* » et de « *catégories particulières de données* » sont larges. En particulier, les lignes directrices et la jurisprudence suggèrent qu'en pratique, il sera très difficile d'aboutir à des données « *anonymes* » (qui ne seront pas considérées comme des données à caractère personnel), bien que les approches réglementaires varient d'une juridiction à l'autre.

- Pseudonymisation – technique de protection de la vie privée par laquelle les informations qui permettent d'attribuer des données à une personne donnée sont conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir qu'elles ne sont pas attribuées à cette personne.

- Violation de données à caractère personnel - les obligations de notification s'appliquent à tous les responsables du traitement et à tous les sous-traitants, quel que soit leur secteur. (Les fournisseurs de services de télécommunications sont soumis aux obligations de notification des violations prévues par la directive sur la vie privée et les communications électroniques).

- Protection des données dès la conception et responsabilité - les organisations sont tenues d'adopter des mesures techniques et organisationnelles significatives pour se conformer au RGPD et être en mesure d'attester de leur conformité.

- Droits renforcés - Les personnes concernées bénéficient de droits importants, notamment du droit à l'oubli, du droit à la portabilité des données et du droit de ne pas faire l'objet d'une prise de décision individuelle entièrement automatisée.

- Les autorités de contrôle et le CEPD - la surveillance réglementaire de la protection des données se fait au niveau national par le biais d'un réseau d'autorités de contrôle, le CEPD jouant un rôle de coordination. Le CEPD supervise également la procédure de résolution des litiges au titre de l'Article 65 relatif à l'application de la législation en matière de traitement transfrontalier.

A faire

Reportez-vous aux « *A faire* » des sections ci-dessous qui traitent de ces sujets en détail.

Les dispositions et obligations du RGPD sont nombreuses, mais les concepts suivants sont particulièrement importants et doivent être pris en compte par les organisations dans leurs programmes de conformité. Des informations plus détaillées sur chacun d'entre eux sont incluses ailleurs dans ce guide.

Consentement

Les conditions d'obtention du consentement sont strictes :

- Le groupe de travail « Article 29 » (aujourd'hui CEPD) a déclaré dans ses lignes directrices sur le consentement que les informations suivantes sont nécessaires a minima pour que le consentement soit valable : (i) l'identité du responsable du traitement, (ii) la finalité de chacune des opérations de traitements pour lesquels le consentement est sollicité, (iii) les (types de) données collectées et utilisées, (iv) l'existence du droit de retirer son consentement, (v) des informations sur l'utilisation des données pour la prise de décision automatisée conformément à l'Article 22(2)(c), le cas échéant, et (vi) les risques éventuels liés à la transmission de données en raison de l'absence de décision d'adéquation et de garanties appropriées, telles que décrites à l'Article 46.

- Il existe une présomption selon laquelle le consentement n'est pas valable à moins que : (i) des consentements distincts aient été obtenus pour de multiples opérations de traitement à différentes fins, (ii) le consentement n'est pas une condition de fourniture d'un service, et (iii) il n'y a pas de « *déséquilibre des rapports de force* » entre la personne concernée et l'organisation.

Le consentement n'est pas le seul mécanisme permettant de justifier le traitement des données à caractère personnel, les autres bases juridiques disponibles étant l'exécution d'un contrat, le respect d'une obligation légale (de l'État membre ou de l'UE), ou les intérêts légitimes de l'organisation, la sauvegarde des intérêts vitaux ou le cadre d'une mission d'intérêt public.

Pour plus d'informations sur ce sujet, voir les sections sur le consentement, les enfants, les catégories particulières de données et la licéité du traitement (voir la section sur les principes de protection des données).

Transparence

Les organisations doivent fournir des informations détaillées aux individus sur le traitement de leurs données à caractère personnel. Le non-respect des obligations de transparence par les responsables du traitement a donné lieu aux amendes parmi les plus élevées à ce jour en vertu du RGPD.

La liste des informations à fournir occupe plusieurs pages dans le RGPD ; les responsables du traitement sont néanmoins tenus de fournir ces dispositions de manière concise, transparente, intelligible et facilement accessible. Le recours à des mentions d'information « *par niveaux* » (contenant des liens vers des informations supplémentaires) est une solution courante, bien que certains régulateurs (tels que l'autorité irlandaise de protection des données (« DPC ») dans ses décisions contre les services Instagram et Facebook de Meta [disponible en anglais uniquement]) aient noté qu'une approche en plusieurs niveaux n'aidera pas à la conformité dans la mesure où elle entraîne une surcharge d'informations pour les personnes concernées. La DPC a également suggéré (voir la décision distincte concernant les pratiques de transparence de WhatsApp, qui fait actuellement l'objet d'un recours) que les organisations devront « *rassembler* » certains types d'informations dans leurs mentions (par exemple, les catégories de données, la finalité, la base juridique et les destinataires tiers). De nombreux responsables du traitement ont commencé à le faire en utilisant des tableaux.

Il est déconseillé aux organisations d'utiliser des « *interfaces truquées* » (« *dark patterns* ») pour manipuler l'utilisateur et l'amener à faire des choix préjudiciables à sa vie privée. Le CEPD a publié des lignes directrices sur les interfaces truquées (« dark patterns ») (disponibles uniquement en anglais), dont la version finale a été publiée en 2023. La loi sur les services numériques (Digital Services Act) prévoit une interdiction similaire d'utilisation d'« *interfaces truquées* » par les plateformes en ligne, mais cette interdiction ne

s'appliquera pas aux pratiques couvertes par le RGPD.

Les informations de transparence des services susceptibles d'être consultés par des enfants sont soumises à des normes plus strictes par les autorités européennes de protection des données.

Le cas échéant, les organisations sont censées mettre en œuvre des mentions d'information adaptées à l'âge des enfants qui y accèdent, ce qui peut impliquer (par exemple) l'utilisation de vidéos, de sons, de graphiques et/ou d'un langage simplifié.

Pour plus d'informations à ce sujet, voir la section sur les mentions d'information.

Les enfants

Conseils sur la protection de la vie privée des enfants

La sécurité en ligne des mineurs est devenue un sujet très débattu en Europe et dans le monde depuis la mise en œuvre du RGPD. C'est pourquoi un certain nombre d'autorités européennes de contrôle ont pris des mesures dans ce domaine et ont publié des lignes directrices spécifiques sur le traitement des données relatives aux enfants.

On peut notamment citer *l'Information Commissioner's Children's Code* publié par l'autorité britannique et le *Data Protection Commissioner's Fundamentals for a Child-Oriented Approach to Data Processing* publié par l'autorité irlandaise. Leurs thématiques sont axées sur la conception des services et incluent la transparence, la garantie de l'âge, les paramètres par défaut et les techniques de persuasion (« *nudge* » en anglais).

Les organisations devront non seulement se conformer aux lignes directrices relatives à la protection de la vie privée des enfants si leurs services s'adressent directement aux enfants, mais aussi si leurs services sont susceptibles d'être consultés par des enfants. Les organisations devront probablement vérifier l'accessibilité de leurs services par des enfants dès le début de la conception de leurs services en ligne.

À ce jour, des amendes considérables ont été infligées pour violation des règles de protection de la vie privée des enfants. Par exemple, en 2022, la DPC a infligé une amende de 405 millions d'euros à Meta pour avoir rendu publiques par défaut les coordonnées des enfants, en violation du RGPD.

L'âge du consentement numérique

Les enfants de moins de 13 ans ne peuvent pas, par eux-mêmes, donner leur consentement au traitement de leurs données à caractère personnel dans le cadre de services en ligne ou sur internet (un point qui se recoupe, mais qui est distinct de ce qui est abordé dans les lignes directrices sur la protection de la vie privée des enfants).

Par conséquent, pour les enfants âgés de 13 à 15 ans (inclus), la règle générale est que si une organisation utilise le consentement comme base juridique pour traiter leurs données à caractère personnel, le consentement parental doit être obtenu, à moins que l'État membre concerné ne légifère pour réduire le seuil d'âge par défaut (16 ans). Ils ne peuvent pas l'abaisser en dessous de 13 ans. Les enfants âgés de 16 ans ou plus peuvent donner eux-mêmes leur consentement au traitement de leurs données à caractère personnel.

Il convient toutefois de noter que le consentement n'est pas la seule base légale disponible pour le traitement des données à caractère personnel des enfants. Par exemple, les responsables du traitement de services en ligne peuvent se fonder sur l'exécution du contrat ou l'intérêt légitime, le cas échéant. Toutefois, il pourrait être plus difficile d'atteindre le seuil requis pour d'autres bases juridiques lorsque des enfants sont concernés - par exemple, il pourrait être plus difficile de satisfaire à une mise en balance des intérêts en présence.

Il n'existe pas de règles spécifiques relatives au consentement parental pour le traitement des données hors ligne : les règles habituelles des États membres en matière de capacité s'appliquent dans ce cas.

Pour plus d'informations sur ce sujet, voir la section sur les enfants.

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

Le RGPD s'applique à toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement. L'identification sera évaluée en tenant compte de « *l'ensemble des moyens raisonnables susceptibles d'être utilisés* ». Avant le RGPD, l'arrêt de la CJUE dans l'affaire *Patrick Breyer c. Allemagne* (C-582/14) d'octobre 2016 (« *Breyer* ») a confirmé qu'une personne n'est pas identifiable lorsque le risque d'identification « *paraît en réalité insignifiant* ».

Les lignes directrices divergent quant à la question de savoir si l'identification doit être évaluée du point de vue de n'importe qui dans le monde, ou uniquement du point de vue de la partie qui cherche à considérer les données comme anonymes. La décision Breyer et l'arrêt T-557/20 du Tribunal semblent favoriser cette dernière interprétation. La question de savoir si les données « *se rapportent à* » une personne physique dépend du fait qu'elles sont liées à cette personne en raison « *de son contenu, sa finalité ou son effet* » (*Peter Nowak v Data Protection Commissioner*, C-434/16 [2017], [35]), ce qui est un critère peu exigeant et susceptible d'être satisfait si une personne est identifiable.

Les considérants du RGPD soulignent que certaines catégories de données en ligne peuvent être personnelles - par exemple, les données constituées d'identifiants en ligne, d'identifiants d'appareils, d'identifiants de cookies et d'adresses IP ou associées à ces identifiants. Nous savons depuis l'arrêt Breyer qu'une adresse IP dynamique peut constituer une donnée à caractère personnel ; le considérant 30 du RGPD renforce ce point.

Les « *catégories particulières de données* » (souvent appelées « *données sensibles* ») comprennent les données génétiques et les données biométriques utilisées pour identifier les personnes concernées. Le traitement des catégories particulières de données est soumis à des conditions plus strictes.

Pseudonymisation

La pseudonymisation est une technique de protection de la vie privée par laquelle les informations qui permettent d'attribuer des données à une personne donnée sont conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir qu'elles ne sont pas attribuées à cette personne.

Les informations pseudonymisées restent une forme de données à caractère personnel, mais l'utilisation de la pseudonymisation est encouragée :

- il s'agit d'un facteur à prendre en compte pour déterminer si le traitement est « *incompatible* » avec les finalités pour lesquelles les données à caractère personnel ont été initialement collectées et traitées ;
- elle est incluse en tant qu'exemple de technique pouvant satisfaire aux exigences de mise en œuvre de la « *protection de la vie privée dès la conception et de protection des données par défaut* » (voir la section sur les obligations de gouvernance des données) ;
- elle peut contribuer à satisfaire aux obligations du RGPD en matière de sécurité des données (voir la section sur les violations de données à caractère personnel et notification) ; et
- pour les organisations qui souhaitent utiliser des données à caractère personnel à des fins de recherche historique ou scientifique ou à des fins statistiques, l'utilisation de données pseudonymisées est recommandée.

Notification des violations de données à caractère personnel

Le RGPD prévoit un régime de notification des violations de données à caractère personnel pour tous les responsables du traitement de données (et tous les sous-traitants), quel que soit le secteur dans lequel ils opèrent. Certaines organisations (principalement les fournisseurs de services de télécommunications) sont soumises aux obligations de notification des violations prévues par la directive sur la vie privée et les communications électroniques.

Les obligations de notification (aux autorités de contrôle et éventuellement aux personnes concernées) sont potentiellement déclenchées par « *la destruction, la perte ou 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, de manière accidentelle ou illicite ».

Pour plus d'informations sur ce sujet, voir la section sur les violations de données à caractère personnel et notification.

Protection des données dès la conception et responsabilité

Les organisations doivent être en mesure de démontrer qu'elles respectent les principes du RGPD, notamment en adoptant certaines mesures de « *protection des données dès la conception* » (par exemple, l'utilisation de techniques de pseudonymisation), des programmes de formation du personnel et des politiques et procédures.

Lorsqu'un traitement « *à risque élevé* » est prévu (comme les activités de contrôle, les évaluations systématiques ou le traitement de catégories particulières de données), une analyse d'impact sur la protection des données (« AIPD ») doit être effectuée et documentée. Lorsqu'une AIPD aboutit à la conclusion qu'il existe effectivement un risque élevé et non atténué pour les personnes concernées, les responsables du traitement doivent en informer l'autorité de contrôle (c'est-à-dire l'autorité de protection des données) et obtenir son avis sur l'adéquation des mesures proposées par la AIPD pour réduire les risques liés au traitement.

Les responsables du traitement et les sous-traitants peuvent décider de désigner un délégué à la protection des données (« DPD ») ou *data protection officer* en anglais(« DPO »). Cette désignation est obligatoire pour les organismes du secteur public, ceux qui sont impliqués dans certaines activités de traitement ou de contrôle sensibles répertoriées ou lorsque la législation locale exige une telle désignation. Les entreprises appartenant à un groupe peuvent désigner conjointement un délégué à la protection des données.

Pour plus d'informations sur ces sujets, voir la section sur les obligations de gouvernance des données.

Droits renforcés pour les individus

Le RGPD prévoit un large éventail de droits pour les individus en ce qui concerne leurs données à caractère personnel.

Il s'agit notamment du droit à l'oubli, du droit de demander le transfert de leurs données à caractère personnel à une nouvelle organisation, du droit de s'opposer à certaines activités de traitement et du droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé et produisant sur ceux-ci des effets juridiques ou d'autres effets significatifs.

Pour plus d'informations sur ces sujets, voir la section sur les mentions d'information et les sections suivantes.

Les autorités de contrôle et le CEPD

Le règlement sur la gouvernance des données (« DGA ») anticipe le fait que des services intermédiaires viseront à aider les personnes concernées à exercer leurs droits et à permettre aux organisations d'accéder à leurs données. Les prestataires de services intermédiaires en matière de données doivent remplir les conditions énoncées dans DGA qui visent à garantir la loyauté et l'indépendance de ces services. Ils doivent également agir dans l'intérêt des personnes concernées (DGA, Article 12).

Les régulateurs de la protection des données sont appelés autorités de contrôle. Une autorité de contrôle unique située dans l'État membre dans lequel une organisation a son établissement « *principal* » prendra la direction des plaintes et des enquêtes transfrontalières concernant la conformité de cette organisation avec le RGPD.

Le CEPD a pour mission (entre autres) d'émettre des avis sur des questions particulières et de statuer sur les litiges découlant des décisions des autorités de contrôle dans le cadre de la procédure de règlement des litiges prévue à l'Article 65.

Pour plus d'informations sur ce sujet, voir la section 6 : Régulateurs.

Principes de protection des données

En bref

Les principes régissant la protection des données sont les piliers du RGPD au sens large. Les principes sous-tendent les obligations spécifiques des responsables du traitement des chapitres suivants. Elles incluent un principe de responsabilité, les responsables devant démontrer en quoi le traitement qu'ils mettent en œuvre respectent ces principes.

À faire

Identifier les moyens pour garantir le respect des principes de protection des données – par exemple via l'adhésion à des codes de conduites approuvés, garder une trace des décisions relatives au traitement de données et, le cas échéant, via la réalisation d'analyses d'impact.

Commentaire

Les principes sont les éléments fondamentaux du RGPD, sur lesquels reposent les obligations ultérieures imposées aux responsables du traitement. Les principes sont les suivants :

Licéité, loyauté et transparence

Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente en relation avec la personne concernée.

Limitation des finalités

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 archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques est réputé compatible avec les finalités initiales du traitement, si les conditions énoncées à l'Article 89(1) (qui énonce les garanties et les dérogations relatives au traitement à de telles fins) sont remplies.

Minimisation des données

Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Exactitude

Les données à caractère personnel doivent être exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes soient effacées ou rectifiées sans délai (compte tenu des finalités pour lesquelles les données sont traitées).

Limitation de la conservation

Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées. Les données à caractère personnel peuvent être conservées plus longtemps dans la mesure où elles sont traitées uniquement à des fins archivistiques dans l'intérêt public, ou à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'Article 89(1), c'est-à-dire sous réserve de l'utilisation de mesures techniques et organisationnelles appropriées, ce que certains États membres ont prévu dans leur législation nationale.

Intégrité et confidentialité

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

Principe de responsabilité

Le responsable du traitement est responsable du respect de ces principes et doit être en mesure de le démontrer.

Principes et application

Les principes sont régulièrement cités par les autorités de contrôle dans le cadre de mesures d'exécution. Bien que certaines obligations soient soumises à un seuil de sanction inférieur en vertu de l'Article 83(4) du RGPD, toutes les violations des principes sont soumises au seuil supérieur de l'Article 83(5).

Où puis-je trouver ces dispositions ?

Article 5 et considérant 39

Licéité du traitement et traitement ultérieur

En bref

Le RGPD énonce différents fondements permettant de traiter de manière licite les données à caractère personnel en vertu de l'Article 6. Ceux-ci incluent notamment le consentement, l'exécution d'un contrat, l'existence d'un intérêt légitime ou d'une obligation légale.

Les exigences relatives à la validité du consentement sont strictes et des règles supplémentaires s'appliquent au traitement des données des enfants en ligne.

Il existe des restrictions spécifiques sur la possibilité d'avoir recours à « *l'intérêt légitime* » comme base de traitement, particulièrement dans le secteur public.

En outre, il y a une liste non-exhaustive de critères à prendre en compte dans le traitement de données à caractère personnel pour une nouvelle finalité incompatible avec la finalité pour laquelle les donnes ont été initialement collectées.

À faire

Veillez à ce que les bases juridiques du traitement invoquées par votre organisation au titre du RGPD soient claires et à ce qu'elles soient documentées dans vos politiques de confidentialité.

Si vous vous appuyez sur le consentement, assurez-vous que la qualité de ce consentement répond aux exigences du RGPD (voir la section sur le consentement pour plus de détails).

Veillez à ce que vos processus de gouvernance interne vous permettent de prouver comment les décisions d'utiliser des données à caractère personnel à des fins de traitement ultérieur ont été prises et que les facteurs pertinents ont été pris en compte.

Commentaire

Pour que le traitement des données à caractère personnel soit valide au sens du RGPD, les responsables du traitement doivent remplir une condition de l'Article 6(1) du RGPD (une base juridique supplémentaire est nécessaire pour traiter des catégories particulières de données, en plus d'une base juridique prévue à l'Article 6 - voir la section sur les catégories particulières de données et la licéité du traitement). La base juridique pertinente pour chaque finalité du traitement doit être décrite dans les mentions d'information (voir notre section sur les mentions d'information). Comme expliqué dans les sections sur les droits des personnes concernées, les personnes peuvent avoir des droits différents en fonction de la base juridique sur laquelle repose le traitement. Les bases juridiques pour le traitement sont les suivantes :

6 (1) (a) - Consentement de la personne concernée

Le test du RGPD pour un consentement valide est exigeant et place la barre très haut pour les responsables du traitement (voir la section le consentement). Des conditions particulières sont également imposées lorsque le consentement des enfants est demandé en ligne (voir la section sur les enfants).

6 (1) (b) - Nécessaire à l'exécution d'un contrat avec la personne concernée ou à l'exécution de mesures précontractuelles dans le cadre d'un tel contrat

Le traitement doit être nécessaire à la conclusion ou à l'exécution d'un contrat avec la personne concernée. Il s'agit d'une base juridique souhaitable, lorsqu'elle est disponible, étant donné les droits supplémentaires dont disposent les personnes concernées lorsque les responsables du traitement s'appuient sur le consentement ou les intérêts légitimes.

En octobre 2019, le CEPD a publié ses lignes directrices 2/2019 sur le traitement des données à caractère personnel en vertu de l'Article 6(1)(b) dans le cadre de la fourniture de services en ligne aux personnes concernées. Concernant la portée de cette condition, le CEPD indique que « *[l]e simple fait de mentionner ou de faire référence au traitement de données dans un contrat ne suffit pas à faire entrer le traitement en question dans le champ d'application de l'Article 6, paragraphe 1, point b). Par ailleurs, le traitement peut être objectivement nécessaire même s'il n'est pas expressément mentionné dans le contrat* ».

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

L'Article 6(3) et les considérants 41 et 45 précisent que l'obligation légale en question doit être :

- une obligation imposée par le droit d'un l'État membre ou de l'Union européenne à laquelle le responsable du traitement est soumis ; et
- « *claire et précise* » et son application doit être prévisible pour les personnes qui y sont soumises.

Les considérants précisent que la « *mesure législative* » en question ne doit pas nécessairement être prévue par la loi (c'est-à-dire que la *common law* suffit, si elle répond au critère de clarté et de précision). Une obligation légale peut couvrir plusieurs opérations de traitement effectuées par le responsable du traitement, de sorte qu'il n'est peut-être pas nécessaire d'identifier une obligation légale spécifique pour chaque activité de traitement.

6 (1) (d) - Nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique lorsque la personne concernée n'est pas en mesure de donner son consentement.

Le considérant 46 suggère que cette base juridique est disponible pour les traitements qui sont nécessaires à des fins humanitaires (par exemple, la surveillance des épidémies) ou dans le cadre d'urgences humanitaires (par exemple, la réaction aux catastrophes naturelles). Le considérant indique que dans les cas où les données à caractère personnel sont traitées dans l'intérêt vital d'une personne autre que la personne concernée, cette base juridique du traitement ne devrait être invoquée qu'à titre exceptionnel et uniquement lorsqu'aucune autre base juridique n'est disponible.

6 (1) (e) - Nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

L'Article 6(3) et le considérant 45 précisent que cette base juridique ne s'applique que lorsque la mission accomplie, ou l'autorité du responsable du traitement, est prévue par le droit de l'Union ou

le droit d'un État membre auquel le responsable du traitement est soumis. Il s'agit de la principale alternative pour les autorités publiques, qui ne peuvent pas traiter des données à caractère personnel dans le cadre de leurs missions publiques sur la base d'intérêts légitimes.

6 (1) (f) - Nécessaire aux fins d'intérêts légitimes

Comme indiqué ci-dessus, cette base juridique ne peut plus être invoquée par les autorités publiques qui traitent des données à caractère personnel dans l'exercice de leurs fonctions. Les considérants 47 à 50 précisent ce qui peut être considéré comme un « *intérêt légitime* ». Les lignes directrices du CEPD indiquent clairement qu'une mise en balance des intérêts légitimes en présence est requise lorsque l'on s'appuie sur cette base juridique, qui doit être mise à la disposition des personnes concernées sur demande (voir la section sur les intérêts légitimes pour plus de détails).

Les États membres sont autorisés à introduire des dispositions spécifiques pour fournir une base au titre de l'Article 6(1)(c) et (e) (traitement dû à une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique). Cela a donné lieu à des différences entre les États membres de l'UE (pour plus de détails, voir la section sur les dérogations et conditions particulières).

Les bases légales sur lesquelles les plateformes en ligne s'appuient pour traiter des données à caractère personnel ont été examinées par la CJUE et le CEPD. Dans la décision *Bundeskartellamt* (C-252/21), la CJUE a suggéré une interprétation étroite de la nécessité contractuelle, notant qu'elle couvrirait le traitement qui est « *objectivement indispensable* » pour l'objet principal du contrat, et du traitement fondé sur les intérêts légitimes. Toutefois, la CJUE a noté que le fait qu'une plateforme ait une position dominante ne l'empêche pas de s'appuyer sur le consentement de l'utilisateur.

Dans sa décision contraignante 03/2022 (disponible uniquement en anglais) le CEPD a demandé à la DPC de constater que l'exécution d'un contrat n'était pas une base juridique appropriée sur laquelle Meta pouvait s'appuyer pour traiter les données à caractère personnel des utilisateurs à des fins de publicité ciblée. Le 7 décembre 2023, le CEPD a adopté une décision contraignante urgente sur ce sujet, concernant l'utilisation de l'exécution d'un contrat et des intérêts légitimes pour le traitement de certaines données à des fins de publicité ciblée.

Des considérations supplémentaires sur la base légale s'appliquent en vertu du règlement sur les marchés numériques (« DMA »). Le règlement sur les marchés numériques ne s'applique qu'à un petit nombre de très grands « *gatekeepers* » (ou « *contrôleurs d'accès* ») (dont la liste figure ici (disponible en anglais uniquement)). La Commission européenne désigne des contrôleurs d'accès pour des services spécifiques. L'Article 5 du DMA interdit aux contrôleurs d'accès d'effectuer certains traitements de données à caractère personnel à moins qu'ils n'aient obtenu le consentement de la personne concernée. Les restrictions s'appliquent :

- au traitement des données à caractère personnel des utilisateurs finaux pour les services de publicité en ligne, lorsque les données à caractère personnel concernent les interactions de l'utilisateur final avec des tiers qui utilisent les services du contrôleur d'accès ;
- à la combinaison de données à caractère personnel provenant d'un service réglementé avec des données à caractère personnel provenant d'autres services ;
- l'utilisation croisée de données à caractère personnel provenant d'un service réglementé avec des données à caractère personnel provenant d'autres services ; et
- à l'inscription des utilisateurs finaux à d'autres services du contrôleur d'accès afin de combiner les données à caractère personnel.

Si le traitement listé ci-dessus est requis par la législation (de l'UE ou d'un État membre), pour protéger des intérêts vitaux ou pour une mission réalisée dans l'intérêt public, le contrôleur d'accès peut néanmoins procéder au traitement.

Traitement ultérieur

Le RGPD énonce également (à l'Article 6(4) les paramètres qu'un responsable du traitement doit prendre en compte pour évaluer si une nouvelle finalité de traitement est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées. Lorsqu'un tel traitement n'est pas fondé sur le consentement ou sur le droit de l'Union ou des États membres relatif aux questions spécifiées à

l'Article 23 (article général sur les limitations liées à la protection de la sécurité nationale, aux enquêtes criminelles, etc.) les paramètres suivants doivent être pris en compte afin de déterminer cette 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 à caractère personnel (notamment s'il s'agit de catégories particulières de données ou de données relatives à des infractions et condamnations pénales) ;
- les conséquences possibles du traitement proposé ; et
- l'existence de garanties (y compris le chiffrement ou la pseudonymisation).

Le considérant 50 et l'Article 5(1)(b), indiquent que le traitement ultérieur à des fins d'archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques doit être considéré comme un traitement compatible (voir la section sur les dérogations et conditions particulières).

Impact de la nouvelle législation européenne

Il existe des restrictions portant sur la capacité des organisations qui reçoivent des données à caractère personnel en vertu du règlement sur les données à faire un usage ultérieur de ces données. Ce règlement renforce le droit à la portabilité en permettant aux utilisateurs finaux d'accéder plus facilement aux données générées par les appareils connectés et les services connexes. L'utilisateur final peut demander à ce que ces données soient mises à la disposition d'un tiers - par exemple, pour que ce dernier puisse fournir à l'utilisateur final des services d'assistance ou de suivi liés à l'appareil connecté. Lorsque des tiers reçoivent des données relatives à un appareil connecté en vertu dudit règlement, l'Article 6 de celui-ci impose à ces tiers des restrictions plus strictes en matière de limitation des finalités. Le tiers ne peut utiliser les données qu'aux fins et dans les conditions convenues avec l'utilisateur de l'appareil. Le tiers n'est pas non plus autorisé à partager les données avec un autre tiers, à moins que ce partage ne se fasse également sur la base d'un contrat avec l'utilisateur final. Cela signifie qu'un tiers qui a reçu des données à caractère personnel (ou autres) en vertu du règlement sur les données n'est pas en mesure de faire un usage ultérieur, compatible, de ces données ; le tiers ne peut utiliser les données qu'aux fins initiales pour lesquelles elles ont été fournies.

Pour en savoir plus :

- Lignes directrices du CEPD 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées
- L'affaire C-268/21 *Norra Stockholm Bygg* porte sur les articles 6, (1), (e), 6, (3), et 6, (4), dans le contexte de la divulgation d'informations en matière civile.
- La Commission européenne a publié en avril 2019 un document de questions-réponses sur l'interaction entre le règlement de l'UE sur les essais cliniques et le RGPD, traitant du traitement ultérieur (disponible en anglais uniquement).
- L'affaire C-77/21 DIGI traite du traitement ultérieur, expliquant la nécessité d'un « lien concret, logique et suffisamment étroit » entre le traitement initial et le traitement ultérieur, ne s'écartant pas des « attentes légitimes » de l'individu
- Les décisions de la DPC à l'encontre de Meta (disponible en anglais uniquement) qui traitent de la possibilité d'invoquer la base légale du contrat

Où puis-je trouver ces dispositions ?

Base légale du traitement (données à caractère personnel)

Articles 6 à 10, considérants 40 à 50

Intérêts légitimes

En bref

L'intérêt légitime est la base juridique la plus polyvalente pour la plupart des responsables du traitement de données.

L'intérêt légitime peut être celui poursuivi par le responsable du traitement ou un tiers, mais il ne doit pas outrepasser les intérêts ou les libertés et droits fondamentaux de la personne concernée, en particulier lorsque celle-ci est un enfant.

Les autorités publiques ne peuvent pas se fonder sur l'intérêt légitime pour justifier un traitement des données effectué dans l'exercice de leurs fonctions.

Les responsables du traitement qui s'appuient sur les intérêts légitimes doivent conserver une trace de l'analyse qu'ils ont réalisée (c.-à-d. la mise en balance des intérêts en présence). Les lignes directrices du CEPD indiquent que cette analyse doit être fournie aux personnes concernées qui en font la demande, et que les personnes doivent être informées qu'elles disposent de ce droit. Cette analyse sera également nécessaire pour aider les responsables du traitement à prouver qu'ils ont bien pris en compte les droits et libertés des personnes concernées.

Les responsables du traitement doivent savoir que les données à caractère personnel traitées sur la base de l'intérêt légitime sont assorties d'un droit d'opposition, qui ne peut être écarté que s'il existe des raisons « *impérieuses* » de le faire.

À faire

Assurez-vous d'avoir identifié la base juridique pertinente pour le traitement des données à caractère personnel de votre organisation, et de l'avoir documenté en interne et dans les mentions d'information.

Si votre organisation est une autorité publique, assurez-vous d'avoir identifié une autre base pour le traitement de données à caractère personnel dans le cadre de vos fonctions publiques (par exemple, le traitement est nécessaire dans l'intérêt public ou à des fins d'exercice de l'autorité publique).

En outre, veillez à ce que les intérêts légitimes en question soient bien identifiés dans les mentions d'information qui doivent être fournies aux personnes concernées conformément aux Articles 13 et 14 (voir la section sur les mentions d'information).

Lorsque des intérêts légitimes sont invoqués, il convient de veiller à ce que toute prise de décision relative à l'équilibre entre les intérêts du responsable du traitement (ou du tiers concerné) et les droits des personnes concernées soit documentée dans une mise en balance des intérêts en présence et que celle-ci soit disponible pour être partagée avec les personnes concernées à leur demande.

Assurez-vous que vos mentions d'information informent les personnes de ce droit.

Commentaire

L'Article 6 (1), du RGPD dispose que le traitement des données à caractère personnel n'est licite que si au moins l'une des dispositions de l'Article 6(1) (a) à (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), précise que le point (f) ne s'applique pas au « *traitement effectué par les autorités publiques dans l'exécution de leurs missions* ». Cela dit, les intérêts légitimes peuvent toujours être pertinents pour les autorités publiques dans la mesure où le traitement est effectué à des fins qui ne relèvent pas de leur mission publique. En outre, la nécessité de prendre en considération les intérêts et les droits des enfants est également nouvelle (voir la section sur les enfants).

Dans la pratique, les principales considérations des organisations lorsqu'elles invoquent des intérêts légitimes en vertu du RGPD concernent le principe de responsabilité (la nécessité d'effectuer et de documenter la mise en balance des intérêts en présence) et les droits des personnes concernées liés à cette condition de traitement (y compris les droits de notification et d'opposition).

Qu'est-ce qu'un intérêt légitime ?

Les considérants du RGPD donnent des exemples de traitements qui pourraient être nécessaires à l'intérêt légitime d'un responsable du traitement de données. Il s'agit notamment de :

- Considérant 47 : traitement à des fins de prospection commerciale ou de prévention de la fraude ;
- Considérant 48 : transmission de données à caractère personnel au sein d'un groupe d'entreprises à des fins administratives internes, y compris les données relatives aux clients et aux employés (il convient de noter que les exigences en matière de transfert international restent applicables - voir la section relative aux transferts de données à caractère personnel) ;
- Considérant 49 : traitement visant à assurer la sécurité des réseaux et de l'information, y compris la prévention de l'accès aux réseaux de communications électroniques et la lutte contre les dommages causés aux systèmes informatiques et de communications électroniques ; et
- Considérant 50 : signalement à une autorité compétente d'éventuelles infractions pénales ou de menaces pour la sécurité publique.

Le considérant 47 indique également que les responsables du traitement doivent tenir compte des attentes des personnes concernées lorsqu'ils évaluent si leurs intérêts légitimes (c'est-à-dire ceux des responsables du traitement) sont dépassés par les intérêts des personnes concernées. Les intérêts et les droits fondamentaux des personnes concernées « *pourraient, en particulier prévaloir* » sur ceux du responsable du traitement lorsque les personnes concernées « *ne s'attendent pas raisonnablement à un traitement ultérieur* ».

Le considérant 47 précise également que les responsables du traitement sont censés « » *en tout état de cause* » » procéder à une « *évaluation attentive* » afin de déterminer s'il existe un intérêt légitime. Afin de se conformer au principe de responsabilité, les responsables du traitement doivent documenter cette évaluation ou « *mise en balance* ». Selon la CJUE, il s'agit d'un test en trois parties, comme indiqué dans l'affaire *Valsts policijas Rigas regiona parvaldes Kartibas policijas parvalde v Rigas pašvaldibas SIA 'Rigas satiksme* (C13/16) :

- identifier les intérêts pertinents ;
- déterminer si le traitement est nécessaire ; et
- le mettre en balance avec les intérêts des personnes concernées.

Les mentions d'information doivent indiquer les intérêts légitimes - et éventuellement la manière d'accéder aux détails des tests de mise en balance

Lorsque des intérêts légitimes sont invoqués en relation avec des traitements spécifiques, ils devront être indiqués dans les mentions d'information correspondantes, en vertu de l'Article 13, (1) (d), et de l'Article 14, (2) b).

Les lignes directrices sur la transparence au sens du règlement (UE) 2016/679 du groupe de travail « Article 29 » développent cette exigence : « *Par souci de bonne pratique, le responsable du traitement peut également fournir à la personne concernée les informations issues de la mise en balance, qui doit être réalisée pour pouvoir invoquer l'article 6, paragraphe 1, point f), […] En*

tout état de cause, la position du G29 est que les informations communiquées aux personnes concernées devraient indiquer clairement que ces dernières ont la possibilité d'obtenir sur simple demande des informations relatives à la mise en balance. ».

Les responsables du traitement doivent veiller à nommer spécifiquement les intérêts légitimes pertinents sur lesquels ils s'appuient dans leurs mentions d'information et envisager d'informer en même temps les personnes de leur droit d'accès à des tests de mise en balance des intérêts en présence.

Bien qu'il ne s'agisse pas d'une obligation spécifiquement mentionnée dans le RGPD lui-même, les lignes directrices précitées indiquent que cela est considéré comme « *essentiel pour garantir une transparence efficace* ».

Droit d'opposition spécifique

Les personnes concernées peuvent s'opposer à un traitement fondé sur des intérêts légitimes, mais elles doivent démontrer des « *raisons tenant à* [leur] *situation particulière* ». Il incombe alors aux responsables du traitement de prouver qu'ils ont des raisons impérieuses de continuer à traiter les données. Ce droit d'opposition peut conduire à l'exercice des droits de limitation et d'effacement des données (voir la section sur le droit d'opposition pour plus d'information).

Vérifier l'existence de codes de conduite

L'Article 40 impose aux États membres, aux autorités de contrôle, au CEPD et à la Commission européenne d'encourager la création de codes de conduite relatifs à un large éventail de sujets, y compris les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques. Bien que des progrès limités aient été accomplis à ce jour, les membres d'associations professionnelles ou d'organismes sectoriels similaires devraient être attentifs à la création de tels codes, qui pourraient imposer des exigences supplémentaires particulières.

Transferts de données - un nouveau fondement, mais qui ne sera probablement pas utile en pratique

L'Article 49, (1), prévoit une dernière possibilité pour les intérêts légitimes : les transferts peuvent être effectués sur la base d'« *intérêts légitimes impérieux* » lorsqu'ils ne sont pas répétitifs, qu'ils ne concernent qu'un nombre limité de personnes concernées et que le responsable du traitement a évalué et garanti le caractère adéquat du traitement. Toutefois, ce motif ne peut être invoqué que lorsque le responsable du traitement ne peut s'appuyer sur aucune autre méthode pour garantir l'adéquation, y compris les clauses contractuelles types, les règles d'entreprise contraignantes (« *BCR* »), les contrats approuvés et toutes les dérogations prévues à l'Article 49, (1), points (a) à (f). Comme indiqué dans les lignes directrices 2/2018 du CEPD sur les dérogations au titre de l'Article 49, « *Cette dérogation est envisagée par le droit comme un dernier ressort* ». Le responsable du traitement devra alors notifier à l'autorité de contrôle qu'il s'appuie sur ce motif de transfert - bien que les lignes directrices précitées reconnaissent qu'il ne soit pas nécessaire de demander une autorisation.

Pour en savoir plus :

- Lignes directrices du CEPD 8/2020 sur le ciblage des utilisateurs de médias sociaux
- Lignes directrices du CEPD attendues sur les intérêts légitimes dans le programme de travail 2024-2027 du CEPD
- Lignes directrices du CEPD 2/2018 relatives aux dérogations à l'article 49 du Règlement 2016/679
- Décisions de la DPC à l'encontre de Meta qui utilise l'intérêt légitime comme base légale (disponibles en anglais uniquement)
- Décision de la DPC contre WhatsApp sur le niveau d'information requis sur les intérêts légitimes dans les mentions d'information (disponible en anglais uniquement)
- La prochaine affaire C-621/22 de la CJUE examinera la possibilité de s'appuyer sur des intérêts légitimes uniquement commerciaux (ce qui a été envisagé de manière étroite par l'autorité néerlandaise de protection des données).

Où puis-je trouver ces dispositions ?

Intérêts légitimes

Article 6, (1), (f), article 13, (1), (d), article 14, (2), (b), et article 49, (1).

Considérants 47, 48, 49, 50

Consentement

En bref

Le consentement est soumis à des conditions de validité strictes dans le cadre du RGPD.

Le consentement peut être « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte* ». En pratique, cela signifie que le consentement doit être réellement volontaire, séparé des autres demandes de consentement, activement communiqué et aussi facile à retirer qu'à donner. Ces exigences sont souvent difficiles à respecter en pratique.

Des règles spécifiques s'appliquent également aux enfants en ce qui concerne les services de la société de l'information, pour lesquels le consentement des parents peut être requis

À faire

Veillez à ce que la base juridique sur laquelle s'appuie votre organisation est clairement identifiée.

Déterminez si les règles relatives aux enfants en ligne vous concernent et, le cas échéant, quelles règles nationales vous devez suivre pour obtenir le consentement (voir la section sur les enfants pour plus de détails).

Si votre organisation s'appuie sur le consentement pour traiter des données à caractère personnel à des fins de recherche scientifique, envisagez de proposer aux personnes concernées la possibilité de ne consentir qu'à certains domaines de recherche ou à certaines parties des projets de recherche. Pensez également aux dérogations nationales en matière de recherche comme solution alternative (voir la section sur les dérogations et conditions particulières).

Lorsque le consentement sert de base à un traitement licite, il convient de s'assurer que

- le consentement est actif et ne repose pas sur le silence, l'inactivité ou des cases précochées ;
- le consentement au traitement se distingue, est clair et n'est pas associé à d'autres accords ou déclarations écrits ;
- la fourniture de services n'est pas subordonnée au consentement à un traitement qui n'est pas nécessaire pour le service fourni (en dehors des situations autorisées limitées, voir ci-dessous) ;
- les personnes concernées sont informées qu'elles ont le droit de refuser ou de retirer leur consentement à tout moment sans préjudice, mais que cela n'affectera pas la licéité du traitement fondé sur le consentement avant son retrait ;
- il existe des méthodes simples pour retirer le consentement, y compris des méthodes utilisant le même support que celui utilisé pour obtenir le consentement en premier lieu ;
- des consentements distincts sont obtenus pour des opérations de traitement distinctes ; et
- le consentement n'est pas utilisé lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement (en particulier si le responsable du traitement est une autorité publique).

Commentaire

Qu'est-ce que le consentement, qu'est-ce qu'une indication non ambiguë de la volonté de la personne concernée et quand est-il nécessaire ?

L'Article 4, (1) du RGPD 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* ».

Le consentement est l'une des bases juridiques du traitement autorisées par l'Article 6 du RGPD (voir la section sur la licéité du traitement et traitement ultérieur).

Le considérant 32 suggère qu'une indication non ambiguë de la volonté de la personne concernée peut se matérialisée « *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'inactivité* ».

Le CEPD a publié des lignes directrices sur le consentement 5/2020 qui précisent en outre que « *Le recours à des cases cochées par défaut n'est pas valable en vertu du RGPD. Le silence ou l'inactivité de la personne concernée, ainsi que le simple fait qu'elle continue à utiliser un service, ne peuvent être considérés comme une indication active de choix* ».

Le consentement explicite reste nécessaire pour justifier le traitement de catégories particulières de données, à moins que d'autres bases ne s'appliquent (voir la section sur les catégories particulières de données et licéité du traitement). En outre, le consentement explicite, en l'absence de conditions adéquates ou autres, peut être invoqué en vertu du RGPD pour le transfert de données à caractère personnel en dehors de l'UE (voir la section sur les transferts de données à caractère personnel) et comme l'une des bases juridiques pour la prise de décisions automatisées significatives concernant une personne (voir la section sur le profilage et processus de décision automatisé).

Étapes nécessaires à la validité - spécifique, éclairé, univoque, révocable, granulaire et libre

L'Article 7, (1), du RGPD dispose que lorsque le consentement est invoqué comme base légale du traitement, les responsables du traitement doivent être en mesure de démontrer que la personne concernée a donné son consentement au traitement. Le reste de l'Article 7 est consacré à l'établissement des conditions d'un consentement valable.

Il s'agit de :

- Article 7, (2) : Le consentement au traitement contenu dans une déclaration écrite produite par le responsable du traitement doit pouvoir être distingué des autres éléments de cette déclaration, être intelligible, facilement accessible et rédigé dans un langage clair et simple. Le considérant 42 cite la directive concernant les clauses abusives dans les contrats conclus avec les consommateurs (directive 93/13/CEE) comme source d'inspiration pour ces obligations. En pratique, cela signifie que le consentement au traitement devra être clairement distingué dans le cadre de contrats ou d'accords plus larges.

- Le considérant 42 indique également que le consentement ne sera donné en connaissance de cause que si la personne concernée connaît (au moins) l'identité du responsable du traitement et les finalités prévues du traitement. Cette disposition est complétée par les lignes directrices du CEPD sur le consentement, qui précisent que les personnes doivent en outre être informées des données (type de données) qui seront collectées et utilisées, l'existence du droit de retirer son consentement, des informations sur de l'utilisation de techniques de traitement automatisé qui ont un effet juridique ou un effet similaire significatif et (si le consentement concerne des transferts de données en dehors de l'EEE) des risques éventuels des transferts de données vers des pays tiers. Tous les éléments susmentionnés doivent figurer (le cas échéant) dans le texte du mécanisme de consentement lui-même.

- Article 7(3) : cette disposition explique en outre que les personnes concernées doivent avoir le droit de retirer leur consentement à tout moment et qu'il doit être aussi facile de retirer le consentement que de le donner. Dans la pratique, il est probable que les

organisations devront au minimum permettre le retrait du consentement par le même moyen (site internet, courriel, texte) que celui par lequel il a été obtenu (dans ses lignes directrices sur le consentement, le CEPD a déclaré que lorsque le consentement a été obtenu par une interface électronique particulière, « *il est évident qu'une personne concernée doit pouvoir retirer son consentement moyennant la même interface électronique, dès lors que changer d'interface à la seule fin de retirer son consentement nécessiterait des efforts inutiles* ». Le RGPD reconnaît que le retrait du consentement ne rend pas rétrospectivement le traitement illégal et que le traitement peut se poursuivre sur une autre base juridique, le cas échéant, mais cela exige que le responsable du traitement en informe les personnes concernées avant que le consentement ne soit donné. Le CEPD a souligné que « *les responsables du traitement ont l'obligation de supprimer les données ayant été traitées sur la base du consentement une fois le consentement retiré, à condition qu'aucune autre finalité ne justifie leur conservation* » ».

- Article 7(4) : lorsque l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution de ce contrat, cela risque de remettre en question la mesure dans laquelle le consentement peut être considéré comme librement donné. Par conséquent, la fourniture d'un service ne devrait pas être subordonnée au consentement de la personne concernée au traitement de ses données à des fins qui ne sont pas nécessaires à la fourniture du service.

- Les lignes directrices du CEPD sur le consentement confirment que « L'adjectif "libre" implique un choix et un contrôle réel pour les personnes concernées. En règle générale, le RGPD dispose que si la personne concernée n'est pas véritablement en mesure d'exercer un choix, se sent contrainte de consentir ou subira des conséquences négatives importantes si elle ne donne pas son consentement, le consentement n'est pas valable » ».

Le considérant 43 du RGPD indique que le consentement sera présumé ne pas avoir été donné librement si bien qu'il soit conforme au vu des circonstances, il n'est pas prévu que des consentements distincts soient donnés pour différentes opérations de traitement ou « 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 ».

Il s'agit d'une exigence visant à garantir la granularité du consentement. Les lignes directrices du CEPD prévoient que « *si le responsable du traitement a regroupé plusieurs finalités de traitement et n'a pas cherché à obtenir un consentement distinct pour chaque finalité, la liberté est limitée* ». Les responsables du traitement doivent veiller à ne pas combiner plusieurs finalités de traitement dans un seul consentement.

Le considérant 43 note également qu'un déséquilibre de pouvoir entre les parties peut conduire à considérer que le consentement n'est pas valable et qu'il n'a pas été donné librement. Ce considérant indique spécifiquement que ce risque existe lorsque le responsable du traitement est une autorité publique.

Un autre exemple est donné par le CEPD relatif au consentement des employés : « *vu le déséquilibre des rapports de force entre un employeur et les membres de son personnel, les employés ne peuvent donner librement leur consentement que dans des situations exceptionnelles, lorsqu'absolument aucune conséquence négative ne résultera de leur refus de donner leur consentement* ».

Enfin, le considérant 42 dispose que « *le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice* ». Les lignes directrices du CEPD en matière de consentement traitent assez longuement du préjudice, indiquant que le RGPD n'« *exclut pas tous les incitants* », mais que les personnes doivent être en mesure de retirer ou de ne pas donner leur consentement sans encourir de coûts ou de « *désavantage évident* ». Malgré l'absence d'opposition du CEPD sur la question de l'incitation, il convient de noter que certaines autorités de contrôle des États membres sont clairement opposées à de telles techniques (par exemple, la CNIL en France), tandis que d'autres (par exemple, au Danemark et en Finlande) ont conclu que cela pouvait permettre aux organisations de subordonner les concours ou l'adhésion à des programmes de fidélisation au consentement à la prospection commerciale (voir plus loin).

Les enfants et la recherche

Des conditions spécifiques s'appliquent à la validité du consentement donné par les enfants en ce qui concerne les services de la société de l'information, avec l'obligation d'obtenir et de vérifier le consentement parental en dessous de certaines limites d'âge (voir la section les enfants pour plus de détails).

Le considérant 33 du RGPD traite du consentement obtenu à des fins de recherche scientifique. Il reconnaît que « *souvent, il n'est pas possible de cerner entièrement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données* » « et précise que :

- les personnes concernées devraient pouvoir consentir à certains domaines de la recherche scientifique, lorsque cela répond à des « *normes éthiques* » pour ce type de recherche ; et
- les personnes concernées ne devraient pouvoir donner leur consentement que pour *« certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet ».*

Les lignes directrices du CEPD sur le consentement soulignent que « *lorsque le consentement est la base juridique de la conduite de recherches conformément au RGPD, celui-ci devrait se distinguer des autres exigences de consentement qui servent de norme éthique ou d'obligation procédurale* ». Le débat sur la base juridique la plus appropriée pour la recherche et sur la possibilité de s'appuyer sur une base juridique préexistante pour un traitement ultérieur (voir la section sur la licéité du traitement et traitement ultérieur) est toujours d'actualité.

Langue du consentement

Le RGPD exige que le consentement soit intelligible, informé et sans ambiguïté. Les lignes directrices du CEPD sur le consentement soulignent qu'« e*n sollicitant un consentement, les responsables du traitement devraient s'assurer d'utiliser systématiquement des termes clairs et simples. Cela signifie qu'un message devrait être facilement compréhensible pour l'homme de la rue et pas uniquement pour les avocats* ». Il est également peu probable que le consentement réponde à ces exigences s'il est rédigé dans une langue étrangère incompréhensible pour l'individu.

Nouvelles lois européennes

Le DMA impose des restrictions supplémentaires au consentement. L'Article 5 du DMA prévoit que si la personne concernée refuse ou retire son consentement, le responsable du traitement ne peut pas réitérer sa demande de consentement pour la même finalité au cours de la même année.

Pour en savoir plus :

- Lignes directrices du CEPD 8/2020 sur le ciblage des utilisateurs des réseaux sociaux
- Lignes directrices du CEPD 5/2020 sur le consentement au sens du règlement (UE) 2016/679
- Lignes directrices du CEPD 3/2022 sur les interfaces truquées (« dark patterns ») dans les interfaces des plateformes de médias sociaux (disponibles en anglais uniquement)
- Décisions de l'autorité danoise de protection des données (disponible uniquement en danois ici) et de l'autorité finlandaise de protection des données (disponible uniquement en finlandais ici) sur l'incitation au consentement
- Affaire C-673/17 *Planet 49* de la CJUE (le consentement doit être actif et ne peut être obtenu par le biais de cases précochées).
- Rapport du groupe de travail sur les bannières de cookies du CEPD (disponible en anglais uniquement)
- Affaire C-252/21 de la CJUE portant sur la question de savoir si le consentement peut être donné librement à une entreprise dominante (Facebook/Instagram)

Où puis-je trouver ces dispositions ?

Article 4, (1)1, article 6, (1), point a), articles 7 et 8 et article 9, (2), point a).

Considérants 32, 33, 42 et 43

Les enfants

En bref

Le RGPD contient quelques dispositions spécifiques aux enfants, notamment en ce qui concerne la base juridique du traitement et les mentions d'information.

Les enfants sont considérés comme des « *personnes vulnérables* » et méritent une « *protection spécifique* ».

Le traitement des données relatives aux enfants comporte certains risques particuliers et des restrictions supplémentaires peuvent être imposées à la suite de codes de conduite.

Lorsque des services en ligne sont fournis à un enfant et que le consentement est invoqué comme base pour le traitement de ses données, le consentement doit être donné ou autorisé par une personne exerçant l'autorité parentale à l'égard de l'enfant. Cette exigence s'applique aux enfants de moins de 16 ans (sauf si l'État membre a prévu une limite d'âge inférieure, qui ne peut être inférieure à 13 ans).

De nombreuses autorités nationales ont commencé à adopter des lignes directrices spécifiques aux enfants, et de nouvelles lignes directrices sont attendues de la part du CEPD en 2024.

À faire

Vérifiez si les règles et les lignes directrices relatives aux enfants sont susceptibles de vous concerner.

Si votre organisation offre directement aux enfants des services de la société de l'information pour lesquels un consentement est requis, évaluez les règles nationales applicables et veillez à ce que des mécanismes appropriés de consentement parental soient mis en œuvre, y compris des processus de vérification.

Restez au fait de la législation et des lignes directrices nationales relatives au traitement des données hors ligne concernant les données des enfants.

En cas de traitement de données relatives à des enfants - ciblé ou non - veillez à ce que les mentions soient rédigées clairement en tenant compte de la capacité de compréhension de l'enfant.

Veiller à ce que tout recours à l'« *intérêt légitime* » pour justifier le traitement de données relatives à des enfants soit étayé par un examen minutieux et documenté de la question de savoir si les intérêts de l'enfant l'emportent sur ceux de votre organisation.

Commentaire

L'importance de la protection des enfants est mentionnée à plusieurs reprises dans le RGPD et a été soulignée dans les lignes directrices du CEPD. Dans la pratique, le RGPD lui-même n'offre que peu d'harmonisation, et les restrictions substantielles proviennent des lois nationales, de la conformité avec les lignes directrices du CEPD ou des codes de conduite (voir la section sur les codes de conduite et la certification pour plus de détails).

Consentement parental

La principale disposition relative aux enfants est l'Article 8, qui exige le consentement des parents pour les services de la société de l'information offerts directement à un enfant de moins de 16 ans - bien que ce plafond puisse être fixé à 13 ans par les États membres, et ne s'applique que lorsque le traitement est fondé sur le consentement de l'enfant. Les États membres ont choisi un large éventail d'âges, le Danemark, la Belgique et d'autres pays ont fixé l'âge minimum à 13 ans, l'Autriche à 14 ans, la France et la République tchèque à 15 ans et de nombreux pays comme les Pays-Bas et l'Irlande ont choisi l'âge de 16 ans.

Le responsable du traitement est également tenu, en vertu de l'Article 8, (2), du RGPD, de faire des « *efforts raisonnables* » pour vérifier que le consentement a été donné ou autorisé par le titulaire de l'autorité parentale, à la lumière des technologies disponibles.

Cela ne concerne que certaines données en ligne - les données hors ligne continuent d'être soumises aux règles habituelles des États membres en matière de capacité de consentir. L'Article 8, (1), ne doit pas non plus être considéré comme affectant le droit général des contrats des États membres en ce qui concerne la validité, la formation ou l'effet d'un contrat avec un enfant. Les organisations devront toujours tenir compte des lois locales dans ce domaine.

Les mentions d'information adressées aux enfants doivent être adaptées à ces derniers

L'Article 12 du RGPD prévoit que l'obligation de veiller à ce que les informations fournies aux personnes concernées soient concises, transparentes et rédigées en langage clair doit être respectée « *particulièrement pour toute information adressée spécifiquement à un enfant* ».

Le considérant 58 développe ce point : « *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 RGPD reconnaît la définition de l'enfant de la Convention des Nations Unies comme étant toute personne âgée de moins de 18 ans. Les responsables du traitement doivent donc être prêts à remplir ces exigences dans les mentions destinées aux adolescents. Le CEPD indique que les responsables du traitement doivent « *veiller à ce que le vocabulaire, le ton et le style du langage utilisé soient adaptés aux enfants et trouvent un écho auprès d'eux* ». Les lignes directrices du CEPD indiquent que « *dans le cas d'enfants très jeunes ou préalphabétisés, les mesures de transparence peuvent également être adressées aux titulaires de la responsabilité parentale, étant donné que ces enfants ont, dans la plupart des cas, peu de chances de comprendre même les messages écrits ou non écrits les plus élémentaires concernant la transparence* ».

Analyse d'Impact relative à la Protection des Données - le traitement des données relatives aux enfants peut contribuer à ce que le traitement soit considéré comme présentant un risque élevé selon les circonstances.

Comme indiqué ailleurs dans le présent guide, une AIPD doit être réalisée lorsqu'un responsable du traitement effectue un traitement à haut risque. Les lignes directrices du CEPD sur les AIPD ont noté que le traitement des données de personnes vulnérables - qui incluent les enfants - est un critère qui, lorsqu'il est pris en compte avec d'autres facteurs, peut conduire à une activité de traitement à haut risque « *en raison du déséquilibre de pouvoir accru entre les personnes concernées et le responsable du traitement des données, ce qui signifie que les personnes peuvent être incapables de consentir facilement au traitement de leurs données, de s'y opposer ou d'exercer leurs droits* ».

Dispositions diverses - lignes d'assistance, codes de conduite et travail des autorités de contrôle

L'Article 6(1)(f) du RGPD indique que les droits et libertés d'une personne concernée peuvent « » *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 veiller à conserver une documentation claire démontrant que les intérêts concurrents ont été dûment pris en compte dans le cadre d'une mise en balance lorsqu'ils s'appuient sur des intérêts légitimes pour le traitement de données relatives à des enfants.

Le considérant 38 note que l'utilisation de données relatives aux enfants à des fins de marketing ou de profilage, ou en relation avec la fourniture de services aux enfants, est un sujet de préoccupation qui nécessite une protection spécifique au titre du RGPD. Le considérant indique également que le consentement parental ne devrait pas être requis dans le cadre de services de prévention et/ou de conseil offerts directement à un enfant, bien que cette suggestion ne semble pas se refléter dans les articles du RGPD lui-même.

L'article 40 impose aux États membres, aux autorités de contrôle, au CEPD et à la Commission européenne d'encourager la création de codes de conduite, y compris dans le domaine de la protection des enfants, et concernant la manière dont le consentement peut être recueilli auprès du titulaire de l'autorité parentale concernée. Les organisations qui traitent des données à caractère personnel concernant des enfants devraient veiller à la création de tels codes, qui pourraient imposer des exigences supplémentaires particulières.

Depuis que l'autorité britannique de protection des données a publié *l'Age Appropriate Design Code* (disponible en anglais uniquement) en janvier 2020, certains États membres ont adopté des lignes directrices sur le traitement des données des enfants, notamment l'Irlande et la France. Le CEPD doit également publier des lignes directrices sur le traitement des données des enfants dans le cadre de son programme de travail 2023-2024.

Enfin, les autorités de contrôle, lorsqu'elles s'efforcent de sensibiliser le public et de souligner les risques, les règles, les garanties et les droits liés au traitement des données à caractère personnel, conformément à l'obligation qui leur est faite par l'Article 57(1)(b) sont tenues d'accorder une « *attention particulière* » aux activités s'adressant aux enfants.

Où puis-je trouver ces dispositions ?

Articles 6, (1) (f), 8, 12, (1), 40, (2) (g), 57, (1), (b)

Considérants 38, 58, 75

Catégories particulières de données et licéité du traitement

En bref

Les « catégories particulières de données à caractère personnel » sont des données qui révèlent « *l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* ».

Les justifications permettant le traitement de catégories particulières de données en vertu du RGPD sont restreintes et spécifiques. Dans un certain nombre de cas, ces dispositions impliquent encore le recours aux lois de l'UE ou des États membres.

Les États membres ont également la possibilité d'introduire de nouvelles conditions (y compris des limitations) concernant le traitement des données génétiques, biométriques ou de santé.

À faire

Veillez à ce que les motifs invoqués par votre organisation pour traiter des catégories particulières de données soient clairs et à ce que l'application de la législation de l'UE ou des États membres soit prise en compte le cas échéant ;

Si vous vous appuyez sur un consentement explicite, assurez-vous que le consentement répond aux conditions de validité (voir la section sur le consentement) ; et

Assurez-vous d'avoir vérifié et de continuer à prêter attention aux développements nationaux, car les États membres ont le droit d'imposer des conditions supplémentaires - y compris des restrictions - aux conditions énoncées dans le RGPD.

Commentaire

L'Article 9(2) énonce les circonstances dans lesquelles des catégories particulières de données peuvent faire l'objet d'un traitement qui est par ailleurs interdit. Il s'agit des catégories de données suivantes, telles que définies à l'Article 9(1) :

- l'origine raciale ou ethnique ;
- les opinions politiques ;
- les convictions religieuses ou philosophiques ;
- l'appartenance à un syndicat ;
- les données relatives à la santé ou à la vie sexuelle et à l'orientation sexuelle ;
- les données génétiques ; et
- les données biométriques traitées pour identifier une personne de manière unique.

Le considérant 51 suggère que le traitement des photographies ne sera pas automatiquement considéré comme un traitement de données biométriques (comme c'était le cas dans certains États membres avant le RGPD) ; les photographies ou les enregistrements ne seront couverts que dans la mesure où elles permettent l'identification unique ou l'authentification d'une personne (comme lorsqu'elles sont utilisées dans le cadre d'un passeport électronique).

Dans l'affaire *Bundeskartellamt* (C-252/21), la CJUE a conclu que si une personne visite un site internet ou une application qui se rapporte à l'une des catégories particulières de données, et s'inscrit sur le site ou passe une commande, alors ces données seront des données sensibles - y compris si elles sont automatiquement collectées par un réseau social qui s'interface avec le site ou l'application. La CJUE a également conclu que les données relatives à votre partenaire (telles que son nom) peuvent révéler des informations sur l'orientation sexuelle d'une personne (C-184/20).

Les motifs de traitement des catégories particulières sont les suivants :

9(2)(a) - Consentement explicite de la personne concernée, à moins que le droit de l'UE ou de État membre n'interdise de se fonder sur le consentement

Si l'on invoque ce motif, il convient d'examiner attentivement les conditions de validité du consentement (voir la section sur le consentement).

9(2)(b) - Nécessaire à l'exécution des obligations découlant du droit du travail, de la sécurité sociale ou de la protection sociale, ou d'une convention collective

9(2)(c) - Nécessaire pour protéger les intérêts vitaux d'une personne concernée qui est physiquement ou légalement incapable de donner son consentement

9(2)(d) - Traitement effectué par un organisme à but non lucratif ayant un objectif politique, philosophique, religieux ou syndical, à condition que le traitement ne concerne que les membres ou anciens membres (ou ceux qui ont des contacts réguliers avec lui dans le cadre de ces objectifs) et qu'il n'y ait pas de divulgation à un tiers sans consentement

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

9(2)(f) - Nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou lorsque les tribunaux agissent dans l'exercice de leurs fonctions juridictionnelles

9(2)(g) - Nécessaire pour des motifs d'intérêt public important sur la base du droit de l'Union ou d'un État membre qui est proportionné à l'objectif poursuivi et qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et intérêts de la personne concernée

Cela permet aux États membres d'étendre par la loi les circonstances dans lesquelles des catégories particulières de données peuvent être traitées dans l'intérêt public. Dans de nombreux pays, cela n'a nécessité aucun changement, dès lors que de telles dispositions figuraient dans la législation préexistante. Dans d'autres, il existe des dispositions générales et substantielles relatives à l'intérêt public au sein des lois sectorielles ou de la législation sur la protection des données.

9(2)(h) - Nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, d'un diagnostic médical, de la fourniture de soins de santé ou de soins sociaux ou de traitements ou de la gestion de systèmes et de services de soins de santé ou de soins sociaux

sur la base du droit de l'Union ou de l'État membre ou d'un contrat conclu avec un professionnel de la santé

9(2)(i) - Nécessaire pour des raisons d'intérêt public dans le domaine de la santé publique, telles que la protection contre les menaces transfrontalières graves pour la santé ou la garantie de normes élevées en matière de soins de santé et de médicaments ou de dispositifs médicaux

Ces deux dispositions fournissent une justification juridique formelle à l'utilisation des données relatives aux soins de santé dans les secteurs de la santé et des produits pharmaceutiques par les prestataires de services sociaux. Il est important de rappeler que la première de ces dispositions nécessite toujours une base légale en vertu de la législation européenne ou locale, et que les deux conditions requièrent des obligations de confidentialité comme garantie supplémentaire.

9(2)(j) - nécessaire à des fins archivistiques dans l'intérêt public, ou à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89(1)

Cette disposition prévoit le traitement de catégories particulières de données à des fins d'archivage, de recherche et de statistiques, sous réserve du respect de garanties appropriées, y compris de garanties visant à assurer le respect du principe de minimisation des données (voir la section sur les dérogations et conditions particulières pour plus de détails).

Focus sur la France : catégories particulières de traitement

En France, la Loi Informatique et Libertés (« LIL ») consacre plusieurs de ses dispositions à des catégories particulières de traitements, tels que :

- Les traitements de données de santé, qui font l'objet d'un régime spécifique (Section III de la LIL). Ils sont soumis à déclaration ou demande d'autorisation auprès de la CNIL, notamment pour les traitements de recherche en santé, dès que les opérations de traitement concernent des personnes en France (patients ou professionnels de santé) ou que le responsable du traitement est établi en France ;

- Le numéro d'identification des personnes au répertoire national d'identification des personnes physiques (le NIR ou numéro de sécurité sociale) ne peut être utilisé que par certains organismes et pour des usages définis (Article 30 de la LIL ; Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire) ;

- Les traitements de données sur les infractions, condamnations ou mesures de sûreté connexes sont interdits sauf s'il s'agit de certains organismes spécifiques (notamment autorités publiques, juridictions, auxiliaires de justice dans le cadre de leurs attributions légales et missions spécifiques) (Article 46 de la LIL).

Données génétiques, biométriques ou de santé

Les États membres sont également autorisés, en vertu de l'Article 9 (4), du RGPD, à maintenir ou à imposer des conditions supplémentaires (y compris des limitations) en ce qui concerne les données génétiques, biométriques ou de santé.

Condamnations pénales et infractions

Les données relatives aux condamnations pénales et aux infractions ne sont pas considérées comme une catégorie particulière de données aux fins du RGPD. Ceci est cohérent avec les dispositions précédentes, puisque les données de ce type n'étaient pas traitées comme une catégorie particulière de données dans le cadre de la directive sur la protection des données.

De même, les règles du RGPD concernant les données relatives aux condamnations pénales et aux infractions reflètent celles qui s'appliquaient dans le cadre de la directive sur la protection des données. L'Article 10 prévoit que ces données ne peuvent être traitées que sous le contrôle d'une autorité officielle ou lorsque le traitement est autorisé par le droit de l'Union ou le droit d'un État membre qui prévoit des garanties appropriées. Il existe des divergences nationales notables dans ce domaine.

Focus sur la France : Formalités préalables

En France, la Loi Informatique et Libertés maintient des formalités préalables (autorisation, déclaration ou avis) pour :

1. Certains traitements de données de santé, notamment dans le cadre de la recherche :

- les traitements de données de santé dans le domaine de la santé, sauf ceux rentrant dans l'une des exceptions prévues à l'Article 65 de la Loi Informatique et Libertés ;
- les traitements de données de santé dans le domaine de la recherche.
- Ce régime s'applique
  - Soit dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire français, que le traitement ait lieu ou non en France ;
  - Soit lorsque les personnes concernées résident en France, y compris lorsque le responsable du traitement n'est pas établi en France.

2. Certains traitements mis en œuvre pour le compte de l'État :

- les traitements comportant le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (NIR) fondés sur l'intérêt public ou mis en œuvre à des fins de recherche, d'étude ou d'évaluation ;
- les traitements qui intéressent la sûreté de l'État, la défense, la sécurité publique ou qui ont pour objet la prévention et la répression des infractions pénales ;
- les traitements de données génétiques ou biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes mis en œuvre pour le compte de l'État.

Mentions d’information

En bref

Les responsables du traitement doivent fournir des mentions d’information afin d’assurer la transparence du traitement.

Des informations spécifiques doivent être fournies, et il existe également une obligation générale de transparence.

L’accent est mis sur des mentions claires et concises.

À faire

Faites un audit des mentions d’information existantes et mettez-les à jour.

Pour les données qui sont collectées de manière indirecte, assurez-vous que des mentions d’information sont communiquées au moment adéquat.

Travaillez avec les partenaires concernés qui peuvent être amenés à collecter des données pour le compte de votre organisation et désignez des responsables pour la revue des mentions, leur mise à jour et leur validation.

Commentaire

Tout traitement doit être « *loyal et transparent* », ce qui signifie que le responsable du traitement doit fournir des informations aux personnes sur le traitement de leurs données, à moins que la personne ne dispose déjà de ces informations. Les informations à fournir sont spécifiées dans le RGPD et énumérées ci-dessous. Le responsable du traitement peut également être tenu de fournir des informations supplémentaires si, dans des circonstances et un contexte spécifique, cela est nécessaire pour que le traitement soit loyal et transparent.

Les informations doivent être fournies de manière concise, transparente, intelligible et facilement accessible, en utilisant un langage clair et simple (en particulier lorsque la personne concernée est un enfant).

Que doit dire le responsable aux personnes ?

Des lignes directrices supplémentaires de l'ancien groupe de travail « Article 29 » (« G29 ») sur la transparence sont incluses ci-dessous. Il est à noter que les lignes directrices de l'ancien G29 vont plus loin que les exigences du RGPD sur un certain nombre de points :

- Identité et coordonnées du responsable du traitement (ou de son représentant, dans le cas d'un responsable du traitement non établi dans l'UE) ; coordonnées du délégué à la protection des données. Les lignes directrices précisent que le responsable du traitement doit également prévoir différents canaux de communication (téléphone, courriel, adresse postale, etc.).

- Finalités du traitement et base juridique du traitement - y compris l'intérêt légitime » poursuivi par le responsable du traitement (ou le tiers) s'il s'agit de la base juridique. Les lignes directrices précisent que les finalités doivent être énoncées en même temps que la base juridique pertinente invoquée. Cela a été confirmé par les décisions contraignantes du CEPD concernant les amendes infligées par l'autorité irlandaise de protection des données à Meta concernant Facebook, Instagram et WhatsApp. Il convient également de préciser que la personne peut obtenir, sur demande, des informations supplémentaires sur l'exercice de l'intérêt légitime (communément abrégé en « *LIA* » de l'anglais *Legitimate Interest Assessment*), lorsque ces informations ne figurent pas déjà dans les mentions d'information.

- Lorsque des catégories particulières de données sont traitées, la base légale prévue à l'Article 9 du RGPD doit être précisée (ainsi que toute autre loi de l'UE ou d'un État membre, le cas échéant). Lorsque les données relatives aux condamnations pénales et aux infractions sont traitées, il convient d'indiquer la législation de l'UE ou de l'État membre sur la base de laquelle le traitement est effectué.

- Destinataires ou catégories de destinataires : d'après les lignes directrices, les responsables du traitement doivent fournir aux individus des informations sur les destinataires qui sont les plus significatives possibles, ce qui implique généralement de nommer ces derniers. Les destinataires comprennent les responsables du traitement, les responsables conjoints du traitement et les sous-traitants. Selon les lignes directrices, lorsqu'un responsable du traitement choisit de ne nommer que des catégories de destinataires, il doit être aussi précis que possible et indiquer le type de destinataire, l'industrie, le secteur et le sous-secteur, ainsi que le lieu où se trouve le destinataire.

- Détails des transferts de données en dehors de l'UE :

  - compris la manière dont les données seront protégées (par exemple, le destinataire se trouve dans un pays adéquat, des règles d'entreprise contraignantes sont en place, etc.), et

  - la manière dont la personne peut obtenir une copie des BCR ou d'autres garanties, ou l'endroit où ces garanties ont été mises à disposition.

  - D'après les lignes directrices, l'article pertinent du RGPD autorisant le transfert et le mécanisme d'adéquation correspondant doivent être spécifiés. Dans la mesure du possible, il convient d'inclure un lien vers le mécanisme d'adéquation utilisé ou des informations sur l'endroit où le document peut être consulté. Les informations fournies sur les transferts vers des pays tiers doivent également être aussi significatives que possible pour les individus ; selon les lignes directrices, cela signifie

généralement que les pays tiers doivent être nommés.

- La période de conservation des données - si cela n'est pas possible, les critères utilisés pour la déterminer. Selon les lignes directrices, il ne suffit pas que le responsable du traitement indique de manière générique que les données seront conservées aussi longtemps que nécessaire. Le cas échéant, les différentes périodes de conservation doivent être stipulées pour les différentes catégories de données à caractère personnel et/ou les différentes finalités de traitement, y compris, le cas échéant, les périodes d'archivage.

- La personne a le droit d'accéder aux données et de les porter, de les rectifier, de les effacer et de les restreindre, de s'opposer au traitement et, si le traitement est fondé sur le consentement, de retirer ce dernier. Selon les lignes directrices, lorsque la législation de mise en œuvre d'un État membre limite ou restreint les droits des personnes concernées, le responsable du traitement doit notifier aux personnes concernées toute limitation de leurs droits sur laquelle le responsable du traitement peut s'appuyer.

- Le droit pour la personne concernée de déposer une plainte auprès d'une autorité de contrôle.

- L'existence d'une obligation légale ou contractuelle de fournir les données, ou d'une obligation de fournir les données pour conclure un contrat, et les conséquences de la non-fourniture des données.

- S'il y a une prise de décision automatisée - avec des informations sur la logique impliquée ainsi que l'importance et les conséquences du traitement pour l'individu.

Dans le cas d'activités de collecte indirecte de données, le responsable du traitement doit également indiquer aux personnes concernées les catégories d'informations et la ou les sources de ces informations, y compris si elles proviennent de sources accessibles au public. Selon les lignes directrices, les détails doivent inclure la nature des sources (c'est-à-dire des sources publiques/privées), les types d'organisation/industrie/secteur et le lieu où l'information a été détenue (UE ou non-UE).

Le responsable du traitement n'est pas tenu de fournir ces informations à la personne si cela s'avère impossible ou implique des efforts disproportionnés. Dans ces cas, des mesures adéquates doivent être prises pour protéger les intérêts des personnes et les mentions d'information doivent être rendues publiques.

Il n'est pas non plus nécessaire de fournir les mentions d'information :

- s'il existe une obligation légale de l'UE ou d'un État membre obligeant le responsable du traitement à obtenir/divulguer les informations ; ou

- si l'information doit rester confidentielle en raison d'obligations de secret professionnel ou légal, régies par la législation de l'UE ou des États membres.

- si le responsable du traitement traite ultérieurement des données à caractère personnel pour une nouvelle finalité, non couverte par la mention initiale, il doit fournir une nouvelle mention couvrant le nouveau traitement.

Il est difficile de concilier la fourniture de toutes ces informations avec les exigences de concision et de clarté du RGPD. Pour y parvenir, la Commission européenne a la possibilité d'introduire des icônes normalisées au moyen d'actes délégués. Si ces icônes sont introduites, elles devront également être présentées aux personnes.

Quand le responsable du traitement doit-il fournir ces informations ?

Le responsable obtient des informations directement auprès de la personne

- Au moment où les données sont obtenues.

- Le responsable du traitement doit également indiquer aux personnes quelles informations sont obligatoires à fournir et quelles sont les conséquences si ces informations ne sont pas fournies.

Le responsable n'obtient pas d'informations directement de la personne

- Dans un délai raisonnable à compter de la collecte des données (maximum un mois) ; ou

- Si les données sont utilisées pour communiquer avec la personne concernée,

au plus tard lors de la première communication ; ou

- Si la divulgation à un autre destinataire est envisagée, au plus tard avant la divulgation des données.

Exigences supplémentaires éventuelles des États membres en matière de divulgation

En plus des exigences prévues par les Articles 13 et 14 du RGPD, certains États membres ont ajouté ou maintenu des éléments supplémentaires à mentionner dans les mentions d'information.

Focus sur la France : droit des personnes de définir des directives sur les traitements de leurs données après leur décès en France

En France, l'Article 85 de la Loi Informatique et Libertés prévoit que « *Toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès*. ». Les directives définissent la manière dont la personne entend que soient exercés, après son décès, ses droits tels que définis par le RGPD. Les directives de la personne sont « *générales* » lorsqu'elles portent sur l'ensemble des données relatives à la personne et « *particulières* » lorsqu'elles concernent certains traitements mentionnés par la personne concernée. Les directives générales peuvent être enregistrées auprès d'un tiers de confiance certifié par la CNIL. La personne peut modifier ou révoquer ses directives à tout moment. Ce droit doit être précisé dans les notes et mentions d'informations aux personnes en sus des informations prévues aux Articles 13 et 14 du RGPD.

Mises à jour des mentions d'information

Selon l'ancien groupe de travail « Article 29 », les responsables du traitement doivent prendre « *toutes les mesures* » nécessaires pour porter toutes modifications spécifiques à l'attention des personnes concernées (ces communications doivent également être distinctes du contenu de toute prospection commerciale). L'ancien groupe de travail « Article 29 » donnait des exemples non exhaustifs de modifications des mentions d'information qui devraient toujours être communiquées aux personnes concernées, à savoir : une modification de la finalité du traitement, un changement d'identité du responsable du traitement et des modifications concernant la manière dont une personne peut exercer ses droits.

Pour en savoir plus :

Lignes directrices du groupe de travail « Article 29 » sur la transparence au sens du règlement 2016/679

Lignes directrices 03/2022 du CEPD sur les interfaces truquées (« dark patterns ») dans les interfaces des plateformes de médias sociaux : comment les reconnaître et les éviter (disponibles en anglais uniquement)

Décisions du DPC irlandais à l'encontre de Meta Ireland (Facebook et Instagram) (disponibles en anglais uniquement)

Décisions contraignantes du CEPD concernant le différend soumis par l'autorité de protection irlandaise sur les services Meta Platforms, WhatsApp, Instagram et Facebook (disponibles en anglais uniquement)

Où puis-je trouver ces dispositions ?

Articles 12 à 14

Considérants 58, 60, 61 et 62

Droits d’accès, de rectification et droit à la portabilité des personnes concernées

En bref

Les responsables du traitement doivent, sur demande :

- confirmer s’ils traitent les données à caractère personnel d’une personne ;
- fournir une copie des données (sous forme électronique couramment utilisée dans de nombreux cas) ; et
- fournir des documents explicatifs (et détaillés).

Les personnes concernées peuvent également exiger que leurs données à caractère personnel leur soient transférées ou soient transférées à un nouveau fournisseur dans un format lisible par machine si les données en question ont été (a) fournies par la personne concernée au responsable du traitement (au sens large), (b) traitées automatiquement et (c) traitées sur la base du consentement ou de l’exécution d’un contrat.

La demande doit être satisfaite dans un délai d’un mois (avec des prolongations dans certains cas) et toute intention de ne pas s’y conformer doit être expliquée à la personne concernée.

Les droits d’accès sont destinés à permettre aux personnes de vérifier la licéité du traitement et le droit à une copie ne doit pas porter atteinte aux droits d’autrui de manière déraisonnable.

À faire

Examinez les processus, les procédures et la formation des équipes en contact avec la clientèle - sont-ils suffisants pour répondre aux règles d’accès et de portabilité du RGPD ?

Élaborez des modèles de lettres de réponse, afin de vous assurer que tous les éléments d’information sont fournis.

Évaluez la capacité de votre organisation à fournir des données conformément aux obligations du RGPD en matière de format et de délai. Il peut être nécessaire de développer des capacités de formatage pour répondre aux demandes d’accès.

Si droit à la portabilité s’applique, déterminez quels sont les fichiers concernés.

Vérifiez si les données (et les métadonnées associées) peuvent être facilement exportées dans des formats structurés et lisibles par machine.

Soyez attentif aux initiatives sectorielles visant à développer des formats interopérables.

Si vous fournissez un produit IoT/connecté, ou un service associé à un tel produit, ou si vous êtes un contrôleur d’accès, vérifiez que vous pouvez vous conformer aux exigences de portabilité renforcées.

Envisagez de développer des portails d’accès pour les personnes concernées, afin de permettre l’exercice direct des droits d’accès des personnes concernées.

Droit d'information et d'accès

Une personne dispose des droits suivants à l'égard d'un responsable du traitement de données :

- obtenir la confirmation que ses données à caractère personnel font l'objet d'un traitement ;
- accéder aux données (c'est-à-dire à une copie et non au document lui-même) ; et
- recevoir des informations complémentaires sur le traitement.

Comme pour tous les droits des personnes concernées, le responsable du traitement doit s'y conformer « *dans les meilleurs délais* » et « *au plus tard dans un délai d'un mois* », bien qu'il soit possible de prolonger ce délai de deux mois supplémentaires.

Avant de fournir des données au demandeur, le responsable du traitement doit également utiliser des moyens raisonnables pour vérifier l'identité de la personne qui fait la demande, de manière proportionnée à la sensibilité des données traitées, mais il ne doit pas conserver ou collecter des données dans le seul but de pouvoir répondre aux demandes d'accès des personnes concernées. Ces points sont particulièrement importants pour les services en ligne.

Droit d'accès aux données

Le responsable du traitement doit fournir « *une copie des données à caractère personnel faisant l'objet du traitement* ». Il ne s'agit pas d'un droit au document, mais d'une copie des données (affaire C-487/21, *F.F. c. Österreichische Datenschutzbehörde*). Cette affaire a également clarifié un certain nombre d'autres points relatifs au droit d'accès aux données :

- le responsable du traitement doit donner à la personne concernée une reproduction fidèle et intelligible de toutes les données à caractère personnel en cours de traitement ;
- le droit d'accès ne doit pas porter atteinte aux droits et libertés d'autrui (ce qui réaffirme la nécessité pour les responsables du traitement de mettre en balance les droits des personnes concernées et les droits et libertés d'autrui). Cette information doit être fournie gratuitement, bien que le responsable du traitement puisse facturer des frais administratifs raisonnables si d'autres copies sont demandées ou si la demande est manifestement infondée ou excessive, ce qui est un seuil difficile à atteindre.

Si la demande est faite sous forme électronique, les informations doivent être fournies sous une forme électronique couramment utilisée (sauf demande contraire de la personne concernée). Cela pourrait entraîner des coûts pour les responsables du traitement qui utilisent des formats spéciaux ou qui conservent des dossiers papier.

Le considérant 63 suggère également que, dans la mesure du possible, le responsable du traitement peut fournir un système sécurisé permettant à la personne concernée d'accéder directement à ses données. Cela semble être encouragé plutôt qu'exigé.

Informations complémentaires

Le responsable du traitement doit également fournir les informations suivantes :

- les finalités du traitement ;
- les catégories de données traitées ;
- les destinataires ou les catégories de destinataires (en particulier, les détails de la divulgation à des destinataires dans des pays tiers ou à des organisations internationales (organismes régis par le droit international public ou créés par un accord entre des pays)). Sur demande, cela inclut l'identité réelle de ces destinataires (affaire C-154/21, *RW c. Österreichische Post AG*). Toutefois, les destinataires internes agissant sous l'autorité du responsable du traitement (par exemple, les employés) ne sont généralement pas considérés comme des « *destinataires* » à cette fin. Les informations sur les autres employés qui ont accédé aux données à caractère personnel de la personne concernée ne devraient être fournies que si elles sont essentielles pour permettre à la personne concernée d'exercer ses droits - et même dans ce cas, les droits et libertés de ces autres employés devraient être pris en compte (affaire C-579/21, question préjudicielle introduite par l'Itä-Suomen hallinto-oikeus (tribunal administratif de Finlande orientale)) ;

- la période de conservation envisagée ou, si cela n'est pas possible, les critères utilisés pour déterminer cette période ;

- les droits de la personne à la rectification ou à l'effacement, à la limitation du traitement ou à l'opposition au traitement et à l'introduction d'une réclamation auprès d'une autorité de contrôle ;

- des informations concernant la source des données (si elle n'a pas été collectée auprès de la personne concernée) ; et

- toute prise de décision automatisée réglementée (c'est-à-dire les décisions prises entièrement sur une base automatisée et ayant des effets juridiques ou des effets similaires significatifs ; également, la prise de décision automatisée impliquant des catégories particulières de données) - y compris des informations sur la logique impliquée et sur l'importance et les conséquences envisagées du traitement pour la personne concernée.

Si le responsable du traitement n'a pas l'intention de donner suite à la demande ou ne répond dans le délai imparti, il doit également en indiquer les raisons.

Exemptions

Le RGPD reconnaît que l'accès des personnes concernées peut porter atteinte à d'autres personnes et prévoit que le droit de recevoir une copie des données ne doit pas porter atteinte à ces droits. Le considérant 63 note que cela pourrait s'étendre à la protection des droits de propriété intellectuelle et du secret des affaires (par exemple, si la divulgation de la logique de la prise de décision automatisée impliquait la divulgation de ces informations). Toutefois, le considérant indique également qu'un responsable du traitement ne peut pas refuser de fournir toutes les informations au motif que l'accès pourrait porter atteinte aux droits d'autrui.

L'Article 23 du RGPD permet, dans des conditions spécifiques, à un législateur national ou de l'Union de restreindre, au moyen d'une mesure législative, la portée des obligations et des droits prévus par le droit d'accès.

Le considérant 63 contient également deux autres dispositions limitatives utiles :

- si le responsable du traitement détient une grande quantité de données, il peut demander à la personne concernée de préciser les informations ou les activités de traitement sur lesquelles porte la demande. (Toutefois, le considérant ne précise pas qu'il existe une exemption en raison de volumes importants de données pertinentes : la limitation semble davantage liée à la spécificité de la demande qu'à l'importance du temps et des efforts consacrés par le responsable du traitement - bien que les deux puissent, bien entendu, être liés) ;

- le droit de la personne concernée est « *de prendre connaissance du traitement et d'en vérifier la licéité* ». Cela confirme les observations formulées par la CJUE dans l'affaire *YS c. Minister voor Immigratie, Integratie en Asiel* (affaire C-141/12), selon lesquelles la finalité des demandes d'accès des personnes concernées est de permettre à ces dernières de confirmer l'exactitude des données et la licéité du traitement et d'exercer leurs droits de rectification ou d'opposition, le cas échéant. En d'autres termes, la finalité est liée aux droits de la personne en vertu de la législation sur la protection des données : les demandes formulées à d'autres fins, non liées à la protection des données, peuvent éventuellement être rejetées.

Pour en savoir plus :

Lignes directrices du CEPD 01/2022 sur les droits des personnes concernées - Droit d'accès

Rectification

Tout personne concernée peut exiger d'un responsable du traitement qu'il rectifie les inexactitudes dans les données à caractère personnel la concernant. Dans certaines circonstances, si les données à caractère personnel sont incomplètes, une personne peut exiger du responsable du traitement qu'il complète les données ou qu'il enregistre une déclaration complémentaire.

Portabilité

Le droit d'accès prévu par le RGPD donne déjà aux individus le droit d'exiger que leurs données soient fournies sous une forme électronique couramment utilisée.

La portabilité des données va plus loin et exige que le responsable du traitement fournisse les informations sous une forme structurée, couramment utilisée et lisible par machine, de sorte qu'elles puissent être transférées sans entrave par la personne concernée à un autre responsable du traitement.

En outre, le responsable du traitement peut être tenu de transmettre les données directement à un autre responsable du traitement lorsque cela est techniquement possible. Le RGPD encourage les responsables du traitement à développer des formats interopérables.

Alors que l'accès à l'information est un droit large, la portabilité est un droit plus étroit. Il s'applique :

- aux données à caractère personnel traitées par des moyens automatisés (pas aux dossiers papier) ;
- aux données à caractère personnel que la personne concernée a fournies au responsable du traitement ; et
- uniquement lorsque la base du traitement est le consentement, ou que les données sont traitées pour l'exécution d'un contrat ou de mesures préparatoires à un contrat.

Les données que la personne « *a fournies* » font l'objet d'une interprétation large. Conformément aux lignes directrices de l'ancien groupe de travail « Article 29 », cette notion ne se limite pas aux formulaires remplis par une personne, mais aux informations recueillies par le responsable du traitement dans le cadre de ses relations avec la personne ou générées par l'observation de son activité. Voici quelques exemples de cas où la portabilité des données s'applique : (i) les données détenues par un service de streaming musical, (ii) les titres de livres détenus par une librairie en ligne, (iii) les données provenant d'un compteur intelligent ou d'autres objets connectés, (iv) les journaux d'activité, (v) l'historique de l'utilisation d'un site internet, (vi) les activités de recherche ou (vii) les courriels envoyés à la personne. Toutefois, le droit à la portabilité ne s'étend pas aux données à caractère personnel qui sont déduites ou dérivées par le responsable du traitement (par exemple, les résultats d'une analyse algorithmique du comportement d'une personne).

Alors que la portabilité des données ne s'applique qu'aux responsables du traitement, les sous-traitants auront l'obligation contractuelle d'aider les responsables du traitement « *par des mesures techniques et organisationnelles appropriées* » à répondre aux demandes de portabilité. Les responsables du traitement doivent donc mettre en œuvre des procédures spécifiques avec leurs sous-traitants pour traiter ces demandes.

La portabilité des données ne doit pas porter atteinte aux droits d'autrui. Toutefois, selon les autorités de contrôle, le responsable initial du traitement des données n'est pas responsable de la conformité du responsable du traitement destinataire. Au contraire, toute organisation recevant les données doit s'assurer que l'utilisation qu'elle en fait est légale.

Il existe des dérogations à la portabilité, par exemple lorsque celle-ci porte atteinte à des droits de propriété intellectuelle ou au secret des affaires. Les autorités de contrôle considèrent que cela ne dispense pas de respecter ce droit.

Les exigences en matière de portabilité des données peuvent également entrer en conflit avec d'autres exigences en matière d'accès et de portabilité prévues par la législation sectorielle de l'UE (par exemple, le droit d'accéder à l'historique de son compte bancaire en vertu de la directive sur les services de paiement 2) ou par la législation des États membres. Les lignes directrices du groupe de travail « Article 29 » expliquent que le droit à la portabilité prévu par le RGPD ne s'appliquera pas si l'individu indique clairement qu'il exerce ses droits en vertu d'une autre loi. Toutefois, si la personne cherche à exercer ses droits en vertu du RGPD, le responsable du traitement doit évaluer l'interaction entre les droits concurrents au cas par cas, mais la législation plus spécifique ne supplantera pas automatiquement le droit RGPD.

Nouvelles lois de l'UE

Dans la pratique, la portabilité a eu un effet limité. En effet, elle ne s'applique qu'à certaines données à caractère personnel (fournies par l'utilisateur) et lorsque la base légale du traitement est le consentement ou le contrat - et le responsable du traitement dispose d'un mois pour répondre aux demandes. Le règlement sur les données et le règlement sur les marchés numériques renforcent les droits en matière de portabilité.

Le règlement sur les données s'applique aux fabricants de produits connectés lorsqu'un produit connecté génère des données conçues pour être récupérées par le fabricant. Elle s'applique également aux données générées par les services connexes, c'est-à-dire les services qui permettent à l'utilisateur de contrôler les fonctionnalités du produit connecté (par exemple, pouvoir déverrouiller une voiture à distance). Le règlement sur les données prévoit que les données relatives aux produits et aux services connexes doivent être mises à la disposition de l'utilisateur sans délai et gratuitement. Le cas échéant et si cela est techniquement possible, l'accès doit se faire en temps réel et en continu. L'utilisateur peut également exiger que les données soient fournies à un tiers.

Les données qui ne sont générées qu'après un investissement supplémentaire du fabricant sont exclues et il existe des protections pour les secrets d'affaires. Si une personne autre que la personne concernée par les données est l'utilisateur final de l'appareil, le règlement sur les données en tient compte en prévoyant que les données ne doivent être mises à la disposition de cet utilisateur que s'il existe une base légale pour cela en vertu du RGPD.

Dans l'ensemble, le droit accordé par le règlement sur les données est plus important que la portabilité prévue par le RGPD : il est plus rapide et s'applique à davantage de données (il n'est pas nécessaire qu'elles soient à caractère personnel ; elles ne doivent pas être fournies par la personne concernée ; et elles ne dépendent pas de la base légale utilisée par le fabricant pour son traitement).

Le règlement sur les marchés numériques étend également la portabilité. Pour leurs services réglementés, les « *contrôleurs d'accès* » doivent assurer la portabilité effective des données fournies par l'utilisateur final ou générées par l'activité de l'utilisateur final sur le service, là encore, par un accès continu et en temps réel aux données, sans frais.

Où puis-je trouver ces dispositions ?

Accès du sujet, article 15, considérants 59, 63, 64

Rectification, article 16

Portabilité, article 20 et WP 242, considérant 68

Droit d’opposition

En bref

Les personnes ont le droit de s’opposer à certains types de traitement :

- la prospection commerciale ;
- le traitement fondé sur les intérêts légitimes ou l’exécution d’une mission d’intérêt public/l’exercice de l’autorité publique ; et
- le traitement à des fins de recherche ou de statistiques.

Seul le droit de s’opposer à la prospection commerciale est absolu (c’est-à-dire qu’il n’est pas nécessaire de justifier des raisons pour lesquelles on s’y oppose et qu’il n’existe aucune dérogation permettant de poursuivre le traitement).

Il est obligatoire d’informer les personnes de ces droits suffisamment tôt, de manière claire et distincte des autres informations.

Les services en ligne doivent offrir une méthode automatisée d’opposition.

À faire

Passez en revue les mentions et politiques relatives à la protection des données à caractère personnel pour vérifier que les personnes sont bien informées de leur droit d’opposition, de manière claire et séparée des autres informations, au moment de la « *première communication* ».

Pour les services en ligne, vérifiez qu’il existe un moyen automatisé à cette fin.

Examinez les listes et processus de suppression marketing (y compris ceux gérés pour le compte de votre organisation par des partenaires ou des fournisseurs de service) afin de vérifier qu’ils sont en mesure de fonctionner en conformité avec le RGPD.

Droits d'opposition

Trois droits d'opposition sont prévus par le RGPD. Tous concernent le traitement effectué à des fins spécifiques ou justifié par une base particulière. Une personne n'a pas le droit de s'opposer à un traitement en général.

Ce sont les droits de s'opposer à :

Traitements à des fins de prospection commerciale

Il s'agit d'un droit absolu ; une fois que la personne s'y oppose, les données ne doivent plus être traitées à des fins de prospection commerciale. Cela inclut le profilage dans la mesure où il est lié à la prospection.

Traitement à des fins scientifiques/historiques/de recherche/statistiques

Dans cette hypothèse, le droit est moins fort que le droit d'opposition à la prospection commerciale, car il doit exister des « *raisons tenant à la situation particulière [de la personne concernée*] ».

Il existe une exception lorsque le traitement est nécessaire à l'exécution d'une tâche effectuée pour des raisons d'intérêt public.

Traitements basés sur deux objectifs spécifiques :

1. des motifs d'intérêt légitime (c'est-à-dire au titre de l'Article 6 (1)(f)) ; ou

2. parce qu'elles sont nécessaires à une mission d'intérêt public ou à l'exercice de l'autorité publique (c'est-à-dire l'article 6(1)(e)).

Là encore, ce droit peut être exercé pour des raisons tenant à la situation particulière de la personne concernée.

Le responsable du traitement doit alors cesser le traitement des données à caractère personnel à moins :

- qu'il puisse démontrer des motifs légitimes impérieux qui l'emportent sur les intérêts de la personne concernée ; ou

- que le traitement soit destiné au constat, à l'exercice ou à la défense de droits en justice.

Ainsi, lorsqu'une personne s'y oppose, sur la base de sa situation particulière, il incombe au responsable du traitement d'établir pourquoi il devrait néanmoins pouvoir continuer à traiter des données à caractère personnel sur cette base.

L'Article 23 du RGPD permet, dans des conditions spécifiques, à un législateur national ou de l'Union de restreindre, au moyen d'une mesure législative, la portée des obligations et des droits prévus par le droit d'opposition.

En décembre 2023, la CJUE a rendu son arrêt dans les affaires combinées C-26/22 et 64/22 portant sur la conservation des données d'insolvabilité par les sociétés d'information financière sur le crédit) en Allemagne. La Cour a estimé que, dans les cas où une agence de notation cherchait à conserver des données relatives à l'insolvabilité au-delà de la période pendant laquelle la loi allemande autorisait leur publication, cette conservation était illégale, nonobstant tout code de conduite disposant le contraire émis par l'autorité compétente en matière de protection des données. Les personnes concernées ont le droit de s'opposer au traitement de leurs données à caractère personnel au-delà de la période légale de publication et si le responsable du traitement ne peut pas prouver qu'il a des motifs légitimes de poursuivre le traitement qui prévalent sur les intérêts des personnes concernées, alors la personne concernée peut demander l'effacement des données en vertu de l'Article 17.

Informer les personnes de leurs droits

En cas de traitement à des fins de prospection commerciale et de traitement fondé sur des missions d'intérêt public/intérêts légitimes, le droit d'opposition de la personne doit être explicitement porté à son attention, au plus tard lors de la première communication avec elle. Ce droit doit être présenté clairement et séparément des autres informations.

Cette nécessité d'informer la personne ne s'applique pas au traitement fondé sur les statistiques et la recherche.

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

Pour en savoir plus :

Lignes directrices du CEPD 10/2020 sur les limitations au titre de l'article 23 du RGPD

Où puis-je trouver ces dispositions ?

Considérants 69 et 70, article 21

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

En bref

Des droits plus étendus et moins clairs ont été introduits : le droit à l'oubli (désormais appelé « *effacement* ») et le droit à la limitation du traitement.

Les personnes peuvent exiger que les données soient « *effacées* » lorsque la licéité sous-jacente du traitement pose problème, lorsqu'elles retirent leur consentement ou lorsque la personne concernée s'est opposée aux intérêts légitimes du responsable du traitement et qu'il n'y a pas de raisons impérieuses de poursuivre le traitement.

La personne concernée peut exiger du responsable du traitement qu'il « *limite* » le traitement des données pendant que les réclamations (par exemple, concernant l'exactitude) sont résolues, ou si le traitement est illicite, mais que la personne s'oppose à l'effacement.

Les responsables du traitement qui ont rendu publiques ou partagé avec des tiers des données qui font ensuite l'objet d'une demande d'effacement sont tenus d'informer les autres personnes qui traitent ces données des détails de la demande. Il s'agit d'une obligation de grande envergure et difficile à remplir.

Lorsque des données à caractère personnel sont obtenues automatiquement auprès de tiers et font ensuite l'objet d'une demande d'effacement, les responsables du traitement doivent veiller à demander à leurs fournisseurs de données de ne pas fournir à nouveau les données à caractère personnel qui ont été effacées.

À faire

Vérifiez que les membres de votre personnel et que vos fournisseurs susceptibles de recevoir des demandes d'effacement les reconnaissent et sachent comment les traiter.

Déterminez si vos systèmes sont capables de respecter les exigences de signalement de données comme étant limitées pendant que les réclamations sont en train d'être résolues ; entreprenez des travaux de développement si nécessaire.

Droit à l'oubli

Les personnes ont le droit d'obtenir l'« *effacement* » de leurs données dans certaines situations spécifiques - essentiellement lorsque le traitement ne satisfait pas aux exigences du RGPD. Ce droit peut être exercé à l'encontre des responsables du traitement, qui doivent répondre dans un délai raisonnable (et en tout état de cause dans un délai d'un mois, bien que ce délai puisse être prolongé dans les cas difficiles).

Quand est-ce que le droit s'applique-t-il ?

- Lorsque les données ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées ou traitées.

- Si la personne retire son consentement au traitement (et s'il n'y a pas d'autre justification au traitement).

    - Il existe un autre élément déclencheur concernant le retrait du consentement précédemment donné par un enfant en ce qui concerne les services en ligne. Toutefois, cela ne semble rien ajouter au principe général selon lequel le consentement peut être révoqué et, le cas échéant, la personne peut exiger que les données soient effacées.

- Au traitement fondé sur des intérêts légitimes - si la personne s'y oppose et que le responsable du traitement ne peut pas démontrer qu'il existe des motifs légitimes impérieux pour le traitement. La charge de la preuve incombe au responsable du traitement et la situation particulière de la personne doit être prise en compte (voir la section sur le droit d'opposition ci-dessus).

- Lorsque les données sont traitées de manière illicite (c'est-à-dire d'une manière qui enfreint le RGPD).

- Si les données doivent être effacées pour se conformer au droit de l'Union ou de l'État membre qui s'applique au responsable du traitement.

La dernière condition pourrait, par exemple, s'appliquer si une personne considère qu'un responsable du traitement conserve des données à caractère personnel alors que la législation prévoit que ces données (par exemple un contrôle lié à l'emploi) doivent être supprimées après une période déterminée.

La disposition générale « fourre-tout » autorisant les demandes d'effacement lorsque les données sont traitées « *illicitement* » est potentiellement complexe : il existe de nombreuses raisons pour lesquelles les données peuvent être traitées illicitement en vertu du RGPD (elles peuvent être inexactes ; un élément d'une mention d'information peut ne pas avoir été fourni à l'individu). Toutefois, il n'est pas évident que cela doive conférer un droit à l'effacement des données. Il sera donc important d'examiner comment les États membres appliquent les dispositions d'exemption.

Données tombées dans le domaine public

Si le responsable du traitement a rendu publiques des données à caractère personnel et qu'il est tenu de les effacer, il doit également informer les autres responsables de traitement qui traitent les données que la personne concernée a demandé l'effacement de ces données. Cette obligation vise à renforcer les droits des personnes dans un environnement en ligne.

L'obligation est de prendre des mesures raisonnables et il faut tenir compte de la technologie disponible et du coût de la mise en œuvre. Cependant, l'obligation est potentiellement étendue et extrêmement difficile à mettre en œuvre. Par exemple, lorsqu'il s'agit de données du domaine public, on peut se demander comment le responsable du traitement d'origine pourra identifier les responsables du traitement qu'il doit notifier.

Autres obligations de notification aux destinataires

Si le responsable du traitement doit effacer des données à caractère personnel, il doit en informer toute personne à laquelle il a communiqué ces données, à moins que cela ne soit impossible ou n'implique des efforts disproportionnés.

Exemptions

L'obligation ne s'applique pas si le traitement est nécessaire :

- pour l'exercice du droit à la liberté d'expression et d'information ;
- pour le respect d'une obligation légale de l'Union ou d'un État membre ;
- pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ;
- pour des raisons de santé publique ;
- à des archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques (si les conditions applicables à ce type de traitement sont remplies) ; ou
- si cela est nécessaire pour l'établissement, l'exercice ou la défense d'un droit en justice.

Voir la section sur les dérogations et conditions particulières pour d'autres situations dans lesquelles des exemptions peuvent être pertinentes - si elles sont prévues par le droit de l'Union ou des États membres.

Pour en savoir plus :

Lignes directrices du CEPD 5/2019 sur les critères du droit à l'oubli dans le cas des moteurs de recherche (partie 1)

Droit à la limitation du traitement

Ce droit remplace les dispositions de l'ancienne directive sur la protection des données relatives au « *verrouillage* ». Dans certaines situations, ce droit donne à la personne concernée une alternative à la demande d'effacement des données. Dans d'autres, il lui permet d'exiger que les données soient maintenues en attente pendant que d'autres problèmes sont résolus.

Qu'est-ce qu'une restriction ?

Si les données à caractère personnel sont « *restreintes* », le responsable du traitement ne peut que les conserver. Il ne peut traiter les données ultérieurement que si :

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

Lorsque les données sont traitées automatiquement, la limitation doit être effectuée par des moyens techniques et consignée dans les systèmes informatiques du responsable du traitement. Il peut s'agir de déplacer les données vers un système distinct, de bloquer temporairement les données sur un site internet ou de rendre les données indisponibles d'une autre manière.

Si les données ont été divulguées à d'autres personnes, le responsable du traitement doit informer ces destinataires du traitement restreint (sauf si cela est impossible ou implique des efforts disproportionnés).

Le responsable du traitement doit informer la personne concernée avant de lever une restriction.

Quand est-ce que la limitation est-elle applicable ?

- Lorsqu'une personne conteste l'exactitude des données, les données à caractère personnel seront limitées pendant la période de vérification ;
- Lorsqu'une personne s'est opposée au traitement (sur la base d'intérêts légitimes), elle peut exiger que les données soient limitées pendant que le responsable du traitement vérifie les motifs du traitement ;
- Lorsque le traitement est illégal, mais que la personne s'oppose à l'effacement et demande la limitation à la place ; et
- Lorsque le responsable du traitement n'a plus besoin des données, mais que la personne a besoin des données à caractère personnel pour la constatation, l'exercice ou la défense d'un droit en justice.

La dernière condition, par exemple, signifie que les responsables du traitement sont obligés de conserver les solutions de stockage de données pour les anciens clients si les données à caractère personnel sont pertinentes pour les procédures dans lesquelles les personnes sont impliquées.

Commentaire de la jurisprudence sur le droit à l'effacement ou à la limitation du traitement

L'affaire C-60/22 concernait une situation dans laquelle le responsable du traitement avait omis de conclure un accord déterminant la responsabilité conjointe du traitement (Article 26) et de tenir un registre des activités de traitement (Article 30) et dans laquelle une personne concernée cherchait à faire valoir que cela déclenchait le droit à l'effacement. La CJUE a déterminé qu'il ne s'agissait pas d'un traitement illicite conférant à la personne concernée un droit à l'effacement ou à la limitation du traitement, dès lors que ce manquement ne constituait pas une violation du principe de « *responsabilité* » énoncé à l'Article 5, (2) du RGPD.

Où puis-je trouver ces dispositions ?

Droit à l'effacement, articles 17 et 19, considérants 65, 66 et 73

Droit à la restriction, articles 18 et 19,

Considérants 67 et 73

Profilage et processus de décision automatisé

En bref

Les règles relatives à la prise de décision automatisée s'appliquent aux décisions :

- prises entièrement sur la base d'un traitement automatisé ; et
- qui produisent des effets juridiques ou des effets similaires significatifs.

Lorsque la décision est :

- nécessaire à la conclusion ou à l'exécution d'un contrat ; ou
- autorisée par le droit de l'Union ou de l'État membre applicable au responsable du traitement ; ou
- repose sur le consentement explicite de la personne concernée, le traitement automatisé peut être utilisé. Toutefois, des mesures appropriées pour protéger les intérêts de la personne doivent toujours être mises en place.

Il existe des restrictions supplémentaires concernant le profilage basé sur des catégories particulières de données - qui nécessite un consentement explicite, ou qui doit être autorisé par le droit de l'Union ou de l'État membre et qui est nécessaire pour des raisons d'intérêt public importantes.

À faire

Vérifier l'importance de la prise de décision automatisée. Identifiez les décisions qui s'appuient sur :

- le consentement ;
- une autorisation légale ; ou
- des données relatives à des catégories particulières de données ou à des enfants.

Si la prise de décision automatisée est fondée sur le consentement, assurez-vous que celui-ci est explicite.

Si la prise de décision automatisée repose sur des catégories particulières de données ou les utilise :

- Vérifiez si vous pouvez obtenir un consentement explicite ;
- Si ce n'est pas le cas, vous ne pouvez effectuer un tel traitement que s'il est autorisé par le droit de l'Union ou des États membres.

Si la prise de décision automatisée concerne des enfants, demandez conseil : ce traitement est limité.

Définition de profilage

Le profilage est « *toute forme de traitement automatisé de données à caractère personnel visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements* ».

Au cours du processus législatif initial, des tentatives ont été faites pour introduire des restrictions significatives à tout profilage. Toutefois, ces restrictions n'ont finalement pas été incluses, bien que le considérant 72 indique que le CEPD peut publier des lignes directrices sur le profilage. En mai 2018, le CEPD a approuvé les lignes directrices de l'ancien groupe de travail « Article 29 » relative à la prise de décision individuelle et au profilage (WP 251 rev.01).

Restrictions à la prise de décision automatisée avec des effets significatifs

Les restrictions concernant les décisions fondées exclusivement sur un traitement automatisé (y compris le profilage) s'appliquent si les décisions produisent des effets juridiques ou affectent de manière significative la personne concernée. Le considérant 71 donne l'exemple des décisions de crédit en ligne et du recrutement en ligne ; il précise également que l'élément répréhensible est l'absence d'intervention humaine significative.

Selon les lignes directrices du CEPD, les « *effets juridiques* » sont ceux qui ont un impact sur les droits légaux d'une personne, tels que les droits statutaires ou contractuels (par exemple, une personne se voyant refuser l'entrée à une frontière, se voyant refuser une prestation sociale accordée par la loi ou l'annulation d'un contrat). L'affectation « *de manière significative de façon similaire* » correspond aux effets qui sont équivalents ou significatifs de la même manière que les effets juridiques. L'effet doit être plus que trivial et doit avoir le potentiel d'influencer de manière significative les circonstances, le comportement ou les choix des individus concernés (par exemple, le refus automatique d'une demande de crédit en ligne ou les pratiques de recrutement en ligne sans intervention humaine significative). Cela dépend en grande partie du contexte et il est donc difficile de dresser une liste fixe de ce qui peut être considéré comme « *significatif* ».

Dans l'affaire *Schufa* (C-634/21), la CJUE a estimé que les agences de référence en matière de crédit prennent des décisions individuelles automatisées lorsqu'elles créent un score de crédit basé sur des probabilités et que des tiers, tels que les créanciers, s'appuient fortement sur ce score pour évaluer les demandes de prêt.

La CJUE a rejeté les arguments selon lesquels les créanciers prenaient les décisions et les agences de référence du crédit se livraient à des actes préparatoires.

Il est possible d'avoir recours à de tels traitements automatisés significatifs si ceux-ci sont :

- nécessaires à la conclusion ou à l'exécution d'un contrat entre une personne concernée et un responsable du traitement ;
- autorisés par le droit de l'Union ou des États membres ; ou
- fondés sur la base du consentement explicite de la personne.

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

Décisions automatisées fondées sur le consentement explicite ou l'exécution d'un contrat

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

Les dispositions équivalentes de l'ancienne directive sur la protection des données disposaient que cela n'était pas nécessaire si la décision avait pour effet d'accéder à la demande de l'individu. Cette disposition n'a pas été reprise dans le RGPD.

Le considérant 71 souligne que des techniques statistiques appropriées doivent être utilisées, que la transparence doit être assurée, que des mesures doivent être mises en place pour corriger les inexactitudes et les risques d'erreurs, et que la sécurité doit être assurée et les effets discriminatoires évités.

Selon les lignes directrices susmentionnées, les responsables du traitement doivent effectuer des tests réguliers sur les ensembles de données qu'ils traitent afin de vérifier l'absence de biais et des mesures doivent être prises pour éviter les erreurs, les inexactitudes ou la discrimination sur la base de catégories particulières de données. Il est également conseillé de procéder à des audits des algorithmes.

Autorisation légale

Dans le second cas (autorisation par la loi), la loi elle-même doit contenir des mesures appropriées pour sauvegarder les intérêts des personnes. Le considérant 71 mentionne le profilage pour assurer la sécurité et la fiabilité des services ou dans le cadre de la surveillance de la fraude et de l'évasion fiscale comme des types de décisions automatisées qui pourraient être justifiées sur la base du droit de l'Union ou des États membres.

Catégories particulières de données

La prise de décision automatisée fondée sur catégories particulières de données à caractère personnel est encore plus limitée. Les décisions fondées sur ces types de données ne peuvent être prises que dans les cas suivants :

- avec un consentement explicite ; ou
- lorsque le traitement est nécessaire pour des raisons d'intérêt public importantes et sur la base du droit de l'Union ou de l'État membre - qui doit comprendre des mesures visant à protéger les intérêts des personnes concernées.

Nouvelles lois de l'UE

Le règlement sur les services numériques prévoit des dispositions supplémentaires en matière de profilage pour les plateformes en ligne qui, à la demande du destinataire du service, conservent et diffusent des informations au public.

Plus précisément, il est interdit à ces plateformes (i) d'utiliser des catégories particulières de données (par exemple, l'origine raciale ou ethnique, les convictions politiques et les données relatives à la santé) pour le profilage à des fins publicitaires (Article 26 (3) du règlement sur les services numériques) et (ii) d'utiliser le profilage à des fins publicitaires lorsqu'il est établi que l'utilisateur est mineur (Article 28 (2) du règlement sur les services numériques).

Le règlement sur les marchés numériques contient également des dispositions sur le profilage. Les « *contrôleurs d'accès* » sont tenus de publier des informations sur leur utilisation du profilage et de se soumettre à un audit indépendant de leur profilage. Les résultats de l'audit doivent être communiqués à la Commission qui, à son tour, les communiquera au CEPD (Article 15 du règlement sur les marchés numériques).

Focus sur la France : Possibilité pour l'Administration de recourir à des décisions individuelles automatisées

En France, l'Article 47 (2°) de la Loi Informatique et Libertés ouvre la possibilité pour l'Administration de recourir à des décisions individuelles automatisées. Néanmoins, le traitement ne peut pas porter sur des catégories particulières de données, et l'Administration doit informer les personnes de leur droit de connaître les informations contenues dans un document administratif dont les conclusions lui s'y opposées. L'Administration est tenue de s'assurer de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard.

Pour en savoir plus :

- Anciennes lignes directrices du groupe de travail « Article 29 » relatives à la prise de décision individuelle automatisée et le profilage aux fins du règlement (UE) 2016/679 (WP 251 rev.01) (approuvées par le CEPD).
- Lignes directrices 10/2020 du CEPD concernant les limitations au titre de l'article 23 du RGPD
- Arrêt de la Cour (première chambre) du 7 décembre 2023. OQ contre Land Hessen (SCHUFA Affaire C-634/21).
- Affaire C-203/22 Dun & Bradstreet Autriche

Où puis-je trouver ces dispositions ?

Article 4, (4), et article 22, considérants 71 et 72

Obligations de gouvernance des données

En bref

Le RGPD exige que toutes les organisations mettent en œuvre un large éventail de mesures pour réduire le risque de violation au RGPD et pour prouver qu'elles prennent la gouvernance des données au sérieux.

Il s'agit notamment de mesures de responsabilisation telles que les AIPD, les audits, les politiques, les registres des activités de traitement et (éventuellement) la désignation d'un délégué à la protection des données (« DPD ») ou *data protection officer* (« DPO »).

À faire

Déterminez les responsabilités et le budget pour la mise en conformité en matière de protection des données au sein de votre organisation. Que vous décidiez ou non de nommer un DPD (ou que vous soyez obligé de le faire), la longue liste de mesures de gouvernance des données du RGPD nécessite l'attribution de la responsabilité pour leur adoption.

Veillez à ce qu'un programme de conformité complet soit conçu pour votre organisation, intégrant des éléments tels que : des AIPD, des audits réguliers, des révisions de politiques et des programmes de formation et de sensibilisation.

Vérifiez les accords existants avec les fournisseurs et assurez-vous que les modèles d'appels d'offres et de contrats d'approvisionnement reflètent les obligations du RGPD du sous-traitant.

Suivez la publication par les autorités de contrôle / l'UE et la publication sectorielle de conditions et codes de pratique des fournisseurs pour voir si elles peuvent être utilisées par votre organisation.

Affinez et tenez à jour les registres des activités de traitement de votre organisation.

Le RGPD consacre un certain nombre de concepts de « *gouvernance des données* », dont les législateurs et les autorités de contrôle vantent les mérites depuis un certain temps. Ces concepts créent des obligations et des coûts opérationnels importants pour de nombreuses organisations des secteurs public et privé.

Les responsables du traitement ont l'obligation générale d'adopter des mesures techniques et organisationnelles appropriées pour satisfaire à leurs obligations au titre du RGPD (et de pouvoir démontrer qu'ils l'ont fait).

Protection des données dès la conception et par défaut (alias « Privacy by design »)

Les responsables du traitement sont tenus de mettre en place des mesures techniques et organisationnelles appropriées qui :

- sont conçues pour mettre en œuvre les principes de protection des données et intégrer des garanties pour la protection des droits des personnes concernées ; et

- garantissent que, par défaut, seules les données à caractère personnel nécessaires à la finalité spécifique du traitement sont utilisées.

Lorsqu'ils envisagent de concevoir des mesures techniques et organisationnelles, les responsables du traitement doivent évaluer l'état de la technique, le coût de la mise en œuvre, la nature, la portée et les raisons de l'utilisation, ainsi que les différents niveaux de risques que l'utilisation donnée des données à caractère personnel fait peser sur les droits et libertés des personnes. Le RGPD dispose qu'une telle évaluation doit être effectuée à la fois au moment de décider comment traiter les données à caractère personnel et pendant le traitement des données à caractère personnel. Parmi les exemples de mesures visant à respecter le principe de minimisation des données mentionnées dans le RGPD, on peut citer l'adoption de politiques du personnel appropriées et l'utilisation de la pseudonymisation.

De plus amples informations sur ce que les organisations sont censées faire peuvent être trouvées dans les lignes directrices 4/2019 relatives à l'Article 25 – protection des données dès la conception et protection des données par défaut (les « *Lignes Directrices Article 25* ») qui ont été adoptées le 20 octobre 2020. Ces Lignes Directrices Article 25 se concentrent sur l'interprétation des exigences de l'Article 25 du RGPD, en explorant les obligations légales imposées et en fournissant un certain nombre d'exemples opérationnels. D'autres sujets couverts par les Lignes Directrices Article 25 comprennent les mécanismes de certification de la conformité à l'Article 25, la façon dont l'Article 25 peut être mis en œuvre par les autorités de contrôle, et les recommandations pour les parties prenantes (qui comprennent les responsables du traitement et les fournisseurs de technologie) sur la façon dont le CEPD considère que la protection des données dès la conception et par défaut peut être mise en œuvre avec succès.

Dispositions relatives aux responsables conjoints du traitement

Les responsables conjoints du traitement (c'est-à-dire deux responsables ou plus qui déterminent conjointement la finalité et les moyens du traitement) sont tenus d'organiser entre eux leurs responsabilités respectives en ce qui concerne le respect du RGPD - et, en particulier, l'exercice des droits des personnes concernées et la fourniture d'informations de transparence aux individus. L'accord doit définir les rôles et responsabilités des parties à l'égard des personnes concernées, et l'essentiel de l'accord doit être mis à la disposition des personnes concernées (par exemple, par le biais d'un avis de confidentialité).

Bien qu'aucune disposition législative n'exige qu'un accord entre responsables conjoints du traitement fasse l'objet d'un contrat formel, il serait judicieux de le faire, par exemple pour des raisons de responsabilité. Dans ses lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD (« *Lignes Directrices RT/ST* ») adoptées le 7 juillet 2021, le CEPD confirme qu'il est recommandé de documenter « *les facteurs pertinents et l'analyse menée en interne afin d'attribuer les différentes obligations* »

Les Lignes Directrices RT/ST se concentrent sur l'appréciation de la responsabilité conjointe et sur les exigences imposées aux parties lorsque leur responsabilité conjointe est établie.

Depuis l'entrée en vigueur du RGPD, la CJUE a rendu un certain nombre d'arrêts qui explorent le concept de responsabilité conjointe, bien que ces décisions aient été rendues dans le cadre des

dispositions de la directive sur la protection des données. L'un des principaux enseignements de cette jurisprudence est qu'une interprétation assez large de la notion de responsabilité conjointe est en train d'émerger.

Les cas les plus importants sont les suivants :

- l'affaire de la « *Page Fan Facebook* » (*Unabhängiges Landeszentrum für Datenschutz SchleswigHolstein c. Wirtschaftsakademie Schleswig-Holstein GmbH* (affaire C-210/16)) ;

- l'affaire des « *Témoins de Jéhovah* » (référencée *Tietosuojavaltuutettu* (Affaire C-25/17)) ; et

- L'affaire du « *bouton J'aime de Facebook* » (*Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV* (affaire C-40/17)).

Analyses d'impact relatives à la protection des données (AIPD)

Qu'est-ce qu'une AIPD et quand est-elle nécessaire ?

Une Analyse d'Impact relative à la Protection des Données, est un processus permettant de démontrer la conformité et d'évaluer et d'atténuer les risques. Le RGPD formalise l'obligation de réaliser des AIPD dans certaines circonstances. Plus précisément, les responsables du traitement doivent s'assurer qu'une AIPD a été réalisée pour toute activité de traitement « *à risque élevé* » avant qu'elle ne commence. Le « *risque élevé* » est ici mesuré par rapport au risque d'atteinte aux droits et libertés d'une personne physique.

Parmi les exemples de traitement à risque élevé définis dans le RGPD, on peut citer

- l'évaluation systématique et approfondie, y compris le profilage et lorsque les décisions ont des effets juridiques - ou des effets significatifs similaires - sur les personnes physiques ;

- le traitement à grande échelle de catégories particulières de données ou de données relatives à des condamnations pénales ou à des infractions ; ou

- la surveillance systématique et à grande échelle d'une zone accessible au public (par exemple, la vidéosurveillance).

Les lignes directrices (WP248 rev.01) publiées en 2017 et approuvées par le CEPD (les « *Lignes Directrices AIPD* »), indiquent que d'autres facteurs peuvent accroître le risque, y compris la présence de personnes concernées vulnérables (par exemple des enfants, et notamment des employés), l'appariement ou la combinaison d'ensembles de données de manière inattendue du point de vue des personnes concernées, et le traitement conçu pour refuser à une personne un droit ou l'accès à un contrat ou à un service.

Les organisations doivent veiller à vérifier également les exigences locales. La plupart des pays de l'UE ont publié et fait approuver par le CEPD leurs listes d'activités de traitement de données à caractère personnel qui nécessitent une AIPD ou (comme c'est le cas pour une poignée d'entre eux) qui n'en nécessitent pas en vertu de l'Article 35 (4) et (5).

Existe-t-il un formulaire type pour les AIPD ?

Il n'existe pas de formulaire obligatoire pour une AIPD et, comme l'indiquent les Lignes Directrices AIPD, de nombreux modèles existent déjà.

Il est intéressant de noter que les Lignes Directrices AIPD tiennent compte de deux documents ISO pertinents - l'un sur le management du risque et l'autre sur les techniques de sécurité des AIPD dans un contexte de technologies de l'information.

Au minimum, le RGPD exige qu'une AIPD comprenne :

- Une description des opérations de traitement envisagées et des finalités du traitement ;

- Une évaluation (i) de la nécessité et de la proportionnalité du traitement et (ii) des risques encourus par les personnes concernées (du point de vue des personnes concernées) ; et

- Une liste des mesures envisagées pour (i) atténuer ces risques (y compris les risques non liés à la protection des données, tels que les atteintes à la liberté de pensée et de circulation) et (ii) assurer la conformité avec le RGPD.

Que devons-nous faire d'autre ?

Si un DPO a été désigné (voir ci-dessous), il convient de lui demander son avis sur la réalisation d'une AIPD.

La consultation de l'autorité de contrôle est requise avant tout traitement de données à caractère personnel lorsque les risques ne peuvent être atténués et restent élevés - par exemple lorsque les personnes peuvent subir des conséquences importantes, voire irréversibles, du fait du traitement. Le RGPD contient des instructions spécifiques pour ce processus.

Les responsables du traitement sont tenus de demander l'avis des personnes concernées « *ou de leurs représentants* » lors de la réalisation d'une AIPD, le cas échéant. Dans le contexte du traitement des données relatives aux ressources humaines, cette disposition a été interprétée comme une obligation de consulter les employés ou leurs représentants, tels que les comités d'entreprise ou les syndicats.

Délégué à la Protection des Données (« DPD ») ou Data Protection Officer (« DPO »)

Les responsables du traitement et les sous-traitants sont libres de désigner volontairement un DPO, mais les personnes suivantes sont tenues de le faire :

- Les autorités publiques (avec quelques exceptions mineures) ;
- Toute organisation dont les activités de base nécessitent :
  - un « *suivi régulier et systématique* » des personnes concernées « *à grande échelle* » ; ou un traitement « *à grande échelle* » de catégories particulières de données ou de données relatives à des condamnations pénales et à des infractions ; et
  - ceux qui y sont contraints par la législation locale (des pays comme l'Allemagne sont susceptibles d'entrer dans cette catégorie).

Les lignes directrices concernant les délégués à la protection des données (WP 243) (« Lignes Directrices DPO ») peuvent aider les organisations à interpréter les termes « *activités de base* », « *suivi régulier et systématique* » et « *à grande échelle* ». Ces Lignes Directrices DPO comprennent 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. Il est rassurant de constater que les Lignes Directrices DPO confirment que le traitement par une organisation des informations relatives à son personnel (qui sont très susceptibles d'inclure des catégories particulières de données) est accessoire à ses activités, et non essentiel. Parmi les exemples d'activités de base, on peut citer : la surveillance exercée par une société de sécurité engagée pour protéger un espace public ; le traitement par un hôpital des données relatives à la santé des patients et le traitement par un prestataire de services de santé au travail externalisés des données relatives aux employés de ses clients.
- « *Suivi régulier et systématique* » : Toutes les formes de suivi et de profilage en ligne sont citées en exemple par le CEPD, y compris à des fins de publicité comportementale et de reciblage par courrier électronique. Parmi les autres exemples cités figurent : le profilage et l'évaluation (par exemple pour l'évaluation du crédit, la prévention de la fraude ou la fixation des primes d'assurance) ; la géolocalisation ; le suivi des données relatives à la condition physique et à la santé ; la vidéosurveillance ; le traitement par des dispositifs connectés (compteurs intelligents, voitures intelligentes, etc.) ; et les activités de marketing fondées sur des données (c'est-à-dire les « *big data* »).
- « *A grande échelle* » : ici, le CEPD indique qu'il n'est actuellement pas favorable à ce que des chiffres précis soient utilisés comme référence pour ce terme, mais qu'il est prévu de publier des seuils à l'avenir. Au lieu de cela, les Lignes Directrices DPO (révisées pour la dernière fois en avril 2017) énumèrent des facteurs génériques assez 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). Parmi les exemples de traitement à grande échelle, on peut citer : une banque ou une compagnie d'assurance qui traite les données de ses clients ; et le traitement des données de géolocalisation des clients d'une chaîne internationale de restauration rapide en temps réel à des fins statistiques par un sous-traitant spécialisé.

Les Lignes Directrices DPO confirment que lorsqu'un DPO est désigné manière volontaire, les mêmes exigences que celles fixées par le RGPD pour les DPO obligatoires s'appliquent à eux. En outre, lorsqu'une organisation choisit de désigner un DPO, elle ne peut pas limiter la portée de l'examen du DPO - le DPO doit avoir le pouvoir d'examiner tous les traitements de données.

En réponse à une incertitude du RGPD, les Lignes Directrices DPO confirment que rien n'empêche une organisation de confier au DPO la tâche de tenir les registres des activités de traitement.

Il est intéressant de noter que les lignes directrices précitées recommandent également qu'une organisation qui décide de ne pas désigner volontairement un DPO devrait documenter les raisons pour lesquelles elle ne pense pas être soumise aux critères de désignation d'un DPO (résumés ci-dessus). Ces évaluations doivent être tenues à jour et réexaminées lorsque de nouvelles activités ou de nouveaux services sont envisagés.

Si le DPO n'est pas obligatoire et qu'il n'est pas désigné volontairement, du personnel ou des consultants peuvent être nommés pour effectuer des tâches similaires, mais le CEPD précise que pour éviter toute confusion, ils ne doivent pas être appelés DPO.

Lorsqu'il est désigné, le DPO doit être choisi en fonction de ses qualités professionnelles et de ses connaissances spécialisées (que les employeurs sont tenus d'aider à conserver). Bien qu'il puisse être assisté par une équipe, il ne peut y avoir qu'un seul DPO par organisation et cette personne doit de préférence être établie dans l'UE. Les Lignes Directrices DPO précisent que plus les activités de traitement des données d'une organisation sont sensibles ou complexes, plus le niveau d'expertise attendu de son DPO est élevé.

Les organisations doivent veiller à ce que l'objectif premier de leur DPO soit d'assurer la conformité au RGPD. Leurs tâches devraient au minimum inclure : conseiller leurs collègues et contrôler la conformité de leur organisation avec le RGPD/le droit/ les politiques en matière de protection de la vie privée, notamment par la formation et la sensibilisation, la réalisation d'audits, la fourniture de conseils concernant les AIPD et la coopération avec les autorités de contrôle. Les Lignes Directrices DPO soulignent que les DPO ne seront pas personnellement responsables de la non-conformité de leur organisation au RGPD. La responsabilité incombera à l'organisation, y compris si elle entrave ou ne soutient pas le DPO dans la réalisation de son objectif principal.

Des ressources adéquates doivent être fournies pour permettre aux DPO de s'acquitter de leurs obligations au titre du RGPD, et ils doivent rendre compte au plus haut niveau de la direction.

Les entreprises d'un même groupe peuvent désigner un seul DPO. Le DPO peut être un membre du personnel ou un contractant embauché. Les principales caractéristiques des compétences d'un DPO (selon les lignes directrices sur les DPO) sont qu'il doit bien connaître les organisations qu'il représente et qu'il doit être accessible - il doit notamment être capable de communiquer facilement avec les autorités de contrôle et les personnes concernées (par exemple, les clients et le personnel) dans les pays dans lesquels l'organisation exerce ses activités. Il semble donc que les lignes directrices attendent des DPO qu'ils soient polyglottes et experts en matière de protection des données ou, du moins, qu'ils aient facilement accès à de bons services de traduction.

Les responsables du traitement et les sous-traitants doivent veiller à ce que leur DPO soit impliqué dans toutes les questions matérielles relatives à la protection des données (y compris, selon les Lignes Directrices DPO en la matière, à la suite d'une plainte pour violation du droit à la vie privée) et qu'il puisse travailler indépendamment de toute consigne et qu'il ne soit pas licencié ou pénalisé pour avoir accompli sa mission. Il reste à voir comment cette disposition sera interprétée en droit du travail. Les organisations doivent s'assurer qu'il existe un canal sécurisé et confidentiel par lequel les employés peuvent communiquer avec le DPO.

Les Lignes Directrices DPO précisent 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 en prendre acte officiellement et indiquer les raisons de sa décision. Les lignes directrices du DPO préviennent également que le DPO ne doit pas recevoir de directives sur la manière de traiter une question, sur les résultats à obtenir ou sur la nécessité de consulter ou non une autorité de régulation.

Le RGPD n'interdit pas aux DPO d'occuper d'autres fonctions, mais exige expressément que les organisations veillent à ce que ces autres tâches ne donnent pas lieu à un conflit d'intérêts pour le DPO. Les Lignes Directrices DPO vont plus loin en précisant qu'un DPO ne peut pas

occuper de postes de direction (c'est-à-dire de directeur général, de directeur de l'exploitation ou de directeur financier). D'autres cadres supérieurs, notamment les responsables des ressources humaines, du marketing ou des technologies de l'information, ou des employés de niveau inférieur qui prennent des décisions sur les finalités et les moyens du traitement ne peuvent pas non plus occuper ce poste. Si un DPO externe (par exemple un avocat) fournit des services quotidiens de DPO aux responsables de traitement ou aux sous-traitants, cette personne peut être empêchée de représenter ces entités devant les tribunaux dans des affaires portant sur des questions de protection des données.

Les coordonnées du DPO doivent être publiées et notifiées à l'autorité de contrôle de l'organisation, car le DPO doit être le point de contact pour les questions relatives au respect de la protection des données.

Bird & Bird aide les organisations à remplir cette obligation et peut être désigné comme DPO RGPD. Contactez Bird & Bird Privacy Solutions si vous souhaitez obtenir plus d'informations sur nos services de DPO.

« Représentants » RGPD

De nombreuses organisations « *établies* » hors de l'UE qui ciblent ou suivent des personnes concernées de l'UE sont tenues par le RGPD de désigner un représentant situé dans l'UE. Ce « *représentant RGPD* » doit être mandaté par une organisation en tant que point de contact alternatif ou supplémentaire auquel les personnes concernées et les autorités de contrôle peuvent s'adresser pour toutes les questions relatives au traitement entrant dans le champ d'application du RGPD.

Il n'est pas nécessaire qu'un représentant RGPD soit désigné par une autorité publique ou une organisation qui effectue un traitement occasionnel, non à grande échelle, de catégories particulières de données ou de données relatives à des condamnations pénales et à des infractions qui ne sont « *peu susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques* ». Les lignes directrices 3/2018 du CEPD relatives au champ d'application territorial du RGPD indiquent que le terme « *organisme public* » doit être interprété conformément au droit national, et que des recommandations supplémentaires concernant le traitement « *à grande échelle* » et « *occasionnel* » peuvent être trouvées dans ses Lignes Directrices DPO et sa prise de position sur l'Article 30 du RGPD, respectivement.

Bird & Bird aide désormais les organisations établies en dehors de l'UE à remplir cette obligation et peut être désigné comme représentant RGPD.

N'hésitez pas à contacter Bird & Bird Privacy Solutions si vous souhaitez obtenir de plus amples informations sur nos services de représentation RGPD.

Recours à des prestataires de services (sous-traitants)

L'Article 28 du RGPD impose aux responsables du traitement un devoir de diligence élevé dans la sélection de leurs prestataires de services de traitement des données à caractère personnel, ce qui nécessitera une évaluation régulière des procédures de passation de marchés et des documents d'appel d'offres.

Des contrats doivent être mis en œuvre avec les prestataires de services, comportant une série d'informations (par exemple, les données traitées et la durée du traitement) et d'obligations (par exemple, l'assistance en cas de violation de données à caractère personnel, les mesures techniques et organisationnelles appropriées prises et les obligations d'assistance en matière d'audit, pour n'en citer que quelques-unes). Ces obligations doivent également être répercutées lorsqu'un prestataire de services fait appel à un sous-traitant de second rang.

Le 4 juin 2021, la Commission européenne a publié un ensemble de clauses contractuelles types entre responsables du traitement et sous-traitants (« *CCT Article 28* ») afin de couvrir les exigences énoncées à l'Article 28 du RGPD. Il ne s'agit pas de clauses obligatoires, mais d'une option que les organisations peuvent utiliser en annexe des accords commerciaux pour se conformer aux exigences de l'Article 28. Les CCT Article 28 ne doivent pas être confondues avec les clauses contractuelles types examinées ci-dessous en relation avec les transferts internationaux de données.

Registre des activités de traitement

Les organisations sont tenues de tenir un registre de leurs activités de traitement (le type de données traitées, les finalités pour lesquelles elles sont utilisées, etc.)

Les sous-traitants sont également tenus de tenir un registre des données à caractère personnel que les responsables du traitement leur demandent de traiter, ce qui est particulièrement difficile pour de nombreux fournisseurs de services d'informatique dématérialisée et de communication.

Si une dérogation aux obligations susmentionnées s'applique aux organisations employant moins de 250 personnes, cette dérogation ne s'applique pas lorsque des données relatives à des condamnations pénales et à des infractions sont traitées, ainsi que lorsque des catégories particulières de données sont traitées, ce qui semble susceptible de réduire à néant son utilité, en particulier dans le contexte de l'emploi.

Où puis-je trouver ces dispositions ?

Protection de la vie privée dès la conception, article 25, considérants 74-78

AIPD, articles 35-36, considérants 89-94

DPD, articles 37-39, considérant 97, WP 243

Recours à des sous-traitants, articles 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 les sous-traitants sont soumis à un régime général de notification des violations de données à caractère personnel.

Les sous-traitants doivent signaler les violations de données à caractère personnel aux responsables du traitement.

Les responsables du traitement doivent signaler les violations de données à caractère personnel à l'autorité de contrôle compétente et, dans certains cas, aux personnes concernées, en se conformant dans chaque cas aux dispositions spécifiques du RGPD.

Les responsables du traitement doivent tenir un registre interne des violations.

Le non-respect de cette obligation peut entraîner une amende administrative pouvant aller jusqu'à 10 000 000 € ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

En l'état actuel des choses, le régime spécifique de notification des violations pour les fournisseurs de services de communication, énoncé dans le règlement 611/2013 de la Commission concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE sur la vie privée et les communications électroniques, s'applique toujours (et fait partie des lois retenues au Royaume-Uni).

À faire

Conformément au principe de responsabilité établi par le RGPD, les responsables du traitement et les sous-traitants doivent s'assurer qu'ils ont mis en place des procédures internes de notification des violations, y compris des systèmes d'identification des incidents et des plans d'intervention en cas d'incident.

Ces procédures doivent être régulièrement testées et réexaminées.

Travaillez avec vos équipes IT/IS pour vous assurer qu'elles mettent en œuvre les mesures techniques et organisationnelles appropriées pour rendre les données inintelligibles en cas d'accès non autorisé.

Les polices d'assurance doivent être réexaminées régulièrement afin d'évaluer l'étendue de leur couverture en cas de violation.

Les modèles de contrats de souscription/clauses de protection des données et les documents d'appel d'offres doivent : (i) exiger des fournisseurs qu'ils leur notifient proactivement les violations ; et (ii) mettre l'accent sur le devoir de coopération entre les parties.

Incidents déclenchant une notification

Le RGPD définit une violation de données à caractère personnel 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 28 mars 2023, le CEPD a également adopté les lignes directrices 9/2022 sur la notification de violation de données à caractère personnel en vertu du RGPD (*Guidelines 9/2022 on personal data breach notification under GDPR* – disponibles uniquement en anglais ici), qui fournissent des recommandations supplémentaires sur les notifications (« *Lignes Directrices Notification des Violations* »). Le régime de notification des violations prévu par le RGPD s'applique comme suit :

1. Obligation pour les sous-traitants de notifier les responsables du traitement des données

Calendrier :

Dans les meilleurs délais après en avoir pris connaissance.

Exemption :

Aucune.

Observations :

- Toutes les violations doivent être signalées par le sous-traitant au responsable du traitement. Lorsque plusieurs responsables du traitement sont concernés par la violation commise par le sous-traitant, ce dernier doit notifier chaque responsable du traitement concerné.

- Les Lignes Directrices Notification des Violations recommandent que le contrat entre le responsable du traitement et le sous-traitant fixe des délais, qui peuvent inclure des exigences de notification précoce par le sous-traitant.

- Le CEPD recommande une notification graduelle afin d'aider le responsable du traitement à respecter l'obligation de notifier l'autorité de contrôle dans les 72 heures.

- Le CEPD reconnaît également que, bien que la responsabilité légale de la notification incombe au responsable du traitement, un sous-traitant peut effectuer une notification pour le compte du responsable du traitement lorsque ce dernier a autorisé le sous-traitant à le faire dans le cadre des dispositions contractuelles entre les parties.

2. Obligation pour les responsables du traitement de notifier l'autorité de contrôle

Calendrier :

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

Exemption :

Pas de déclaration si la violation n'est pas susceptible d'entraîner un risque pour les droits et libertés des personnes physiques (par exemple, les données à caractère personnel sont déjà accessibles au public et leur divulgation ne constitue pas un risque probable pour l'individu).

Observations :

- Dans les Lignes Directrices Notification des Violation, le CEPD reconnaît que le moment précis où un responsable du traitement prend connaissance d'une violation dépend des circonstances de la violation en question. Toutefois, le CEPD précise qu'un responsable du traitement doit être considéré comme ayant pris connaissance de la violation lorsqu'il a un degré raisonnable de certitude qu'un incident s'est produit qui a conduit à la compromission des données à caractère personnel. Le CEPD va plus loin en déclarant que les mesures techniques et organisationnelles du responsable du traitement doivent lui permettre d'établir immédiatement si une violation a eu lieu.

- De l'avis du CEPD, la période de 72 heures devrait être mise à profit par le responsable du traitement pour évaluer le risque probable pour les personnes afin de déterminer si l'obligation de notification a été déclenchée, ainsi que la ou les mesures à prendre pour remédier à la violation, y compris la transmission au niveau hiérarchique approprié. Ces évaluations peuvent être influencées par les AIPD précédemment menées par le responsable du traitement.

- Le RGPD prévoit la possibilité d'une notification graduelle dans le cas où le responsable du traitement n'est pas en

mesure de fournir toutes les informations requises à l'autorité de contrôle. Toutefois, lorsque l'obligation de notifier dans le délai prescrit n'est pas respectée, des raisons devront être fournies à l'autorité de contrôle (par exemple, une demande émanant d'une autorité répressive ou plusieurs violations de données sur une courte période).

- Dans les Lignes Directrices Notification des Violations, le CEPD reconnaît la possibilité pour un responsable du traitement de soumettre une notification groupée lorsque le même événement donne lieu à des violations similaires, mais multiples. Toutefois, lorsqu'une série de violations concerne différents types de données à caractère personnel, violées de différentes manières, chaque violation doit être notifiée séparément.

3. Obligation pour le responsable du traitement de communiquer sur une violation de données à caractère personnel aux personnes concernées

Le responsable du traitement doit communiquer sur une violation de données à caractère personnel aux personnes concernées uniquement lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

Si le responsable du traitement ne l'a pas encore fait, l'autorité de contrôle peut obliger le responsable du traitement à communiquer une violation de données à caractère personnel aux personnes concernées, sauf si l'une des exemptions est satisfaite.

Calendrier :

Dans les meilleurs délais : la nécessité d'atténuer un risque immédiat de dommage exigerait une communication rapide avec les personnes concernées, tandis que la nécessité de mettre en œuvre des mesures appropriées contre des violations de données répétées ou similaires pourrait justifier un délai plus long pour la communication. Le CEPD reconnaît que, dans des circonstances exceptionnelles, la communication aux personnes concernées peut précéder la notification à l'autorité de contrôle, par exemple en cas de menace immédiate d'usurpation d'identité ou lorsque des catégories particulières de données sont divulguées en ligne.

Pas de communication si :

- la violation n'est pas susceptible d'entraîner un risque élevé pour les droits et libertés des personnes concernées ;

- une protection technique et organisationnelle appropriée était en place au moment de l'incident pour rendre les données à caractère personnel inintelligibles (par exemple, des données chiffrées, lorsque la clé de chiffrement est toujours intacte et que les données compromises sont toujours disponibles de manière générale) ;

- immédiatement après la violation de données à caractère personnel, le responsable du traitement a pris des mesures pour s'assurer que le risque élevé pour les droits et libertés des personnes n'est plus susceptible de se matérialiser ; ou

- cela entraînerait des efforts disproportionnés (il faudrait plutôt compter sur une campagne d'information publique ou sur des « *mesure[s] similaire[s]* » pour que les personnes concernées puissent être effectivement informées).

Violations transfrontalières de données à caractère personnel

Lorsqu'une violation de données à caractère personnel affecte des personnes concernées dans plus d'un État membre, le responsable du traitement des données doit notifier, s'il a un établissement unique ou principal, son autorité de contrôle chef de file compétente (voir la section sur la coopération et la cohérence entre les autorités de contrôle). Cette autorité n'est pas nécessairement celle où se trouvent les personnes concernées ou celle où la violation a eu lieu. Lors de la notification à l'autorité chef de file, le responsable du traitement doit indiquer si la violation affecte des personnes concernées dans d'autres États membres.

Lorsqu'une organisation établie en dehors de l'UE est soumise au RGPD et subit une violation de données à caractère personnel, le CEPD recommande que la notification soit faite à chaque autorité de contrôle dans l'État membre où résident les personnes concernées. Les Lignes Directrices Notification des Violations précisent que la simple présence d'un représentant dans un État membre ne déclenche pas le mécanisme de guichet unique.

Exigences en matière de documentation

Registre interne des violations : obligation pour le responsable du traitement de documenter chaque incident « *en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier* ». Il est également conseillé de disposer d'un plan interne d'intervention en cas de violation de données à caractère personnel, qui expose clairement la manière dont ces violations et les notifications qui s'ensuivent sont traitées. L'autorité de contrôle peut être invitée à évaluer la manière dont les responsables du traitement se conforment à leurs obligations en matière de notification des violations de données.

La communication à l'autorité de contrôle doit également satisfaire à certaines exigences (par exemple, décrire la nature de la violation de données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation), de même que la communication aux personnes concernées (par exemple, décrire dans un langage clair et simple la nature de la violation de données à caractère personnel et fournir au moins les informations suivantes : i) le nom et les coordonnées du DPO ou d'un autre point de contact où de plus amples informations peuvent être obtenues ; ii) les conséquences probables de la violation de données à caractère personnel ; et iii) les mesures prises ou proposées par le responsable du traitement pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, pour en atténuer les effets néfastes éventuels). De nombreuses autorités de contrôle ont élaboré des formulaires types pour la notification des violations de données à caractère personnel.

Sanctions en cas de non-conformité

Le non-respect des exigences susmentionnées expose l'organisation à une amende administrative pouvant aller jusqu'à 10 000 000 euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

En outre, certains États membres ajoutent des sanctions pénales au niveau national en cas de non-respect de la législation (par exemple, la France).

Qu'en est-il des autres régimes européens de notification des violations ?

En l'état actuel des choses, le règlement 611/2013 - qui détaille une procédure spécifique pour la notification des violations (prévue par la directive 2002/58/CE (la « *directive vie privée et communications électroniques* ») telle que modifiée) - s'applique toujours aux fournisseurs de services de télécommunications accessibles au public (par exemple, les entreprises de télécommunications, les fournisseurs de services internet et les fournisseurs de services de communications électroniques).

Au moment où nous écrivons ces lignes, sept ans après que la Commission européenne a publié sa proposition de texte pour le nouveau règlement sur la vie privée et les communications électroniques le 10 janvier 2017, un projet final de règlement sur la vie privée et les communications électroniques n'a pas encore été approuvé par les législateurs européens.

Pour le Royaume-Uni, les exigences de fond du règlement 611/2013 sont maintenues dans le droit britannique nonobstant la sortie du Royaume-Uni de l'UE – avec toutefois quelques ajustements opportuns (par exemple, le remplacement des références à l'autorité de contrôle compétente par des références à l'ICO ou au secrétaire d'État concerné) (Electronic Communications (Amendment etc) (EU exit) Règlement 2019/919.

En outre, les exigences en matière de notification des violations prévues par les lois sur la cybersécurité, y compris en particulier par la nouvelle directive (UE) 2022/2555 (la « *Directive NIS2* »), devront être prises en compte. La Directive NIS2 remplacera la Directive NIS à partir du 18 octobre 2024, modifiant les règles relatives à la sécurité des réseaux et des systèmes d'information dans 18 secteurs (voir notre tracker de mise en œuvre de la directive NIS2 (disponible en anglais uniquement)). Une fois mises en œuvre localement par les États membres de l'UE, les nouvelles exigences renforcées en matière de cybersécurité et de déclaration s'appliqueront à un large éventail d'entreprises (y compris, les fournisseurs de services d'informatique en nuage, les centres de données et les places de marché en ligne) qui atteignent certains seuils et fournissent leurs services ou exercent leurs activités au sein de l'UE.

Si la Directive NIS2, en conjonction avec sa mise en œuvre locale, s'applique à une organisation, en fonction des circonstances propres à un incident, cette organisation devra également notifier les autorités de cybersécurité et les destinataires de ses services. En pratique, cela signifie que, pour se préparer à la notification d'un incident, les organisations entrant dans le champ d'application de ce texte législatif majeur devront :

- revoir les processus et procédures actuels afin d'évaluer les changements à apporter pour s'aligner sur les exigences de la Directive NIS2 ; et

- mettre à jour leurs plans et processus de réponse aux incidents, y compris ceux visant à se conformer au RGPD et à d'autres législations.

Où puis-je trouver ces dispositions ?

Considérants 85-88, articles 33, 34, 70, 83 et 84

Codes de conduite et certification

En bref

Le RGPD contient des dispositions relatives à la validation des codes de conduite (« *Codes* ») et à la mise en place de mécanismes de certifications, marques et labels afin d'aider les responsables du traitement et les sous-traitants à démontrer qu'ils respectent les règles et les meilleures pratiques.

Codes de conduite :

- Les associations et les organismes représentatifs peuvent préparer des Codes pour validation, enregistrement et publication par une autorité de contrôle ou, lorsque les activités de traitement se déroulent dans plusieurs États membres, par le CEPD. La Commission européenne peut déclarer que les codes recommandés par le CEPD ont une validité générale au sein de l'UE.
- Les Codes peuvent être approuvés pour un large éventail de sujets et le respect des Codes aidera les responsables du traitement et les sous-traitants à démontrer qu'ils se conforment aux obligations du RGPD.
- Le respect des Codes fera l'objet d'un contrôle, qui pourra être effectué par des organismes dûment qualifiés et accrédités. Les responsables du traitement et les sous-traitants qui ont enfreint un Code pertinent peuvent être suspendus de leur participation au Code et signalés à l'autorité de contrôle.

Certifications, marques et labels :

- La mise en place de mécanismes de certification de la protection des données ainsi que des marques et de labels doit être encouragée.
- Les certificats seront délivrés par des organismes de certification accrédités.
- La certification est volontaire, mais elle permettra aux responsables du traitement et aux sous-traitants de prouver qu'ils respectent le RGPD.
- Les certificats seront valables trois ans et pourront être renouvelés.
- Le CEPD tiendra un registre accessible au public de tous les mécanismes de certification, marques et labels.

À faire

Les organisations devraient suivre les tendances et se demander si elles souhaitent déposer une demande de certification ou se conformer à un Code qui a été approuvé et publié par le CEPD.

Une fois les mécanismes de certification établis, les responsables du traitement devraient se familiariser avec les mécanismes pertinents et tenir compte des certifications, des marques et des labels lors de la sélection de leurs sous-traitants/prestataires de services.

Codes de conduite

Bien qu'ils ne constituent pas encore un aspect important du régime de protection des données dans l'UE, les Codes devraient, lorsqu'ils auront pris de l'ampleur, remplir un rôle important dans l'élargissement et l'adaptation des outils de conformité à la protection des données auxquels les responsables du traitement et les sous-traitants peuvent faire appel, par le biais d'un mécanisme de « *semi-auto-régulé* ».

Il est prévu que les Codes fournissent des lignes directrices faisant autorité dans certains domaines clés, notamment

- intérêt légitime dans des contextes spécifiques ;
- la pseudonymisation ;
- l'exercice des droits des personnes concernées ;
- la protection des mineurs et les modalités du consentement parental ;
- la mise en œuvre adéquate de la protection de la vie privée dès la conception et par défaut, ainsi que des mesures de sécurité ;
- la notification des violations de données à caractère personnel ; et
- le règlement des litiges entre les responsables du traitement et les personnes concernées.

L'élaboration et l'approbation des Codes sont susceptibles d'apporter un certain nombre d'avantages, notamment :

- l'établissement et la mise à jour des meilleures pratiques en matière de conformité dans des contextes de traitement spécifiques ;
- permettre aux responsables du traitement et aux sous-traitants de s'engager à respecter des normes et des pratiques reconnues et d'être reconnus pour cela ;
- l'adhésion aux Codes peut démontrer que les importateurs de données (responsables du traitement et sous-traitants) situés en dehors de l'UE/EEE ont mis en œuvre des garanties adéquates afin d'autoriser les transferts au titre de l'Article 46 ; les transferts effectués sur la base d'un Code approuvé et d'engagements contraignants et exécutoires de l'importateur d'appliquer des garanties appropriées peuvent avoir lieu sans autorisation spécifique d'une autorité de contrôle ; les Codes peuvent donc constituer un mécanisme alternatif de gestion des transferts internationaux, au même titre que les clauses contractuelles types et les BCR.

Approbation des Codes

Les Codes proposés par des associations ou des organismes représentatifs en rapport avec des activités de traitement de données qui n'affectent qu'un seul État membre doivent être soumis à l'autorité de contrôle compétente pour commentaires et - sous réserve d'éventuelles modifications ou extensions - approbation. Certaines autorités de contrôle prennent des mesures pour mettre en œuvre ces Codes. Par exemple, l'autorité de contrôle française (la CNIL) a approuvé un Code relatif aux fournisseurs d'infrastructures cloud et a indiqué que d'autres Codes sectoriels spécifiques, tels que ceux relatifs à la recherche médicale, sont en cours de préparation.

Si un Code couvre des opérations de traitement dans plusieurs États membres, il doit être soumis au CEPD pour avis. Sous réserve d'éventuelles modifications ou extensions, le Code et l'avis du CEPD peuvent ensuite être soumis à la Commission européenne qui, après un examen approfondi, peut déclarer sa validité générale. Les Codes doivent être conservés et mis à disposition dans des registres accessibles au public.

Contrôle de la conformité

Le contrôle du respect des Codes sera effectué uniquement par des organismes accrédités par l'autorité de contrôle compétente.

Pour obtenir l'accréditation, ces organismes devront démontrer :

- leur indépendance et leur expertise ;
- qu'ils ont mis en place des procédures pour évaluer la capacité des responsables du traitement et des sous-traitants à appliquer le Code et pour en contrôler le respect, ainsi que pour réviser périodiquement le Code ;
- leur capacité à traiter les plaintes relatives aux infractions ; et
- qu'ils ont mis en place des procédures pour éviter les conflits d'intérêts.

Les accréditations sont révocables si les conditions d'accréditation ne sont plus remplies.

En juin 2019, le CEPD a adopté les lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de suivi au titre du règlement (UE) 2016/679. Ces lignes directrices définissent les critères d'évaluation des codes et les modalités de leur approbation.

Certifications, marques et labels

Le concept de certification des opérations de traitement des données est un développement important dans la création d'un cadre fiable et contrôlable pour les opérations de traitement des données. Il devrait être particulièrement pertinent dans le contexte de l'informatique en nuage et d'autres formes de services à multiples facettes, où les audits individuels ne sont souvent pas réalisables dans la pratique.

Les États membres, les autorités de contrôle, le CEPD et la Commission sont tous encouragés à mettre en place des mécanismes de certification de la protection des données, des marques et des labels, en ce qui concerne des opérations de traitement spécifiques.

L'autorité de contrôle compétente ou le CEPD approuvera les critères de certification. Le CEPD peut élaborer des critères pour une certification commune, le label européen de protection des données.

En 2018, le CEPD a publié les lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux Articles 42 et 43 du règlement.

Les certifications présentent deux avantages majeurs :

- les responsables du traitement et les sous-traitants seront en mesure de démontrer leur conformité, notamment en ce qui concerne la mise en œuvre de mesures techniques et organisationnelles.

- Les certifications peuvent démontrer que les importateurs de données (responsables du traitement et sous-traitants) situés en dehors de l'UE/EEE ont mis en œuvre des garanties adéquates aux fins de l'Article 46 ; les transferts effectués sur la base d'un mécanisme de certification approuvé et d'engagements contraignants et exécutoires de l'importateur d'appliquer des garanties appropriées peuvent avoir lieu sans autorisation spécifique d'une autorité de contrôle ; les certificats offrent donc un mécanisme alternatif de gestion des transferts internationaux, au même titre que les clauses contractuelles types et les BCR.

Les certifications relatives aux opérations de transformation seront délivrés pour une période de trois ans et pourront être renouvelées ou retirées si les conditions de délivrance de la certification ne sont plus remplies.

Le CEPD doit tenir un registre public de tous les mécanismes de certification, marques et labels en matière de protection des données. Les certificats peuvent être délivrés par des organismes de certification accrédités - privés ou publics. Les organismes nationaux d'accréditation et/ou les autorités de contrôle peuvent accréditer des organismes de certification (afin qu'ils puissent délivrer les certifications, marques labels), qui (entre autres) :

- possèdent l'expertise requise et sont indépendants par rapport à l'objet de la certification ;
- disposent de procédures d'examen périodique et de retrait des certifications, des marques et des labels ;
- sont en mesure de traiter les plaintes concernant les violations des certifications ; et
- disposent de règles pour gérer les conflits d'intérêts.

Les critères d'agrément seront élaborés par les autorités de contrôle ou le CEPD et seront rendus publics.

Les agréments des organismes de certification seront délivrés pour une durée maximale de cinq ans et pourront être renouvelées ou retirées si les conditions d'agrément ne sont plus remplies.

Le CEPD a également publié les lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'Article 43 du règlement général sur la protection des données (2016/679). Ces lignes directrices s'adressent principalement aux États membres, aux autorités de contrôle et aux organismes nationaux d'accréditation et ne concernent pas directement les responsables du traitement et les sous-traitant

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 et 43

Considérants 77, 81, 100, 166 et 168

Transferts de données à caractère personnel

En Bref

Les transferts de données à caractère personnel à des destinataires situés dans des « *pays tiers* » (c'est-à-dire en dehors de l'Espace économique européen (« *EEE* »)) sont limités.

Les obligations du RGPD sont largement similaires à celles imposées par la directive sur la protection des données, avec quelques améliorations du mécanisme de conformité, notamment la suppression de la nécessité de notifier les clauses contractuelles types aux autorités de contrôle, et l'encouragement au développement de codes de pratique et de systèmes de certification sur l'adéquation des transferts.

La conformité des transferts de données reste une question importante pour les organisations multinationales et pour toute personne utilisant des chaînes d'approvisionnement qui traitent des données à caractère personnel en dehors de l'EEE.

La violation des dispositions du RGPD relatives au transfert de données fait partie des cas de non-conformité pour lesquels le niveau maximal d'amende peut être imposé (jusqu'à 4 % du chiffre d'affaires annuel mondial).

Des procédures de non-conformité peuvent être engagées à l'encontre des responsables du traitement et/ou des sous-traitants.

À faire

Identifiez tous les transferts de données à caractère personnel ; procédez à des évaluations des risques de transfert et assurez le suivi de ces évaluations ; mettez en œuvre des mesures de protection.

Examinez les questions incluses dans les contrats standards de fourniture de services et de clauses contractuelles pour vous assurer que les informations sur le transfert de données à caractère personnel proposé par votre fournisseur et dont vous êtes responsable sont incluses.

Examinez les transferts de données de l'EEE vers le Royaume-Uni ; ces transferts devront être mentionnés dans les registres des activités de traitement (et éventuellement dans les politiques de confidentialité).

Si vous transférez des données à caractère personnel en dehors de l'EEE dans le cadre de la fourniture de biens ou de services, attendez-vous à ce que vos clients vous posent des questions sur votre approche (et celle de votre fournisseur) en matière de conformité.

Commentaire

Les transferts de données à caractère personnel vers des « *pays tiers* » (c'est-à-dire en dehors de l'EEE) sont limités.

Le CEPD a publié les lignes directrices 05/2021 sur l'interaction entre l'application de l'Article 3 et des dispositions relatives aux transferts internationaux du chapitre V du RGPD. Ces lignes directrices notent que le RGPD ne définit pas ce qu'est un « *transfert* ». Les lignes directrices proposent trois critères cumulatifs : (i) l'exportateur de données (un responsable du traitement ou un sous-traitant) est soumis au RGPD pour le traitement donné ; (ii) l'exportateur de données transmet ou met à disposition les données à caractère personnel à l'importateur de données (une personne morale distincte qui est un responsable du traitement, un responsable conjoint du traitement ou un sous-traitant) ; et (iii) l'importateur de données se trouve dans un pays tiers ou est une organisation internationale. Un point souligné dans les lignes directrices est que les responsables du traitement et les sous-traitants qui sont soumis au RGPD sur une base extraterritoriale (en vertu de l'Article 3 (2)) devront se conformer au chapitre V lorsqu'ils transfèrent des données à caractère personnel à un pays tiers ou à une organisation internationale.

La Commission européenne a le pouvoir de déterminer que certains pays, territoires, secteurs spécifiques ou organisations internationales offrent un niveau de protection adéquat pour les transferts de données. La liste des pays approuvés par la Commission européenne est la suivante : Andorre, Argentine, Canada (où la législation *PIPEDA* s'applique), États-Unis d'Amérique (organisations commerciales participant au *Cadre de la protection des données UE - États-Unis* (en anglais, « Data Privacy Framework »)), Guernesey, Îles Féroé, Israël, Île de Man, Japon, Jersey, République de Corée, Royaume-Uni, Nouvelle-Zélande, Uruguay et Suisse. Les pays qui seront ajoutés ou retirés de cette liste seront publiés au Journal officiel. Il convient toutefois de noter que les données transférées de l'EEE au Royaume-Uni aux fins du contrôle de l'immigration britannique ne sont pas incluses dans la décision d'adéquation.

Le RGPD fournit plus de détails sur les procédures et les critères particuliers que la Commission européenne doit prendre en compte pour déterminer le caractère adéquat, en soulignant la nécessité de s'assurer que le pays tiers offre un niveau de protection « *essentiellement équivalent à celui qui est garanti dans l'Union* », et qu'il fournit aux personnes concernées des droits et des moyens de recours effectifs et exécutoires. La Commission européenne consulte le CEPD lors de l'évaluation des niveaux de protection et veille à ce qu'il y ait un suivi et un examen continus de toute décision d'adéquation prise (au moins tous les quatre ans). La Commission européenne a également le pouvoir d'abroger, de modifier ou de suspendre toute décision d'adéquation. Le CEPD a publié en novembre 2017 les lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel.

Autres méthodes de transfert de données à caractère personnel : les clauses contractuelles types (« CCT ») (adoptées par la Commission ou adoptées par une autorité de contrôle et approuvées par la Commission européenne), les règles d'entreprise contraignantes (« BCR ») et les instruments juridiquement contraignants et exécutoires entre les autorités publiques sont également acceptés.

Il est important de noter que les transferts sont également autorisés en cas d'utilisation d'un code de conduite approuvé (fondé sur le système de l'Article 40) ou d'un mécanisme de certification approuvé (fondé sur le système de l'Article 42), à condition que le responsable du traitement ou le sous-traitant dans le pays tiers s'engage de manière contraignante et exécutoire à appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées. Il existe également des dispositions permettant de convenir de garanties ad hoc, sous réserve de l'autorisation de l'autorité de contrôle compétente.

Le CEPD a publié des lignes directrices 1/2019 relatives aux codes de conduite et organismes de suivi au titre du règlement (UE) 2016/679, ainsi que des lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'Article 43 du règlement général sur la protection des données (2016/679).

Les dérogations (conformément à l'Article 49 du RGPD) autorisent les transferts de données à caractère personnel dans des circonstances limitées, notamment : le consentement explicite, la nécessité contractuelle, les raisons importantes d'intérêt public, les demandes légales, les intérêts vitaux et les données des registres publics. Il existe également une dérogation (limitée) pour les transferts non répétitifs impliquant un nombre limité de personnes concernées, lorsque le transfert est nécessaire pour des intérêts

légitimes impérieux des responsables du traitement (qui ne sont pas supplantés par les intérêts ou les droits de la personne concernée) et lorsque le responsable du traitement a évalué (et documenté) toutes les circonstances entourant le transfert de données et a conclu qu'elles étaient adéquates. Le responsable du traitement doit informer l'autorité de contrôle et les personnes concernées lorsqu'il se prévaut de cette dérogation. Le CEPD a publié des lignes directrices relatives aux dérogations prévues à l'Article 49 du règlement UE 2016/679. Il a souligné que cette dérogation relative à l'intérêt légitime impérieux est « *envisagée par le droit comme un dernier ressort* ».

Enfin, le RGPD précise qu'il n'est pas licite de transférer des 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 ne soit fondée sur un accord international ou que l'un des autres motifs de transfert ne s'applique. Le Royaume-Uni a choisi de ne pas appliquer cette disposition.

Pour en savoir plus :

- Lignes directrices du CEPD 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679
- Lignes directrices du CEPD 05/2021 sur l'interaction entre l'application de l'article 3 et des dispositions relatives aux transferts internationaux du chapitre V du RGPD
- Recommandations du CEPD 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE
- Commissaire à la protection des données contre Facebook Ireland Limited et Maximillian Schrems (Schrems II)

Où puis-je trouver ces dispositions ?

Articles 44 à 50, considérants 101 à 116

Désignation des autorités de contrôle

En bref

Les autorités de contrôle sont établies dans chaque État membre et sont chargées de surveiller l'application du RGPD.

Elles doivent coopérer entre elles et avec la Commission européenne, et contribuer à l'application cohérente du RGPD dans l'ensemble de l'UE.

Elles doivent agir en toute indépendance.

Les membres des autorités de contrôle doivent être nommés de manière publique et transparente et posséder des compétences en matière de protection des données.

Il peut y avoir plus d'une autorité de contrôle dans un pays (par exemple, lorsque le pays est composé d'États fédéraux).

À faire

Aucune action n'est requise, mais il est judicieux d'établir ou de maintenir un point de contact avec votre autorité de contrôle principale.

Commentaire

Les autorités de contrôle (appelées familièrement « *autorités de protection des données* » ou « *APD* ») sont établies dans chaque État membre. Elles contrôlent l'application du RGPD afin de protéger les droits fondamentaux en matière de traitement et de faciliter la libre circulation des données à caractère personnel au sein de l'UE.

Elles doivent coopérer entre elles et avec la Commission européenne afin de contribuer à l'application cohérente du RGPD.

Les États comme l'Allemagne peuvent avoir (et ont) plus d'une autorité de contrôle, mais l'une d'entre elles est désignée comme représentant national au sein du CEPD.

Les autorités de contrôle doivent agir en toute indépendance (sous réserve de l'audit financier et du contrôle judiciaire). Les membres des autorités de contrôle restent à l'abri de toute influence extérieure et ne doivent ni solliciter ni accepter d'instructions de quiconque. Ils ne doivent pas non plus agir de manière incompatible avec leurs fonctions ni, pendant la durée de leur mandat, exercer une activité professionnelle incompatible, qu'elle soit rémunérée ou non.

Les États membres doivent fournir à leurs autorités de contrôle les ressources humaines, techniques, financières et autres nécessaires à l'accomplissement de toutes leurs tâches et à l'exercice effectif de leurs pouvoirs.

Chaque autorité de contrôle choisit son propre personnel et en assure seule la direction. Le budget d'une autorité de contrôle doit être public et identifié séparément, même s'il fait partie du budget national.

La législation de l'État membre doit établir une autorité de contrôle, prescrire les règles applicables aux membres de l'autorité, leurs qualifications et leur éligibilité. Le mandat (renouvelable) des membres d'une autorité de contrôle ne doit pas être inférieur à quatre ans. Les obligations d'indépendance des membres, décrites ci-dessus, doivent être inscrites dans le droit national. Les membres des autorités de contrôle et leur personnel sont tenus au « *secret professionnel* », tant pendant leur mandat que par la suite.

Les dispositions relatives à la création des autorités de contrôle sont assez détaillées - certains points méritent d'être soulignés : la spécificité du mandat, l'accent mis sur l'indépendance, l'insistance sur la mise à disposition de ressources adéquates pour chaque autorité de contrôle, et l'exigence que « *chaque membre [d'une autorités 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* ».

Nouvelle législation européenne sur les données

Le règlement sur les données prévoit que, lorsque ses dispositions concernent le traitement de données à caractère personnel, les autorités chargées de la protection des données seront compétentes pour ce traitement et pourront exercer les pouvoirs prévus par le règlement sur les données, ainsi que ceux prévus par le RGPD.

Où puis-je trouver ces dispositions ?

Considérants 117-123, chapitre VI, section 1, Articles 51 à 54

Compétences, missions et pouvoirs

En bref

Les autorités de contrôle disposent de compétences spécifiques pour agir sur leur propre territoire.

L'autorité chef de file (lorsqu'elle existe) est compétente pour les affaires transfrontalières (voir la section sur la coopération et cohérence entre les autorités de contrôle pour plus de détails).

Les autorités de contrôle disposent d'une liste étendue de pouvoirs et de tâches spécifiques.

À faire

Si vous effectuez des traitements transfrontaliers, veillez à une bonne compréhension du système de l'autorité chef de file (voir la section sur la coopération et cohérence entre les autorités de contrôle). Identifiez l'autorité que vous pensez être votre autorité chef de file et préparez des mesures de conformité en conséquence, par exemple des plans d'intervention en cas d'incident (voir sur la coopération et cohérence entre les autorités de contrôle).

Familiarisez-vous avec l'ensemble des pouvoirs et des missions des autorités de contrôle.

Compétence

Chaque autorité de contrôle est compétente *« pour exercer les missions et les pouvoirs »* tels que décrits dans le RGPD, sur son territoire national. Le considérant 122 nous indique que cette compétence comprend « *traitement affectant des personnes concernées sur le territoire de l'État 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'État membre dont elle relève* ».

Dans les cas où la base juridique du traitement, qu'il soit effectué par un organisme privé ou une autorité publique, est le respect d'une obligation légale, la mission d'intérêt public ou l'exercice de l'autorité publique, l'autorité de contrôle de l'État membre concerné est compétente et le système de l'autorité chef de file ne s'applique pas. La formulation est plutôt obscure, mais le considérant 128 indique qu'une autorité de contrôle détient une compétence exclusive sur le traitement effectué dans l'intérêt public à la fois par des autorités publiques et des organismes privés qui, dans les deux cas, sont établis sur le territoire de l'État membre de cette autorité de contrôle. Il n'est pas clair si cette disposition envisage des établissements multiples et constitue un moyen d'exclure le guichet unique ou si elle confère une compétence exclusive à l'autorité de contrôle du pays d'origine, et même si le traitement a lieu ailleurs dans l'UE. Cela pourrait s'appliquer largement aux organismes du secteur privé, par exemple aux institutions financières qui mènent des activités de lutte contre le blanchiment d'argent à l'égard de clients situés ailleurs dans l'UE que dans leur pays d'origine.

Les autorités de contrôle ne peuvent exercer leur compétence sur les juridictions agissant dans l'exercice de leur fonction juridictionnelle. Le terme « *juridiction* » n'est pas défini et il n'est pas clair jusqu'à quel niveau de la hiérarchie judiciaire cette règle s'appliquera.

Un système d'autorité chef de file est mis en place pour gérer le traitement transfrontalier (voir la section sur la coopération et la cohérence entre les autorités de contrôle pour plus d'informations sur ce dispositif complexe).

Dans l'affaire *Bundeskartellamt* (C-252/21), la CJUE a confirmé qu'une autorité de la concurrence d'un État membre pouvait également se prononcer sur le respect par une entreprise de la législation relative à la protection des données, lorsque cela était pertinent pour une question relevant du droit de la concurrence. L'autorité de concurrence aurait le devoir de coopérer loyalement avec les autorités de protection des données.

Missions

L'Article 57 du RGPD dresse une liste très complète des tâches confiées aux autorités de contrôle. Il n'est pas nécessaire de les énumérer toutes, car la dernière de la liste est « *s'acquitte de toute autre mission relative à la protection des données à caractère personnel* ». Les autorités de contrôle doivent donc faire tout ce qui peut raisonnablement être considéré comme relevant de la « *protection des données à caractère personnel* ».

Certaines missions méritent d'être soulignées. Les autorités de contrôle doivent faire respecter l'« *application* » du RGPD et sensibiliser le public, les responsables du traitement et les sous-traitants.

Elles doivent conseiller leurs gouvernements et leurs parlements sur les nouvelles lois proposées.

Elles doivent également aider les personnes concernées, traiter et enquêter sur les plaintes déposées par des personnes ou des organes représentatifs, mener des enquêtes et plus particulièrement coopérer avec les autres autorités de contrôle, de même que surveiller le développement des pratiques techniques et commerciales dans le domaine des technologies de l'information.

Les autorités de protection encouragent le développement de codes de conduite et de mécanismes de certification et « *procède à l'agrément* » des organismes de certification ainsi que des organisations chargées du suivi des codes de conduite.

Les autorités de contrôle ne peuvent pas facturer leurs services aux personnes concernées ou aux délégués à la protection des données/DPO ; le RGPD ne dit toutefois pas si les responsables du traitement et les sous-traitants peuvent se voir facturer des frais pour les services qu'ils reçoivent des autorités de contrôle.

Pouvoirs

L'Article 58 du RGPD énumère les pouvoirs des autorités de contrôle, que les États membres

peuvent compléter s'ils le souhaitent. De nombreux pouvoirs correspondent aux missions spécifiques énumérées à l'Article 57 et n'ont pas besoin d'être répétés.

Il convient de mentionner : l'injonction faite à un responsable du traitement ou à un sous-traitant de fournir des informations ; la réalisation d'audits ; l'accès aux locaux et aux données ; l'émission d'avertissements et de blâmes et l'imposition d'amendes ; l'injonction faite aux responsables du traitement et aux sous-traitants de se conformer au RGPD et aux droits des personnes concernées ; l'interdiction du traitement et des flux transfrontaliers de données en dehors de l'UE ; l'approbation de clauses contractuelles types et de règles d'entreprise contraignantes. L'exercice des pouvoirs par une autorité de contrôle doit être soumis à des garanties et pouvoir faire l'objet d'un recours juridictionnel.

Les États membres doivent donner aux autorités de contrôle le droit de saisir la justice 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* ».

Enfin, les autorités de contrôle doivent produire des rapports annuels. En résumé, les compétences, pouvoirs et missions des autorités de contrôle constituent une liste exhaustive de tout ce qu'une autorité de contrôle doit ou peut faire.

Où puis-je trouver ces dispositions ?

Considérants 117-123, WP 244, Chapitre VI Section 2 Articles 55-59

Coopération et cohérence entre les autorités de contrôle

En bref

En cas de traitement transfrontalier au sein de l'UE, les autorités de contrôle doivent coopérer afin de garantir une application cohérente du RGPD. Dans les cas prévus, il existe une autorité chef de file, qui sera l'autorité de contrôle de l'unique établissement de l'UE ou de l'établissement principal (« *guichet unique* ») du responsable du traitement. Les autorités de contrôle des autres pays dans lesquels un responsable du traitement est établi, ou dans lesquels les personnes concernées sont substantiellement affectées, ou les autorités auprès desquelles une plainte a été déposée, peuvent être impliquées dans les dossiers, et l'autorité chef de file doit coopérer avec elles.

À faire

Si vous êtes un responsable du traitement ou un sous-traitant basé en dehors de l'UE (et que vous tombez sous le coup des dispositions du RGPD), le système de l'autorité chef de file ne s'appliquera pas.

Si vous n'exercez vos activités que dans un seul État membre, l'autorité de contrôle de cet État membre sera l'autorité chef de file pour tout traitement transfrontalier.

Si vous exercez des activités dans deux États membres ou plus, vérifiez si vous remplissez les critères pour avoir une autorité chef de file (en tenant compte des recommandations du CEPD) et prenez contact avec cette autorité. Demandez-vous si les personnes chargées du respect de la protection des données dans votre organisation possèdent les compétences linguistiques nécessaires pour communiquer avec l'autorité chef de file.

Commentaire

Compétence de l'autorité chef de file

Si un responsable du traitement ou un sous-traitant effectue un « *traitement transfrontalier* » par l'intermédiaire de plusieurs établissements dans l'UE ou même d'un seul établissement (lorsque le traitement est susceptible d'affecter de manière substantielle des personnes dans plusieurs États membres), l'autorité de contrôle de l'établissement « *principal* » ou de l'établissement unique fait office d'autorité chef de file en ce qui concerne ce traitement transfrontalier.

Le CEPD a adopté les lignes directrices 8/2022 concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant. Lorsqu'une organisation possède plusieurs établissements, l'établissement principal et donc l'autorité chef de file sont déterminés par le lieu où se prennent les décisions concernant les finalités et les modalités du traitement des données à caractère personnel en question - bien qu'il puisse s'agir du lieu de l'administration centrale de l'organisation, si les décisions sont effectivement prises dans un autre établissement de l'UE, l'autorité de ce lieu sera l'autorité chef de file. Les lignes directrices précitées reconnaissent qu'il peut y avoir des situations où plus d'une autorité chef de file peut être identifiée pour différentes activités de traitement, par exemple lorsqu'une entreprise multinationale décide d'avoir des centres de prise de décision distincts, dans différents pays.

En ce qui concerne les responsables conjoints du traitement, les lignes directrices ont précisé qu'il n'est pas possible de désigner un établissement principal commun - et donc une autorité chef de file pour les deux responsables conjoints. Chaque responsable conjoint peut avoir son propre établissement principal, mais celui-ci ne peut pas être considéré comme l'établissement principal des responsables conjoints du traitement pour le traitement effectué sous leur responsabilité conjointe.

De même, les sous-traitants qui fournissent des services à plusieurs responsables du traitement ne bénéficient pas du guichet unique dans les cas impliquant leurs responsables, car l'autorité chef de file est l'autorité chef de file de chaque responsable.

Les lignes directrices précisent également que « *le RGPD n'autorise pas l'élection de juridiction ("forum shopping")* » - il doit y avoir un exercice effectif et réel de l'activité de gestion ou de la prise de décision sur le traitement dans l'établissement principal de l'organisation. Les organisations doivent être en mesure de démontrer aux autorités de contrôle où les décisions relatives au traitement des données sont réellement prises et mises en œuvre, car il peut leur être demandé de prouver leur position. Les lignes directrices précisent que les responsables du traitement qui n'ont pas d'établissement dans l'UE ne peuvent pas bénéficier du mécanisme de guichet unique (la simple présence d'un représentant de l'UE ne déclenche pas le mécanisme de guichet unique). Ils doivent ainsi traiter avec les autorités de contrôle locales dans chaque État membre où ils sont actifs, par l'intermédiaire de leur représentant local.

Par dérogation au guichet unique, une autorité nationale de contrôle reste compétente pour exercer ses pouvoirs si elle est saisie d'une plainte ou si une infraction se produit sur son territoire et si l'objet de la plainte ou de l'infraction ne concerne qu'un établissement situé sur ce territoire ou n'affecte substantiellement les personnes concernées que dans cet État. Les lignes directrices du CEPD contiennent des indications sur la signification de l'expression « *affecte sensiblement* ».

Ces cas « *locaux* » doivent être notifiés à l'autorité chef de file qui dispose de trois semaines pour décider d'intervenir ou non (en tenant compte de l'existence ou non d'un établissement dans l'autre État) conformément à la procédure de coopération. Si elle le fait, l'autorité non chef de file peut proposer une décision à l'autorité chef de file.

Si l'autorité chef de file n'intervient pas, l'autorité locale traite le dossier en utilisant, le cas échéant, les pouvoirs d'assistance mutuelle et d'enquête conjointe.

En janvier 2019, la CNIL a infligé à Google une amende de 50 millions d'euros pour des violations du RGPD qui comportaient un élément transfrontalier. Étant donné que les activités européennes de Google ont leur siège en Irlande (et que Google considérait l'autorité irlandaise comme son autorité chef de file), cette décision a donné un aperçu intéressant de la manière dont les autorités de contrôle interprètent les mécanismes de coopération et de cohérence. Selon la CNIL, étant donné que le responsable du traitement des données en question était Google LLC (et non Google France), Google Ireland Limited ne pouvait pas être considéré comme l'établissement principal de Google LLC, car il ne

pouvait pas avoir de pouvoir de décision réel et effectif sur les activités de traitement concernées au moment considéré. Par conséquent, en l'absence d'un établissement principal dans l'UE, Google LLC ne pouvait pas bénéficier du mécanisme de l'autorité chef de file et la CNIL a estimé qu'elle était compétente pour agir en vertu des Articles 55 et 58 du RGPD. La décision de la CNIL a été confirmée par la plus haute juridiction administrative française.

En juin 2021, la CJUE s'est prononcée sur une affaire qui lui avait été soumise par la Cour d'appel de Bruxelles, concernant une action en justice intentée par l'autorité belge à l'encontre de Facebook pour des infractions présumées au RGPD. La CJUE a jugé que, sous certaines conditions, une autorité de contrôle nationale peut porter toute violation alléguée du RGPD devant une juridiction de son État membre, conformément à l'Article 58(5) du RGPD, même si cette autorité n'est pas l'autorité chef de file. C'est en principe le cas lorsque l'autorité non chef de file est compétente pour adopter une décision constatant que le traitement est contraire au RGPD en vertu de l'Article 56 et qu'elle exerce ce pouvoir en tenant dûment compte du mécanisme de coopération et de cohérence du RGPD, alors qu'il n'est pas nécessaire que le responsable du traitement ait un établissement principal ou un autre établissement sur le territoire de l'État membre de l'autorité de contrôle en question. La Cour a également confirmé l'effet direct de l'Article 58(5) du RGPD, qui dispose que les États membres de l'UE doivent prévoir que les autorités de contrôle ont le pouvoir de porter les infractions au RGPD devant les autorités judiciaires et d'engager des procédures judiciaires le cas échéant. Cela signifie qu'une autorité de contrôle peut s'appuyer sur cette disposition, même si elle n'a pas été spécifiquement mise en œuvre dans la législation de l'État membre concerné.

Où puis-je trouver ces dispositions ?

Considérants 124-138 et chapitre VII, Sections 1 et 2

Procédure de coopération

L'autorité chef de file doit coopérer avec les autres autorités de contrôle « *concernées* ». Elles doivent échanger des informations et tenter de parvenir à un consensus. Une autorité de contrôle est « *concernée* » lorsque le responsable du traitement (ou le sous-traitant) dispose d'un établissement sur le territoire de l'État membre de cette autorité, lorsque les personnes concernées sur ce territoire sont (susceptibles d'être) substantiellement affectées par le traitement ou lorsqu'une plainte a été déposée auprès de cette autorité.

L'autorité chef de file doit fournir des informations aux autres autorités de contrôle concernées et peut leur demander une assistance mutuelle et mener des enquêtes conjointes avec elles sur leur territoire. L'autorité chef de file doit soumettre sans délai un projet de décision aux autorités concernées, qui disposent d'un délai de quatre semaines pour s'y opposer. Il peut y avoir un autre cycle de soumission de projets de décision avec une période d'objection de deux semaines. Si l'autorité chef de file ne souhaite pas suivre l'avis des autorités concernées, elle doit se soumettre à la procédure de cohérence supervisée par le CEPD.

Il existe des règles détaillées concernant l'autorité de contrôle qui doit adopter la décision formelle et la notifier au responsable du traitement, mais l'autorité chef de file a l'obligation de veiller à ce que, conformément à une décision formelle, des mesures de conformité soient prises par un responsable du traitement dans tous ses établissements. Une autorité de contrôle concernée peut toutefois, à titre exceptionnel, prendre des mesures temporaires urgentes sans attendre l'achèvement du processus de cohérence.

Le système de l'autorité chef de file présente un certain nombre de faiblesses apparentes et pourrait être mis à mal lorsque des autorités non chefs de file sont en mesure de s'affirmer au motif que les personnes concernées relevant de leur juridiction sont substantiellement affectées par un traitement effectué par un responsable du traitement dont l'établissement principal se trouve ailleurs.

Assistance mutuelle, opérations conjointes et cohérence

Les autorités de contrôle sont tenues de se prêter mutuellement assistance, notamment sous la forme d'informations ou en procédant à des « *autorisations et consultations préalables, inspections et enquêtes* ». La Commission européenne peut préciser les formes et les procédures d'assistance mutuelle.

Les autorités de contrôle peuvent mener des enquêtes et des opérations d'exécution conjointes. Une autorité de contrôle a le droit d'être incluse dans ces opérations si le responsable du traitement ou le sous-traitant a un établissement sur son territoire ou si un nombre important de ses personnes concernées sont susceptibles d'être affectées de manière substantielle.

Si la législation locale le permet, l'autorité de contrôle du pays d'accueil peut confier des pouvoirs d'enquête formels au personnel détaché. Les autorités de contrôle menaient des enquêtes conjointes avant le RGPD, de sorte qu'en pratique, le RGPD a développé et renforcé ces dispositions.

Lorsque les autorités de contrôle prennent certaines mesures formelles, sont en désaccord ou souhaitent que des mesures soient prises par une autre autorité de contrôle, le RGPD prévoit un mécanisme de cohérence et de résolution des litiges.

Le CEPD doit rendre des avis sur diverses propositions des autorités de contrôle, y compris l'approbation de règles d'entreprise contraignantes, de mécanismes de certification et de codes de conduite. Si une autorité de contrôle ne demande pas l'avis du CEPD ou ne suit pas un avis du CEPD, l'affaire est soumise à la procédure de résolution des litiges.

La procédure de résolution des litiges s'applique également aux litiges entre l'autorité chef de file et l'autorité concernée. Dans tous ces cas, le CEPD prend une décision contraignante sur la base d'un vote à la majorité des deux tiers. Si cette majorité n'est pas atteinte, une majorité simple suffit après un certain délai. Les autorités de contrôle concernées sont tenues de se conformer et des décisions formelles doivent être prises conformément à la décision du CEPD.

Les décisions contraignantes les plus notables du CEPD dans le cadre du mécanisme de coopération et de cohérence concernent l'autorité irlandaise (la « DPC ») dans les affaires concernant WhatsApp (juillet 2021 et décembre 2022) et les services Facebook et Instagram de Meta Platforms (juillet 2022 et décembre 2022). Suite à la décision contraignante du CEPD dans l'affaire WhatsApp de 2021, la DPC a dû modifier

son projet de décision concernant les violations des règles relatives à la transparence, le calcul de l'amende et le délai dans lequel WhatsApp devait mettre son traitement en conformité. WhatsApp a introduit un recours en annulation de la décision contraignante du CEPD devant la CJUE, qui a été déclaré irrecevable (actuellement en appel).

Les résultats de grande portée du mécanisme de cohérence apparaissent également dans les décisions contraignantes du CEPD de 2022 concernant les affaires Instagram, Facebook et WhatsApp : dans la première décision, concernant Instagram (juillet 2022), le CEPD a chargé la DPC de modifier son projet de décision afin d'y inclure une violation de l'Article 6 (1) du RGPD, après avoir conclu qu'Instagram traitait illégalement des données à caractère personnel d'enfants et de réévaluer l'amende administrative envisagée. Dans les décisions concernant Facebook et Instagram (décembre 2022), le CEPD a demandé à la DPC d'inclure dans sa décision finale une injonction à Meta de mettre son traitement de données à caractère personnel à des fins de publicité comportementale en conformité avec l'Article 6 (1) du RGPD dans un délai de trois mois, une constatation de violation du principe de loyauté, ainsi qu'une obligation d'adopter des mesures correctives appropriées. En outre, la décision contraignante du CEPD a conduit la DPC à augmenter considérablement les amendes dans ses décisions finales (d'un total de 58 millions d'euros dans les projets de décision, à un total de 390 millions d'euros dans les décisions finales). Le CEPD a également décidé que la DPC devait mener une nouvelle enquête concernant le traitement de catégories particulières de données à caractère personnel. Ces décisions sont actuellement examinées par la CJUE.

Une position similaire a été adoptée dans la décision contraignante du CEPD de décembre 2022 dans l'affaire WhatsApp, dans laquelle le CEPD a demandé à la DPC d'inclure dans sa décision finale une violation de l'Article 6(1) du RGPD et une amende administrative correspondante, ainsi qu'une violation du principe de loyauté, et d'ordonner à WhatsApp de mettre ses opérations de traitement en conformité dans un délai de trois mois. Le CEPD a également décidé que la DPC devait mener une enquête supplémentaire sur les activités de traitement de WhatsApp. Cette décision a créé des tensions avec la DPC qui a estimé que l'instruction du CEPD de mener des enquêtes supplémentaires posait un problème en termes de compétence et a déclaré qu'elle introduirait un recours en annulation devant la CJUE, dans la mesure où l'instruction pourrait impliquer un excès de pouvoir de la part du CEPD.

En vertu de l'Article 66, dans des circonstances exceptionnelles, lorsqu'une autorité de contrôle estime qu'il est urgent d'agir pour protéger les droits et libertés des personnes concernées, elle peut, par dérogation à l'autorité chef de file ou au mécanisme de cohérence, adopter immédiatement des mesures provisoires destinées à produire des effets juridiques sur son propre territoire, qui n'excèdent pas trois mois. C'est ce sur quoi s'est appuyée l'autorité de protection d'Hambourg lorsqu'elle a ouvert une procédure administrative contre Google (dont l'autorité chef de file est la DPC) en août 2019 en ce qui concerne le système Speech Assistant de Google. Elle a fait valoir qu'une protection efficace des personnes concernées contre l'écoute, la documentation et l'évaluation des conversations privées par des tiers ne peut être obtenue que par une exécution rapide.

Lorsqu'une autorité de contrôle a pris des mesures provisoires dans le cadre de la procédure d'urgence et qu'elle estime que des mesures définitives doivent être adoptées d'urgence, elle peut demander un avis urgent ou une décision contraignante urgente au CEPD. La première décision contraignante urgente de ce type a été adoptée par le CEPD en juillet 2021, à la suite d'une demande de l'autorité d'Hambourg, qui avait ordonné, à titre de mesure provisoire, l'interdiction du traitement des données des utilisateurs de WhatsApp par Facebook pour les besoins propres de cette dernière. Le CEPD a conclu que les conditions requises pour démontrer l'existence d'une violation et d'une urgence n'étaient pas réunies et a décidé qu'aucune mesure finale ne devait être adoptée par l'autorité chef de file (la DPC).

Le CEPD a également examiné en détail les mécanismes de coopération et de cohérence dans le cadre de sa contribution à l'évaluation du RGPD au titre de l'Article 97 (adopté le 18 février 2020) et a publié des lignes directrices à ce sujet. Elles soulignent que la mise en œuvre du mécanisme de l'autorité chef de file reste difficile et que son succès dépendra à l'avenir de l'interprétation cohérente des termes clés du RGPD, de l'alignement des procédures administratives nationales, des ressources humaines et financières adéquates des autorités de contrôle, de la poursuite de l'amélioration des outils de communication et des délais raisonnables pour le traitement des dossiers.

Où puis-je trouver ces dispositions ?

Considérants 124-138 et chapitre VII, Sections 1 et 2

Comité européen de protection des données

En bref

Le groupe de travail « Article 29 », dont les membres étaient les autorités de contrôle nationales de l'UE, le Contrôleur européen de la protection des données (« EDPS ») et la Commission européenne, a été transformé en Comité européen de la protection des données (« CEPD » ou « EDPB » en anglais), dont la composition est similaire, mais dont le secrétariat est indépendant.

Le CEPD a le statut d'un organe de l'UE doté de la personnalité juridique et de pouvoirs étendus pour trancher les litiges entre les autorités de contrôle nationales, donner des conseils et des orientations et approuver des codes et des certifications à l'échelle de l'UE.

À faire

Aucune action requise.

Commentaire

Depuis le 25 mai 2018, le CEPD a remplacé le groupe de travail « Article 29 », qui avait été créé en vertu de la directive sur la protection des données. Le CEPD est un organe de l'UE composé des chefs des autorités de contrôle nationales (ou de leurs représentants) et de l'EDPS.

Le représentant de la Commission européenne au sein du CEPD est un membre sans droit de vote. Dans les États (comme l'Allemagne) où il existe plusieurs autorités de contrôle, la législation nationale doit prévoir la désignation d'un représentant commun. Dans les cas de résolution de litiges, lorsqu'une décision contraignante doit être prise, les pouvoirs de vote de l'EDPS sont limités aux circonstances dans lesquelles les principes de l'affaire seraient applicables aux institutions de l'UE.

Le statut du CEPD a été considérablement amélioré. Il ne s'agit pas d'un simple comité consultatif, mais d'un organe indépendant de l'Union européenne doté d'une personnalité juridique propre.

Il est officiellement représenté par son président, qui a pour rôle principal d'organiser les travaux du CEPD et, en particulier, de gérer la procédure de conciliation pour les litiges entre les autorités nationales de surveillance. Le président et les deux adjoints sont élus parmi les membres du CEPD pour un mandat de cinq ans, renouvelable une fois.

Le CEPD prend normalement ses décisions à la majorité simple, mais les règles de procédure et les décisions contraignantes (en premier lieu) doivent être adoptées à la majorité des deux tiers.

Le CEPD a adopté son propre règlement intérieur et ses propres règles d'organisation. L'indépendance du CEPD y est soulignée. Il semble que l'on suggère implicitement que la Commission a exercé une trop grande influence sur le groupe de travail « *Article 29* » dans le passé et qu'elle cherche à consolider ce pouvoir.

Le CEPD dispose de son propre secrétariat, fourni par l'EDPS, mais qui agit uniquement sous la direction du président du CEPD.

Le CEPD dispose d'une liste de tâches longue et détaillée, mais son rôle principal est de contribuer à l'application cohérente du RGPD dans l'ensemble de l'Union. Il conseille la Commission européenne, 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 propositions de bonnes pratiques : par exemple, sur des questions telles que les cas où une violation de données est « *susceptible d'engendrer un risque élevé pour les droits et libertés* » des personnes ou sur les exigences en matière de règles d'entreprise contraignantes. À noter que lors de sa première réunion plénière, le CEPD a approuvé les lignes directrices du groupe de travail « Article 29 » relatives au RGPD qui ont été publiées jusqu'à ce jour.

Le rôle spécifique du CEPD est de concilier et de trancher les litiges entre les autorités nationales de surveillance. Pour en savoir plus sur cette activité, voir la section sur les compétences, missions et pouvoirs. L'ancien groupe de travail « Article 29 » a souvent été critiqué pour ne pas avoir consulté suffisamment les parties intéressées avant de prendre des décisions. Le CEPD est tenu de consulter les parties intéressées « *le cas échéant* ». Il s'agit d'un avantage majeur pour les personnes susceptibles d'être concernées par les avis, les lignes directrices, les conseils et les propositions de bonnes pratiques.

Les discussions du CEPD doivent être « *confidentielles, comme le prévoit son règlement intérieur* ». Cela signifie que les réunions et les discussions seront, en principe, publiques, sauf décision contraire.

Enfin, le CEPD publie des rapports annuels.

Pour en savoir plus :

Lignes directrices et rapports du CEPD :

Lignes directrices du CEPD 09/2020 relatives à l'objection pertinente et motivée au titre du règlement 2016/679

Lignes directrices du CEPD 02/2022 relatives à l'application de l'article 60 du RGPD

Lignes directrices du CEPD 8/2022 concernant la désignation d'une autorité de contrôle chef de file d'un responsable d'un traitement ou d'un sous-traitant

Contribution du CEPD à l'évaluation du RGPD au titre de l'article 97 (disponible en anglais uniquement)

Décisions contraignantes du CEPD :

Décision contraignante 1/2021 concernant le litige relatif au projet de décision de l'autorité de contrôle irlandaise concernant WhatsApp Ireland en application de l'article 65, paragraphe 1, point a), du RGPD

Décision contraignante 2/2022 concernant le litige relatif du projet de décision de l'autorité de contrôle irlandaise concernant Meta Platforms Ireland Limited (Instagram) en vertu de l'article 65, (1), point a), du RGPD

Décision contraignante 3/2022 relative au litige soumis par la SA irlandaise concernant Meta Platforms Ireland Limited et son service Facebook (article 65 RGPD) (disponible en anglais uniquement)

Décision contraignante 4/2022 relative au litige soumis par l'autorité de contrôle irlandaise concernant Meta Plateformes Ireland Limited et son service Instagram (article 65 RGPD)

Décision contraignante 5/2022 relative au litige soumis par l'autorité de contrôle irlandaise concernant WhatsApp Ireland Limited (Article 65 RGPD) (disponible en anglais uniquement)

Décision contraignante urgente 01/2021 relative à la demande, au titre de l'article 66, paragraphe 2, du RGPD, de l'autorité de contrôle de Hambourg (Allemagne) visant à ordonner l'adoption de mesures finales concernant Facebook Ireland Limited

Affaires judiciaires

Affaire C-645/19, *Facebook Ireland Ltd, Facebook Inc. et Facebook Belgium BVBA, contre Gegevensbeschermingsautoriteit*

Affaire T-709/21, *WhatsApp Ireland c. Comité européen de la protection des données*

Affaire T-129/23, *Meta Platforms Ireland c. Comité européen de la protection des données*

Affaire C-252/21, *Meta Platforms Inc, Meta Platforms Ireland Limited, Facebook Deutschland GmbH contre Bundeskartellamt*

CNIL c. Google, délibération du 21 janvier 2019 et arrêt du Conseil d'Etat confirmant la décision de la CNIL

Où puis-je trouver ces dispositions ?

Considérants 139 et 140, et chapitre VII, section 3

Voies de recours et responsabilités

En Bref

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

- le droit de déposer une plainte auprès des autorités de contrôle lorsque leurs données à caractère personnel ont été traitées d'une manière non conforme au RGPD ;
- le droit à un recours juridictionnel effectif lorsqu'une autorité de contrôle compétente ne traite pas correctement une plainte ;
- le droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant concerné ; et
- le droit d'obtenir d'un responsable du traitement ou d'un sous-traitant concerné une indemnisation pour les dommages matériels ou immatériels résultant d'une violation du RGPD.

Les personnes physiques et morales ont le droit de faire appel devant les juridictions nationales d'une décision juridiquement contraignante prise à leur encontre par une autorité de contrôle.

Les particuliers peuvent intenter une action en réparation d'un préjudice moral. La possibilité pour les organes représentatifs d'intenter des actions est facilitée.

Les recours juridictionnels et la responsabilité en matière d'indemnisation s'étendent à la fois aux responsables du traitement et aux sous-traitants qui enfreignent le règlement.

À faire

Les responsables du traitement et leurs sous-traitants devraient veiller à ce que les accords relatifs aux traitements des données et les accords de gestion des contrats précisent clairement l'étendue des responsabilités du sous-traitant et doivent convenir de mécanismes de résolution des litiges concernant leurs responsabilités respectives en matière de résolution des demandes en réparation.

Les responsables du traitement et les sous-traitants devraient convenir de signaler aux autres responsables du traitement ou sous-traitants impliqués dans le même traitement tout manquement à la conformité et toute plainte ou réclamation.

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 obligeait les autorités de contrôle à entendre les plaintes déposées par les personnes concernées afin de vérifier la licéité du traitement des données et d'informer les personnes concernées qu'un contrôle avait eu lieu.

Sous l'empire du RGPD, les personnes dont les données à caractère personnel sont traitées d'une manière non conforme au RGPD ont le droit spécifique d'introduire une plainte auprès des autorités de contrôle et celles-ci doivent informer les personnes concernées de l'évolution et de l'issue des plaintes.

Recours judiciaires contre les décisions prononcées par les autorités de contrôle

Les personnes concernées et les autres parties intéressées ont droit à un recours juridictionnel effectif contre certains actes et décisions des autorités de contrôle.

- Toute personne a droit à un recours juridictionnel effectif contre les décisions juridiquement contraignantes la concernant, prises par une autorité de contrôle.

- Les personnes concernées ont droit à un recours juridictionnel effectif lorsqu'une autorité de contrôle ne traite pas une plainte ou n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de sa plainte.

Le considérant 143 du RGPD explique que les décisions et les actions qui peuvent être contestées devant les tribunaux comprennent l'exercice des pouvoirs d'enquête, rectificatifs et d'autorisation par l'autorité de contrôle ou le rejet des plaintes. Ce droit n'englobe pas les autres mesures des 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 contre les responsables du traitement et les sous-traitants

Les personnes concernées dont les droits ont été violés ont droit à un recours juridictionnel effectif contre le responsable du traitement ou le sous-traitant responsable de la violation présumée. Cette disposition va au-delà de la disposition équivalente contenue précédemment dans la directive sur la protection des données, qui prévoyait un recours judiciaire uniquement contre les responsables du traitement des données, mais pas contre les sous-traitants.

Responsabilité en matière d'indemnisation

Toute personne ayant subi un préjudice du fait d'une violation du RGPD a le droit d'être indemnisée par le responsable du traitement ou le sous-traitant. Auparavant, en vertu de la directive sur la protection des données, la responsabilité en matière d'indemnisation était limitée aux seuls responsables du traitement.

La répartition de la responsabilité en matière d'indemnisation entre les responsables du traitement et les sous-traitants se fait comme suit :

- les responsables du traitement sont responsables des dommages causés par un traitement non conforme au RGPD ;

- les sous-traitants ne sont responsables que des dommages causés par un traitement effectué en violation des obligations spécifiquement imposées aux sous-traitants par le RGPD, ou causé par un traitement effectué en dehors de ce cadre ou contraire aux instructions des responsables du traitement ; et

- afin d'assurer une indemnisation efficace des personnes concernées, les responsables du traitement et les sous-traitants qui sont impliqués dans le même traitement et sont responsables de tout dommage causé, sont tenus responsables de l'intégralité du dommage. Toutefois, un sous-traitant ou un responsable du traitement qui est tenu de verser une indemnisation sur cette base a le droit de récupérer auprès des autres parties concernées la partie de la réparation correspondant à leur part de responsabilité dans le dommage.

Alors que la directive sur la protection des données ne mentionnait que le droit à l'indemnisation des « *dommages* », le RGPD précise que l'indemnisation peut être demandée pour les pertes pécuniaires et non pécuniaires. Cette clarification est toutefois cohérente avec l'interprétation actuelle du droit anglais de la signification du terme « *dommage* » aux fins des demandes d'indemnisation introduites précédemment en vertu de la loi de 1998 sur la protection des données (*Data Protection Act 1998* en anglais) (voir Google Inc. v VidalHall & Others [2015] EWCA Civ 311 (disponible en anglais uniquement)).

Dans l'affaire *Österreichische Post* (affaire C-300/21), la CJUE a établi que le droit à réparation prévu par le RGPD est soumis à trois conditions cumulatives : (i) une violation du RGPD, (ii) un dommage matériel ou immatériel résultant de cette violation et (iii) un lien de causalité entre le dommage et la violation. Ainsi, une simple violation du RGPD ne donne pas lieu à un droit à réparation. La CJUE a également estimé qu'il n'est pas nécessaire que le préjudice moral subi atteigne un certain seuil de gravité pour ouvrir un droit à réparation.

En décembre 2023, la CJUE a approfondi ces questions dans l'affaire C-340/21 - *Natsionalna agentsia za prihodite*, impliquant l'Agence nationale bulgare des recettes publiques (la NAP). La Cour a établi que la crainte d'une éventuelle utilisation abusive de données à caractère personnel est susceptible, en soi, de constituer un préjudice moral. Toutefois, lorsqu'une personne demandant réparation sur ce fondement invoque la crainte que ses données à caractère personnel soient utilisées abusivement à l'avenir en raison de l'existence d'une telle violation, la juridiction nationale saisie de l'affaire doit vérifier que cette crainte peut être considérée comme fondée, dans les circonstances spécifiques en cause et à l'égard de la personne concernée.

Le RGPD prévoit que les responsables du traitement et les sous-traitants sont exonérés de toute responsabilité s'ils prouvent que *« le fait générateur du dommage* [ne lui est] *pas imputable »*. Cette exonération semble légèrement plus restrictive que celle qui pouvait être invoquée en vertu de la directive sur la protection des données par un responsable du traitement qui pouvait prouver « *qu'il n'est pas responsable de l'évènement ayant provoqué le dommage* ».

Instances représentatives

Le RGPD permet aux instances représentatives, agissant au nom des personnes concernées, d'introduire des réclamations auprès des autorités de contrôle et d'introduire des recours judiciaires contre une décision d'une autorité de contrôle ou contre des responsables du traitement ou des sous-traitants. Cette disposition s'applique à tout organe de représentation qui est :

- un organisme, une organisation ou une association à but non lucratif ;
- dûment constitué conformément à la législation de l'État membre ;
- avec des objectifs statutaires qui sont dans l'intérêt du public ; et
- active dans le domaine de la protection des données.

Les personnes concernées peuvent également mandater ces organismes pour qu'ils exercent en leur nom le droit de demander réparation aux responsables du traitement ou aux sous-traitants, pour autant que la législation de l'État membre le permette.

Lorsqu'ils sont habilités à le faire par la législation de l'État membre, ces organes représentatifs peuvent, indépendamment du mandat de la personne concernée, déposer des plaintes auprès des autorités de contrôle et former des recours juridictionnels contre les décisions d'une autorité de contrôle ou contre les responsables du traitement des données ou les sous-traitants.

La CJUE dans l'affaire *Meta Platforms Ireland Limited c. Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.* (C-319/20) a confirmé que l'Article 80(2) du RGPD doit être interprété en ce sens qu'il ne s'oppose pas à ce qu'une réglementation nationale permette à une association de protection des consommateurs d'intenter une action en justice pour violation des lois de protection des données à caractère personnel en l'absence de mandat lui ayant été conféré à ce titre et indépendamment de la violation de droits spécifiques des personnes concernées.

La directive sur la protection des données ne contient pas de dispositions équivalentes.

Où puis-je trouver ces dispositions ?

Articles 77 à 82, considérants 141 à 147

Amendes administratives

En bref

Les autorités de contrôle sont habilitées à imposer des amendes administratives importantes aux responsables du traitement et aux sous-traitants.

Les amendes peuvent être imposées à la place ou en plus des mesures qui peuvent être ordonnées par les autorités de contrôle. Elles peuvent être imposées pour un large éventail de violations, 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 niveaux d'amendes administratives :

- Certaines violations feront l'objet d'amendes administratives pouvant aller jusqu'à 10 000 000 € ou, dans le cas des entreprises, jusqu'à 2 % du chiffre d'affaires mondial, le montant le plus élevé étant retenu.

- D'autres seront soumises à des amendes administratives d'un montant maximal de 20 000 000 € ou, dans le cas des entreprises, de 4 % du chiffre d'affaires mondial, 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.

Considérations générales

Les amendes administratives ne sont pas applicables automatiquement et doivent être imposées au cas par cas. Le considérant 148 précise que dans le cas d'une violation mineure, ou lorsqu'une amende imposerait une charge disproportionnée à une personne physique, un blâme peut être émis au lieu d'une amende. Dans ses lignes directrices sur l'application et la fixation des amendes administratives, le CEPD indique que les autorités de contrôle doivent évaluer tous les faits de l'affaire de manière cohérente et objectivement justifiée. En particulier, les autorités de contrôle doivent évaluer ce qui est efficace, proportionné et dissuasif dans chaque cas pour atteindre l'objectif poursuivi par la mesure corrective choisie, c'est-à-dire rétablir le respect des règles ou sanctionner un comportement illicite (ou les deux).

Le prononcé de sanctions financières par les autorités de contrôle variait beaucoup d'un État membre à l'autre. Bien que les dispositions du RGPD prévoient des sanctions maximales et laissent aux autorités de contrôle un certain pouvoir discrétionnaire quant à leur imposition, le considérant 150 indique que le mécanisme de cohérence peut être utilisé pour promouvoir une application cohérente des amendes administratives. Ceci est renforcé dans les lignes directrices du CEPD sur l'application et la fixation des amendes administratives aux fins du règlement 2016/679 (3 octobre 2017) (WP253), qui poussent à une approche harmonisée par le biais d'une participation active et d'un échange d'informations entre les autorités de contrôle afin de garantir que des sanctions équivalentes sont imposées pour des cas similaires.

Le 12 mai 2022, le CEPD a publié son projet de lignes directrices sur le calcul des amendes eu égard au RGPD, lignes directrices qui ont ensuite été finalisées et adoptées en juin 2023. L'objectif de ces lignes directrices est d'harmoniser la méthodologie utilisée par les autorités de contrôle pour calculer le montant de l'amende et de compléter les lignes directrices du CEPD susmentionnées sur l'application et la fixation des amendes administratives. Les lignes directrices définissent une méthodologie de calcul en cinq étapes selon laquelle les autorités de contrôle doivent :

1. déterminer si l'affaire en question concerne un ou plusieurs comportements passibles de sanction et s'ils ont conduit à une ou plusieurs violations (afin de clarifier si toutes les violations ou seulement certaines d'entre elles peuvent faire l'objet d'une amende) ;
2. s'appuyer sur un point de départ pour le calcul de l'amende pour lequel le CEPD fournit une méthode harmonisée ;
3. s'appuyer sur un point de départ pour le calcul de l'amende pour lequel le CEPD fournit une méthode harmonisée ;
4. prendre en compte les facteurs aggravants ou atténuants qui peuvent augmenter ou diminuer le montant de l'amende, pour lesquels le CEPD fournit une interprétation cohérente ;
5. déterminer les plafonds légaux des amendes comme indiqué à l'Article 83(4) et (6) RGPD et s'assurer que ces montants ne sont pas dépassés ; et
6. analyser si le montant final calculé répond aux exigences d'efficacité, de dissuasion et de proportionnalité ou s'il est nécessaire d'ajuster le montant.

Amendes administratives maximales

Le RGPD fixe deux séries de seuils maximaux pour les amendes administratives qui peuvent être imposées.

Dans chaque cas, l'amende maximale est exprimée en € (euros) ou, pour les entreprises, en pourcentage du chiffre d'affaires annuel mondial total de l'année précédente, le montant le plus élevé étant retenu. Le considérant 150 confirme que, dans ce contexte, le terme « *entreprise* » s'entend au sens des Articles 101 et 102 du traité sur le fonctionnement de l'Union européenne (« *TFUE* ») (c'est-à-dire, au sens large, comme des entités exerçant une activité économique).

La violation des dispositions suivantes du RGPD est passible d'amendes administratives pouvant aller jusqu'à 20 000 000 € ou, dans le cas des entreprises, jusqu'à 4 % du chiffre d'affaires mondial, le montant le plus élevé étant retenu :

- les principes du traitement, y compris les conditions de validité du consentement (Articles 5, 6, 7 et 9) ;
- les droits des personnes concernées (Articles 12 à 22) ;

- les transferts internationaux (Articles 44-49) ;
- les obligations découlant de la législation des États membres adoptée en vertu du chapitre IX ; et
- le non-respect d'une injonction imposée par les autorités de contrôle (visée à l'Article 58(2)) ou le non-respect d'une enquête menée par une autorité de contrôle en vertu de l'Article 58(1).

Les autres infractions sont passibles d'amendes administratives pouvant aller jusqu'à 10 millions d'euros ou, dans le cas des entreprises, jusqu'à 2 % du chiffre d'affaires mondial, le montant le plus élevé étant retenu. Les infractions soumises à ces amendes maximales comprennent la violation des obligations suivantes :

- obtenir le consentement au traitement des données relatives aux enfants (Article 8) ;
- mettre en œuvre des mesures techniques et organisationnelles pour assurer la protection des données dès la conception et par défaut (Article 25) ;
- pour les responsables conjoints du traitement, convenir de leurs obligations de conformité respectives (Article 26) ;
- pour les responsables du traitement et les sous-traitants qui ne sont pas établis dans l'UE, désigner des représentants (Article 27) ;
- pour les responsables du traitement, les obligations relatives à l'engagement des sous-traitants (Article 28) ;
- pour les sous-traitants, ne sous-traiter qu'avec l'accord préalable du responsable du traitement et ne traiter les données que sur instruction du responsable du traitement (Articles 28-29) ;
- tenir des registres écrits (Article 30) ;
- l'obligation pour les responsables du traitement et les sous-traitants de coopérer avec les autorités de contrôle (Article 31) ;
- la mise en œuvre de mesures techniques et organisationnelles (Article 32) ;
- signaler les violations lorsque le RGPD l'exige (Articles 33-34) ;
- la réalisation des analyses d'impact de protection des données (Articles 35-36) ;
- la désignation des Délégués à la Protection des Données (« DPD ») (ou *Data Protection Officer (« DPO »)* en anglais) (Articles 37-39) ;
- les obligations imposées aux organismes de certification (Articles 42-43) ; et
- les obligations imposées aux organes de contrôle pour prendre des mesures en cas d'infraction aux codes de conduite (Article 41).

Dans les cas où le même traitement ou un traitement lié implique une violation de plusieurs dispositions du RGPD, les amendes ne peuvent pas dépasser le montant prévu pour la violation la plus grave.

En décembre 2023, la CJUE a rendu un arrêt dans l'affaire C-683/21, impliquant le Centre national de santé publique relevant du ministère lituanien de la santé. Elle a établi comme principe général qu'un responsable du traitement peut être jugé responsable et se voir infliger une amende pour les actions d'un sous-traitant qui effectue des opérations de traitement de données pour le compte de ce responsable du traitement, à moins que le sous-traitant n'ait agi d'une manière qui était incompatible avec les dispositions contractuelles précédemment convenues avec le responsable du traitement.

Facteurs à prendre en compte

L'Article 83(2) énumère les facteurs qu'une autorité de contrôle doit prendre en compte pour déterminer s'il y a lieu d'infliger une amende administrative et pour décider du montant de l'amende à infliger. Ces facteurs sont les suivants :

- la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ;
- le fait que la violation a été commise délibérément ou par négligence ;
- toute mesure prise 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 ;
- toute violation antérieure pertinente ;
- le degré de coopération avec l'autorité de contrôle ;
- les catégories de données à caractère personnel concernées ;
- si la violation a été notifiée par le responsable du traitement ou le sous-traitant à l'autorité de contrôle ;
- les antécédents en matière d'application de la loi ;
- l'adhésion à des codes de conduite approuvés conformément à l'Article 40 ou à des mécanismes de certification approuvés conformément à l'Article 42 ; et
- toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce (par exemple, les avantages financiers obtenus, les pertes évitées, directement ou indirectement, du fait de la violation).

Lorsque des amendes sont infligées à des personnes qui ne sont pas des entreprises, l'autorité de contrôle doit également tenir compte de la situation économique de ces personnes.

Pour fixer le niveau des amendes administratives au sein de chaque seuil, les lignes directrices 04/2022 du CEPD sur le calcul des amendes au titre du RGPD exigent que les autorités de contrôle évaluent tous les faits du dossier d'une manière cohérente et objectivement justifiée.

Dérogations et conditions particulières

En bref

En vertu du RGPD, les États membres conservent la possibilité d'introduire des dérogations lorsque celles-ci sont nécessaires aux fins de sécurité nationale, de prévention et de détection de la criminalité et dans certaines autres situations.

Conformément à la jurisprudence de la Cour de justice de l'Union européenne, toute dérogation doit respecter « *l'essence* » du droit à la protection des données et constituer une mesure nécessaire et proportionnée.

Le RGPD exige ou permet aux États membres d'introduire des lois complémentaires pour certaines finalités spéciales. Dans le cas de la recherche historique et scientifique, du traitement statistique et de l'archivage, cela peut même constituer une base légale pour le traitement de catégories particulières de données.

Parmi les autres sujets particuliers pour lesquels le RGPD prévoit l'adoption d'une législation par les États membres figurent le traitement des données relatives aux employés, le traitement lié à la liberté d'expression et le secret professionnel (lorsque des restrictions des droits d'audit de l'autorité de contrôle sont prévues).

Les responsables du traitement (et, dans certains cas, les sous-traitants) doivent vérifier les différentes approches des États membres dans ces domaines et s'y adapter.

Les variations locales doivent être prises en compte car elles sont significatives dans de nombreux domaines, par exemple le traitement des données relatives aux ressources humaines.

À faire

Déterminez si les traitements que vous effectuez peuvent faire l'objet de dérogations ou de conditions particulières en vertu du RGPD, et vérifiez les dispositions mises en œuvre dans les législations des États membres qui vous sont applicables.

Commentaire

Cas particuliers

Le RGPD contient de larges dérogations et exemptions dans deux domaines principaux : (1) au chapitre III, section 5, concernant les « *limitations* » aux obligations et aux droits en matière de protection des données ; et (2) au chapitre IX, concernant les « *situations particulières de traitement des données* ». La direction générale de la justice et des consommateurs de la Commission européenne a publié un rapport (disponible uniquement en anglais) résumant la mise en œuvre de ces dispositions spécifiques par les États membres en janvier 2021.

Article 23 - Restrictions

L'Article 23 du RGPD a créé le droit pour les États membres d'introduire des dérogations dans certaines situations. Les États membres peuvent introduire des dérogations aux obligations de transparence et aux droits des personnes concernées, mais uniquement lorsque la mesure *« respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique ».*

Toute dérogation doit préserver l'un des éléments suivants :

- la sécurité nationale ;
- la défense ;
- la sécurité publique ;
- la prévention et la détection d'infractions pénales ou de manquements à la déontologie dans les professions réglementées ;
- d'autres objectifs importants d'intérêt public, notamment des intérêts économiques ou financiers (par exemple, des questions budgétaires et fiscales) ;
- la protection de l'indépendance de la justice et des procédures judiciaires ;
- l'exercice de l'autorité publique dans des fonctions de contrôle, d'inspection ou de réglementation liées à l'exercice de l'autorité publique en matière de sécurité, de défense, d'autres intérêts publics importants ou de prévention de la criminalité et de l'éthique ;
- la protection de la personne concernée ou des droits et libertés d'autrui ; ou
- l'exécution des demandes de droit civil.

Pour qu'une mesure soit acceptable, elle doit (conformément à l'Article 23(2)) comporter des dispositions spécifiques établissant :

- les finalités du traitement ;
- les catégories de données concernées ;
- la portée des limitations au RGPD qui sont introduites par la mesure ;
- les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ;
- les responsables pouvant invoquer ces limitations ;
- la durée de conservation et les mesures de sécurité applicables ;
- le risque pour les droits et libertés des personnes concernées ; et
- le droit des personnes concernées d'être informées de la limitation, à moins que cela ne risque de nuire à la finalité de la limitation.

Articles 85-91 : « *Situations particulières de traitement des données* »

Les dispositions du chapitre IX du RGPD prévoient un ensemble de dérogations, d'exemptions et de pouvoirs permettant d'imposer des exigences supplémentaires, en ce qui concerne les obligations et les droits du RGPD, pour des types de traitement particuliers.

Article 85 : Liberté d'expression et d'information

Cette disposition impose aux États membres d'introduire des dérogations au RGPD lorsque cela est nécessaire pour « *concilie[r], par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression et d'information* ». L'Article 85(2) prévoit une disposition spécifique pour les traitements effectués à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire. Les États membres étaient tenus d'informer la Commission européenne de la manière dont ils comptaient

mettre en œuvre cette exigence et de toute modification apportée à ces lois.

Article 86 : Accès du public aux documents officiels

Cette disposition permet de divulguer les données à caractère personnel contenues dans les documents officiels conformément aux lois de l'Union ou des États membres qui autorisent l'accès du public aux documents officiels. Cette possibilité n'est pas illimitée : ces lois doivent, conformément au considérant 154 du RGPD, « *concilier le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel* ».

Article 87 : Numéros d'identification nationaux

Les États membres conservent le droit de fixer leurs propres conditions pour le traitement des numéros d'identification nationaux, à condition que des garanties appropriées soient mises en place.

Article 88 : Données relatives aux employés

Les États membres sont autorisés à établir (soit par la loi, soit par des conventions collectives) des règles plus spécifiques en ce qui concerne le traitement des données à caractère personnel des employés, couvrant tous les aspects majeurs des relations de travail, du recrutement à la cessation d'emploi. Cela inclut la possibilité de mettre en œuvre des règles établissant quand le consentement peut être considéré comme valide dans une relation de travail. Ces règles doivent comprendre des mesures spécifiques visant à sauvegarder « *la dignité humaine, les intérêts légitimes et les droits fondamentaux* » de la personne concernée, et le RGPD cite la transparence du traitement, les transferts intra-groupes et les systèmes de contrôle comme des domaines dans lesquels une attention particulière doit être accordée à ces questions. Les États membres doivent notifier à la Commission européenne toute loi introduite en vertu de cet article, ainsi que toute modification subséquente de cette législation. Des informations détaillées à ce sujet sont disponibles sur le site internet de la Commission européenne.

Article 89, (1) et (2) : Fins de recherche scientifique et historique ou fins statistiques

L'Article 89(1) reconnaît que les responsables du traitement peuvent traiter des données à ces fins lorsqu'il existe des garanties adéquates (voir les sections sur la licéité du traitement et traitement ultérieur et sur les catégories particulières de données et licéité du traitement). Dans la mesure du possible, les responsables du traitement sont tenus de réaliser ces finalités avec des données qui ne permettent pas ou plus d'identifier les personnes concernées. Ainsi, si l'anonymisation n'est pas possible, il convient de recourir à la pseudonymisation, à moins que cela ne nuise également à la finalité de la recherche ou du processus statistique. Des commentaires utiles sur la pseudonymisation ont été publiés par l'ENISA dans son rapport de janvier 2019 intitulé « *Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation* » (disponible uniquement en anglais), et des lignes directrices sur l'anonymisation figurent dans le programme de travail du CEPD pour 2023-2024.

L'Article 89(2) permet aux États membres et à l'UE de légiférer davantage pour prévoir des dérogations aux droits d'accès, de rectification, d'effacement, de limitation et d'opposition des personnes concernées (sous réserve des garanties prévues à l'Article 89(1) lorsque ces droits « *risqueraient de rendre impossible ou d'entraver sérieusement* » la réalisation de ces finalités spécifiques et que la dérogation est nécessaire pour répondre à ces exigences.

Les considérants apportent des précisions sur l'interprétation des termes « *recherche scientifique* », « *recherche historique* » et « *fins statistiques* ». Le considérant 159 indique que la recherche scientifique doit être « *interprété[e] au sens manière large* » et inclut la recherche financée par le secteur privé, ainsi que les études menées dans l'intérêt public. Pour que le traitement soit considéré comme étant de nature statistique, le considérant 162 précise que le résultat du traitement ne doit pas être « *des données à caractère personnel, mais des données agrégées* » et qu'il ne doit pas être utilisé pour étayer des mesures ou des décisions concernant une personne en particulier.

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

Les mêmes dérogations et garanties existent pour les traitements à des fins « *archivistiques dans l'intérêt public* » que celles mentionnées ci-dessus en ce qui concerne le traitement à des fins de recherche et de statistiques, sauf que des dérogations peuvent également être accordées pour le droit à la portabilité des données. Le considérant 158 fournit de plus amples détails et suggère que seuls les organismes ou autorités ayant l'obligation d'interagir avec des documents qui sont à conserver « *à titre définitif dans l'intérêt public général* » en vertu du droit de l'État membre ou de l'Union peuvent se prévaloir de cette disposition.

Article 90 : Obligations de secret

Cet article permet aux États membres d'introduire des règles spécifiques pour protéger une « *obligation de secret professionnel* » ou « *à d'autres obligations de secret équivalentes* » lorsque les autorités de contrôle sont habilitées à avoir accès à des données à caractère personnel ou à des locaux. Ces règles doivent « *concilier le droit à la protection des données à caractère personnel et l'obligation de secret* » et ne peuvent s'appliquer qu'aux données reçues ou obtenues en vertu d'une telle obligation. Là encore, les États membres doivent notifier à la Commission européenne toute loi introduite en vertu de cet article, ainsi que toute modification. Des informations détaillées à ce sujet sont disponibles sur le site internet de la Commission européenne.

Article 91 : Églises et associations religieuses

Cet article protège les règles « *compl[ètes]* » existantes pour les églises, les associations religieuses et les communautés lorsqu'elles sont mises en conformité avec les dispositions du RGPD. Ces entités devront toujours se soumettre au contrôle d'une autorité de contrôle indépendante dans les conditions prévues au chapitre VI (voir la section relative aux catégories particulières de données et licéité du traitement et celle relative à la coopération et 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

Comme le prévoient les chapitres finaux du RGPD, le RGPD est entré en vigueur le 25 mai 2018. La relation prévue entre le RGPD et d’autres instruments en matière de protection des données de l’UE, y compris la directive 2002/58/CE (la « *directive vie privée et communications électroniques* »), est également exposée dans ces chapitres.

La Commission européenne présentera régulièrement des rapports sur le RGPD. Ces dispositions finales autorisent également la Commission européenne à adopter certains actes délégués en vertu du RGPD (par exemple, en ce qui concerne l’utilisation d’icônes et de mécanismes de certification).

Commentaire

Le chapitre 10 du RGPD confère à la Commission européenne le pouvoir d'adopter des actes délégués (tels que visés à l'Article 12(8) en ce qui concerne les icônes normalisées et à l'Article 43(8) en ce qui concerne les mécanismes de certification). Ces pouvoirs législatifs délégués peuvent être révoqués par le Parlement ou le Conseil à tout moment. Les actes délégués entrent en vigueur au plus tôt trois mois après leur publication, et seulement si ni le Parlement ni le Conseil ne s'y opposent. La Commission européenne sera assistée par un comité, conformément au règlement 182/2011. Il est particulièrement important que la Commission européenne procède à des consultations appropriées lors de ses travaux préparatoires, y compris au niveau des experts (considérant 166).

Des compétences d'exécution sont également conférées à la Commission européenne afin de garantir des conditions uniformes pour la mise en œuvre du RGPD. Ces compétences devraient également être exercées conformément au règlement 182/2011.

Le chapitre 11 du RGPD confirme que la directive sur la protection des données a été abrogée le 25 mai 2018. Les références dans d'autres législations à la directive abrogée sur la protection des données sont désormais interprétées comme des références au RGPD, et les références au groupe de travail « Article 29 » sont désormais interprétées comme des références au CEPD.

La Commission européenne fournira régulièrement des rapports sur le RGPD au Parlement et au Conseil, en mettant l'accent sur les dispositions du RGPD relatives au transfert de données, à la coopération et à la cohérence. Le premier rapport a été publié le 24 juin 2020, et de nouveaux rapports suivront tous les 4 ans. Les rapports seront rendus publics.

L'Article 95 précise que le RGPD doit être interprété de manière à ne pas imposer d'obligations supplémentaires aux fournisseurs de services de communications électroniques accessibles au public dans l'Union dans la mesure où ils sont soumis à des obligations spécifiques au titre de la directive « *vie privée et communications électroniques* » (2002/58/CE, telle que modifiée) qui poursuivent les mêmes objectifs. Un nouveau règlement européen sur la protection de la vie privée a été proposé par la Commission européenne, début 2017, pour remplacer cette directive. Toutefois, le Parlement européen et le Conseil ne sont pas parvenus, à ce jour, à un accord sur le texte final.

Le considérant 171 précise que lorsque le traitement est fondé sur un consentement obtenu avant l'entrée en vigueur du RGPD, il n'est pas nécessaire que l'individu donne à nouveau son consentement si la manière dont celui-ci a été donné est conforme aux conditions du RGPD.

Où puis-je trouver ces dispositions ?

Articles 92-99, considérants 166-173

À propos de nous

Un cabinet d'avocats de premier plan spécialisé dans la protection des données et les technologies

Experts en protection des données

Nous sommes classés parmi les meilleurs dans les annuaires juridiques et nous sommes fiers d'avoir l'une des plus grandes pratiques d'Europe et d'Asie-Pacifique. Nous avons une connaissance approfondie de l'évolution de la technologie et du droit. Nos clients collectent souvent de grandes quantités de catégories particulières de données et sont des entreprises de premier plan, pour lesquelles la divulgation ou l'utilisation abusive de données entraînerait de graves conséquences.

Un certain nombre de nos avocats sont d'anciens membres d'autorités de protection des données. Certains d'entre eux ont également travaillé en entreprise, ce qui donne à l'équipe une expérience pratique et renforce notre approche pragmatique et collaborative de la fourniture de services juridiques à nos clients.

Couverture mondiale

Nous comptons 1 400 avocats dans le monde entier, répartis dans un réseau mondial de 32 bureaux dans 23 pays.

- ***Emplacement des bureaux de Bird & Bird*** : Abu Dhabi ● Amsterdam ● Pékin ● Bratislava ● Bruxelles ● Budapest ● Casablanca ● Copenhague ● Dubaï ● Dublin ● Düsseldorf ● Francfort ● La Haye ● Hambourg ● Helsinki ● Hong Kong ● Londres ● Luxembourg ● Lyon ● Madrid ● Milan ● Munich ● Paris ● Prague ● Rome ● San Francisco ● Shanghai ● Singapour ● Stockholm ● Sydney ● Varsovie ● Shenzhen.

- ***Bird & Bird Plus Firms*** : Construire un réseau de collaboration afin d'offrir à nos clients un service juridique international intégré avec des cabinets d'avocats affiliés.

Contactez-nous

Contactez l'un des membres de notre équipe si vous avez une question concernant la protection des données.

Willy Mikalef

Partner

+33142686349
willy.mikalef@twobirds.com

Benoit Van Asbroeck

Partner

+3222826067
benoit.van.asbroeck@twobirds.com

Gabriel Voisin

Partner

+442079056236
gabriel.voisin@twobirds.com

Vincent Rezzouk-Hammachi

Partner

+442074156055
vincent.rezzouk@twobirds.com

Ariane Mole

Of Counsel

+33142686304
ariane.mole@twobirds.com