



17/FR

WP259 rév.01

**Groupe de travail «Article 29»
Lignes directrices sur le consentement au sens du règlement 2016/679**

Adoptées le 28 novembre 2017

Version révisée et adoptée le 10 avril 2018

**LE GROUPE DE PROTECTION DES PERSONNES À L'ÉGARD DU
TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL**

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LES PRÉSENTES LIGNES DIRECTRICES:

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et État de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013

Site web: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Sommaire

| | | |
|--------|--|----|
| 1. | Introduction..... | 3 |
| 2. | Le consentement dans l'article 4, paragraphe 11, du RGPD..... | 5 |
| 3. | Éléments d'un consentement valable | 5 |
| 3.1. | Manifestation de volonté libre | 6 |
| 3.1.1. | Déséquilibre des rapports de force | 6 |
| 3.1.2. | Conditionnalité | 8 |
| 3.1.3. | Nécessité de détailler le consentement | 11 |
| 3.1.4. | Préjudice | 12 |
| 3.2. | Spécifique | 13 |
| 3.3. | Éclairée | 14 |
| 3.3.1. | Exigences minimales de contenu pour que le consentement soit «éclairé» | 15 |
| 3.3.2. | Comment fournir des informations..... | 15 |
| 3.4. | Univoque | 18 |
| 4. | Obtention d'un consentement explicite | 20 |
| 5. | Conditions supplémentaires d'obtention d'un consentement valable..... | 23 |
| 5.1. | Démonstration du consentement | 23 |
| 5.2. | Retrait du consentement..... | 24 |
| 6. | Interactions entre le consentement et les autres bases juridiques définies par l'article 6 du RGPD | 27 |
| 7. | Domaines critiques spécifiques dans le RGPD..... | 27 |
| 7.1. | Les enfants (article 8) | 27 |
| 7.1.1. | Service de la société de l'information | 28 |
| 7.1.2. | Proposés directement à un enfant | 29 |
| 7.1.3. | Âge..... | 29 |
| 7.1.4. | Consentement des enfants et responsabilité parentale | 30 |
| 7.2. | La recherche scientifique..... | 32 |
| 7.3. | Les droits des personnes concernées..... | 35 |
| 8. | Consentement obtenu en vertu de la directive 95/46/CE | 35 |

1. Introduction

Les présentes lignes directrices fournissent une analyse approfondie de la notion de consentement dans le règlement 2016/679, également connu sous le nom de règlement général sur la protection des données (ci-après le «RGPD»). Le concept de consentement tel qu'utilisé jusqu'à présent dans la directive sur la protection des données (ci-après la «directive 95/46/CE») et dans la directive «vie privée et communications électroniques» a évolué. Le RGPD apporte des clarifications et des précisions complémentaires sur les conditions d'obtention et de démonstration d'un consentement valable. Les présentes lignes directrices se concentrent sur ces modifications afin de fournir des orientations pratiques visant à assurer le respect du RGPD, en s'inspirant de l'avis 15/2011 sur le consentement. Il incombe aux responsables du traitement d'innover afin de trouver de nouvelles solutions qui fonctionnent selon les paramètres de la loi et favorisent davantage la protection des données à caractère personnel ainsi que les intérêts des personnes concernées.

Le consentement demeure l'une des six bases juridiques permettant de traiter des données à caractère personnel, telles qu'énumérées à l'article 6 du RGPD¹. Lorsqu'il entreprend des activités qui impliquent le traitement de données à caractère personnel, le responsable du traitement doit toujours prendre le temps d'examiner quelle serait la base juridique appropriée pour le traitement envisagé.

En général, le consentement ne constitue une base juridique appropriée que si la personne concernée dispose d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées ou de la possibilité de les refuser sans subir de préjudice. Lorsqu'il sollicite un consentement, le responsable du traitement a l'obligation d'évaluer si celui-ci satisfera à toutes les conditions d'obtention d'un consentement valable. S'il a été obtenu dans le plein respect du RGPD, le consentement est un outil qui confère aux personnes concernées un contrôle sur le traitement éventuel de leurs données à caractère personnel. Dans le cas contraire, le contrôle de la personne concernée devient illusoire et le consentement ne constituera pas une base valable pour le traitement des données, rendant de ce fait l'activité de traitement illicite².

Les avis existants du groupe de travail «Article 29» (ci-après le «G29») sur le consentement³ restent pertinents lorsqu'ils sont en phase avec le nouveau cadre juridique, dès lors que le RGPD codifie certaines des orientations et des bonnes pratiques générales du G29 et que la plupart des principaux éléments du consentement restent identiques en vertu du RGPD. Aussi le G29 développe-t-il et complète-t-il dans le présent document ses avis précédents relatifs à des thématiques spécifiques comprenant des références au consentement au sens de la directive 95/46/CE plutôt que de les remplacer.

¹ L'article 9 du RGPD fournit une liste de dérogations possibles à l'interdiction de traiter les catégories particulières de données à caractère personnel. L'une des exceptions citées est lorsque la personne concernée donne son consentement explicite au traitement des données.

² Voir également l'avis 15/2011 sur la définition du consentement (CP 187), p. 6-9 et/ou l'avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE (WP 217), p. 10, 11, 14 et 15.

³ Principalement l'avis 15/2011 sur la définition du consentement (WP 187).

Comme indiqué dans l'avis 15/2011 sur la définition du consentement, l'invitation à accepter le traitement de données devrait être régie par des conditions strictes, dès lors qu'elle concerne les droits fondamentaux des personnes concernées et que le responsable du traitement souhaite procéder à un traitement qui serait illicite sans le consentement de la personne concernée⁴. Le rôle essentiel du consentement est souligné par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. En outre, l'obtention d'un consentement n'annule pas ou ne diminue pas de quelque façon que ce soit l'obligation imposée au responsable du traitement de respecter les principes relatifs au traitement énoncés dans le RGPD, notamment dans son article 5 concernant la loyauté, la nécessité, la proportionnalité ainsi que la qualité des données. Ainsi, même si le traitement de données à caractère personnel a reçu le consentement de la personne concernée, cela ne justifie pas la collecte de données excessives au regard d'une finalité spécifique de traitement, ce qui serait foncièrement abusif⁵.

Dans le même temps, le G29 est conscient de la révision de la directive «vie privée et communications électroniques» (2002/58/CE). La notion de consentement telle que présentée dans le projet de règlement «vie privée et communications électroniques» reste liée à la notion de consentement au sens du RGPD⁶. En vertu de ce nouvel instrument, les entreprises nécessiteront probablement le consentement des personnes concernées pour la plupart de leurs messages commerciaux en ligne et de leurs appels commerciaux, ainsi que pour leurs méthodes de suivi en ligne, y compris moyennant l'utilisation de cookies, d'applications ou d'autres logiciels. Le G29 a déjà fourni des recommandations et des orientations au législateur européen concernant la proposition de règlement «vie privée et communications électroniques»⁷.

Concernant la directive «vie privée et communications électroniques» existante, le G29 note que les références faites à la directive 95/46/CE abrogée s'entendent comme faites au RGPD⁸. Ceci s'applique également aux références faites au consentement dans l'actuelle directive 2002/58/CE, dès lors que le règlement «vie privée et communications électroniques» ne sera pas (encore) entré en vigueur le 25 mai 2018. Selon l'article 95 du RGPD, aucune obligation supplémentaire concernant le traitement de données dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications ne sera imposée dans la mesure où la directive «vie privée et communications électroniques» impose des obligations spécifiques ayant le même objectif. Le G29 note que les exigences relatives au consentement imposées par le RGPD ne sont pas considérées comme des «obligations supplémentaires», mais plutôt comme des conditions préalables essentielles au traitement licite. Aussi les conditions d'obtention d'un consentement valable établies par le RGPD sont-elles applicables dans les situations tombant dans le champ d'application de la directive «vie privée et communications électroniques».

⁴ Avis 15/2011 sur la définition du consentement (WP 187), p. 9.

⁵ Voir également l'avis 15/2011 sur la définition du consentement (WP 187) et l'article 5 du RGPD.

⁶ Selon l'article 9 de la proposition de règlement «vie privée et communications électroniques», la définition et les conditions du consentement figurant à l'article 4, paragraphe 11, et à l'article 7 du RGPD s'appliquent.

⁷ Voir l'avis 03/2016 sur l'évaluation et la révision de la directive «vie privée et communications électroniques» (WP 240).

⁸ Voir l'article 94 du RGPD.

2. Le consentement dans l'article 4, paragraphe 11, du RGPD

L'article 4, paragraphe 11, du RGPD définit le consentement comme suit: *«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 concept fondamental de consentement reste identique à celui de la directive 95/46/CE; et le consentement constitue l'une des bases juridiques sur lesquelles tout traitement de données à caractère personnel doit être fondé conformément à l'article 6 du RGPD⁹. Outre la définition révisée de l'article 4, paragraphe 11, le RGPD fournit des orientations complémentaires dans son article 7 et dans ses considérants 32, 33, 42 et 43 quant à la façon dont le responsable du traitement doit agir afin de respecter les principaux éléments de l'exigence de consentement.

Enfin, l'introduction de dispositions et de considérants spécifiques sur le retrait du consentement confirme que le consentement devrait être une décision réversible et qu'un certain degré de contrôle par la personne concernée demeure.

3. Éléments d'un consentement valable

L'article 4, paragraphe 11, du RGPD stipule que le consentement de la personne concernée signifie 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.

Les sections suivantes analysent dans quelle mesure la formulation de l'article 4, paragraphe 11, exige des responsables du traitement de modifier leurs demandes/formulaires de consentement afin de se conformer au RGPD¹⁰.

⁹ Le consentement était défini par la directive 95/46/CE comme *«toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement»* qui doit être *«indubitablement donné»* afin de rendre le traitement des données à caractère personnel légitime (article 7, point a), de la directive 95/46/CE). Voir l'avis 15/2011 du G29 sur la définition du consentement (WP 187) pour des exemples d'adéquation du consentement en tant que base juridique. Dans cet avis, le G29 a fourni des orientations afin de distinguer les cas où le consentement est une base juridique appropriée de ceux où les intérêts légitimes (avec une éventuelle possibilité de refus) constituent une base suffisante, ou encore lorsqu'une relation contractuelle serait recommandée. Voir également l'avis 06/2014 du G29, paragraphe III.1.2, p. 15 et suivantes. Le consentement explicite constitue également l'une des exceptions à l'interdiction de traitement portant sur des catégories particulières de données: voir l'article 9 du RGPD.

¹⁰ Pour des orientations concernant les activités de traitement en cours basées sur le consentement au sens de la directive 95/46/CE, voir le chapitre 7 du présent document ainsi que le considérant 171 du RGPD.

3.1. Manifestation de volonté libre¹¹

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 valable¹². Si le consentement est présenté comme une partie non négociable des conditions générales, l'on considère qu'il n'a pas été donné librement. Le consentement ne sera par conséquent pas considéré comme étant donné librement si la personne concernée n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice¹³. La notion de déséquilibre entre le responsable du traitement et la personne concernée est également prise en compte par le RGPD.

Au moment de déterminer si le consentement est donné librement, il y a également lieu de tenir compte de la situation spécifique de l'intégration du consentement dans un contrat ou de son association à la fourniture d'un service, comme décrit à l'article 7, paragraphe 4. L'article 7, paragraphe 4, a été rédigé de façon non exhaustive par l'usage des termes «entre autres», ce qui signifie qu'une série d'autres situations peut tomber sous le coup de cette disposition. En termes généraux, toute pression ou influence inappropriée exercée sur la personne concernée (pouvant se manifester de différentes façons) l'empêchant d'exercer sa volonté rendra le consentement non valable.

[Exemple 1]

Une application mobile d'édition de photos demande à ses utilisateurs d'activer leur localisation GPS afin de pouvoir utiliser ses services. L'application indique également à ses utilisateurs qu'elle utilisera les données collectées à des fins de publicité comportementale. Ni la géolocalisation, ni la publicité comportementale en ligne ne sont nécessaires à la fourniture de services d'édition de photos et toutes deux dépassent de ce fait la fourniture du service de base proposé. Dès lors que les utilisateurs ne peuvent pas utiliser l'application sans consentir à ces finalités, le consentement ne peut pas être considéré comme donné librement.

3.1.1. Déséquilibre des rapports de force

Le considérant 43¹⁴ indique clairement qu'il n'est pas probable que des **autorités publiques** puissent se fonder sur le consentement pour le traitement de données à caractère personnel, dès lors

¹¹ Dans plusieurs avis, le groupe de travail «Article 29» a exploré les limites du consentement dans des situations où il ne peut être donné librement. C'était notamment le cas de l'avis 15/2011 sur la définition du consentement (WP 187), du document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (WP 131), de l'avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel (WP 48), du deuxième avis 4/2009 sur le traitement de données par l'Agence mondiale antidopage (deuxième avis 4/2009 sur le standard international de l'Agence mondiale antidopage (AMA) sur la protection de la vie privée et des renseignements personnels, sur les dispositions y afférentes du Code de l'AMA et sur d'autres questions concernant la vie privée dans le contexte de la lutte contre le dopage dans le sport menée par l'AMA et des organisations antidopage (nationales) (WP 162)).

¹² Voir l'avis 15/2011 sur la définition du consentement (WP 187), p. 14.

¹³ Voir les considérants 42 et 43 du RGPD et l'avis 15/2011 du G29 sur la définition du consentement, adopté le 13 juillet 2011 (WP 187), p. 14.

¹⁴ Le considérant 43 du RGPD prévoit que: «Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière. [...]»

que lorsque le responsable du traitement est une autorité publique, il existe souvent un déséquilibre manifeste des rapports de force entre le responsable du traitement et la personne concernée. Il est également clair que dans la plupart des cas, la personne concernée n'aura pas de solution alternative réaliste à l'acceptation du traitement (et des conditions de traitement) de ce type de responsable du traitement. Le G29 considère qu'il existe d'autres bases juridiques en principe plus adaptées aux activités des autorités publiques¹⁵.

Sans préjudice de ces considérations générales, le cadre juridique du RGPD n'exclut pas entièrement le recours au consentement en tant que base juridique du traitement de données par des autorités publiques. Les exemples suivants démontrent que le recours au consentement peut être approprié dans certaines circonstances.

[Exemple 2] Une municipalité locale prévoit des travaux d'entretien de la voirie. Dès lors que les travaux de voirie pourraient perturber la circulation pendant un certain temps, la municipalité offre à ses citoyens la possibilité de s'inscrire sur une liste d'adresses électroniques afin d'être informés de l'état d'avancement des travaux et des retards prévus. La municipalité indique clairement qu'il n'y a aucune obligation de participation et demande le consentement des personnes concernées pour pouvoir utiliser leurs adresses électroniques (exclusivement) à cette fin. Les citoyens qui ne donnent pas leur consentement ne seront en aucun cas privés d'un service de base de la municipalité ou de l'exercice d'un quelconque droit, et sont donc libres de donner ou de refuser leur consentement à ce traitement de leurs données. Toutes les informations sur les travaux de voirie seront également disponibles sur le site Internet de la municipalité.

[Exemple 3] Une propriétaire foncière nécessite certains permis de la part de sa municipalité locale et de l'administration provinciale dans laquelle se situe sa municipalité. Les deux entités publiques ont besoin des mêmes informations afin de délivrer ces permis, mais n'ont pas accès à leurs bases de données respectives. Elles demandent donc les mêmes informations à la propriétaire foncière, qui envoie ses données séparément à ces deux entités publiques. La municipalité et l'administration provinciale demandent son consentement pour fusionner leurs dossiers afin d'éviter une duplication des procédures et de la correspondance. Elles lui assurent que c'est entièrement facultatif et que les demandes de permis seront de toute façon traitées séparément si elle décide de ne pas donner son consentement à la fusion de ses données. La propriétaire foncière peut librement donner son consentement aux autorités concernant la fusion des dossiers.

[Exemple 4] Une école publique demande le consentement de ses étudiants pour utiliser leurs photographies dans une revue étudiante imprimée. Le consentement serait ici le fruit d'un véritable choix dès lors que les étudiants ne se verraient pas privés de tout enseignement ou de tout service et pourraient refuser l'utilisation de ces photographies sans aucun préjudice¹⁶.

Un déséquilibre des rapports de force peut également avoir lieu dans le cadre des relations de **travail**¹⁷. Au vu de la dépendance résultant de la relation employeur/employé, il est peu probable que la personne concernée soit en mesure de refuser de donner son consentement à son employeur concernant le traitement de ses données sans craindre ou encourir des conséquences négatives suite à ce refus. Il est ainsi peu probable qu'un employé soit en mesure de répondre librement à une

¹⁵ Voir l'article 6 du RGPD, notamment le paragraphe 1, points c) et e).

¹⁶ Aux fins de cet exemple, une école publique signifie une école financée par l'État ou un établissement scolaire considéré comme une autorité publique ou un organisme public par le droit national.

¹⁷ Voir également l'article 88 du RGPD, qui souligne la nécessité de protéger les intérêts spécifiques des employés et introduit la possibilité de dérogations dans la législation des États membres. Voir également le considérant 155.

demande de consentement de la part de son employeur visant à activer des systèmes de surveillance, tels que des caméras de surveillance, sur le lieu de travail, ou à remplir des formulaires d'évaluation, sans se sentir obligé de consentir¹⁸. Aussi le G29 considère-t-il problématique que les employeurs traitent les données à caractère personnel de leurs employés actuels ou potentiels en se fondant sur leur consentement, dès lors qu'il est peu probable que celui-ci soit donné librement. Pour la majorité de ces traitements de données au travail, la base juridique ne peut et ne devrait pas être le consentement des employés (article 6, paragraphe 1, point a)) en raison de la nature de la relation employeur/employé¹⁹.

Cela ne signifie toutefois pas que les employeurs ne peuvent jamais avoir recours au consentement en tant que base juridique pour le traitement de données. Il peut exister des situations où l'employeur est en mesure de démontrer que le consentement est de facto donné librement. 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 consentement²⁰.

[Exemple 5]

Une équipe de tournage va filmer dans un bureau. L'employeur demande le consentement de tous les employés travaillant dans la zone concernée à être filmés, dès lors qu'ils pourraient apparaître en arrière-plan de la vidéo. Ceux qui ne souhaitent pas être filmés ne sont pénalisés en aucune façon, et disposeront de bureaux équivalents ailleurs dans le bâtiment pendant toute la durée du tournage.

Les déséquilibres de rapports de force ne se limitent pas aux autorités publiques et aux employeurs, ils peuvent également avoir lieu dans d'autres situations. Comme souligné par le G29 dans plusieurs avis, le consentement ne peut être valable que si la personne concernée est véritablement en mesure d'exercer un choix et s'il n'y a pas de risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes (par ex. coûts supplémentaires importants) si elle ne donne pas son consentement. Le consentement ne sera pas libre lorsque tout élément de contrainte, de pression ou d'incapacité d'exercer un véritable choix sera présent.

3.1.2. Conditionnalité

L'article 7, paragraphe 4, du RGPD joue un rôle crucial au moment de déterminer si le consentement est donné librement²¹.

¹⁸ Voir l'avis 15/2011 sur la définition du consentement (WP 187), p. 14-16, l'avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel (WP 48), chapitre 10, le document de travail concernant la surveillance des communications électroniques sur le lieu de travail (WP 55), paragraphe 4.2, et l'avis 2/2017 sur le traitement des données au travail (WP 249), paragraphe 6.2.

¹⁹ Voir l'avis 2/2017 sur le traitement des données au travail, pages 6-7.

²⁰ Voir également l'avis 2/2017 sur le traitement des données au travail, paragraphe 6.2.

²¹ Article 7, paragraphe 4, du RGPD: «*Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si 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 dudit contrat.*» Voir également le considérant 43 du RGPD, qui prévoit que: «*[...] Le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un*

L'article 7, paragraphe 4, du RGPD indique entre autres que le «couplage» du consentement à l'acceptation de conditions générales et la «subordination» de la fourniture d'un contrat ou d'un service à une demande de consentement au traitement de données à caractère personnel non nécessaires à l'exécution dudit contrat ou service ne sont en aucun cas souhaitables. Le consentement est présumé ne pas avoir été donné librement s'il a été donné dans une telle situation (considérant 43). L'article 7, paragraphe 4, cherche à garantir que la finalité du traitement des données à caractère personnel ne soit pas dissimulée ou associée à la fourniture d'un contrat ou d'un service pour lequel ces données à caractère personnel ne sont pas nécessaires. Ce faisant, le RGPD veille à ce que le traitement de données à caractère personnel pour lequel le consentement est sollicité ne puisse pas devenir directement ou indirectement la contre-performance d'un contrat. Ces deux bases juridiques du traitement de données à caractère personnel, à savoir le consentement et le contrat, ne peuvent pas être fusionnées et amalgamées.

L'obligation de consentir au traitement de données à caractère personnel autres que celles strictement nécessaires limite le choix de la personne concernée et fait obstacle au consentement libre. Dès lors que la législation sur la protection des données vise à protéger les droits fondamentaux, le contrôle d'un individu sur ses données à caractère personnel est considéré comme essentiel, et il semble évident que le consentement au traitement de données à caractère personnel non nécessaires ne peut pas être considéré comme une condition sine qua non de l'exécution d'un contrat ou de la fourniture d'un service.

Lorsqu'une demande de consentement est liée à l'exécution d'un contrat par le responsable du traitement, une personne concernée ne souhaitant pas autoriser le traitement de ses données à caractère personnel par le responsable du traitement risque ainsi de voir les services sollicités lui être refusés.

Afin d'évaluer si une telle situation de couplage ou de subordination a lieu, il est important de déterminer le champ d'application du contrat et les données qui seraient nécessaires à l'exécution dudit contrat.

Selon l'avis 06/2014 du G29, la locution «nécessaire à l'exécution d'un contrat» doit être interprétée de façon restrictive. Le traitement doit être nécessaire pour exécuter le contrat conclu avec chacune des personnes concernées. Cela peut par exemple inclure le traitement de l'adresse de la personne concernée afin que des biens achetés en ligne puissent être livrés, ou le traitement des informations de carte de crédit afin de permettre le paiement. Dans le contexte du travail, ce principe peut par exemple autoriser le traitement des informations liées au salaire et au compte bancaire afin de pouvoir verser les salaires²². Il doit exister un lien direct et objectif entre le traitement des données et l'objectif d'exécution du contrat.

contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution.»

²² Pour plus d'informations et d'exemples, voir l'avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, adopté par le G29 le 9 avril 2014, p. 18-19. (WP 217).

Si un responsable du traitement cherche à traiter des données qui sont effectivement nécessaires à l'exécution d'un contrat, le consentement n'est alors pas la base juridique appropriée²³.

L'article 7, paragraphe 4, n'est pertinent que lorsque les données requises ne sont **pas** nécessaires à l'exécution d'un contrat (y compris la fourniture d'un service) et que l'exécution dudit contrat est conditionnée à l'obtention desdites données sur la base du consentement. Inversement, si le traitement **est** nécessaire à l'exécution du contrat (y compris la fourniture d'un service), l'article 7, paragraphe 4, ne s'applique pas.

[Exemple 6]

Une banque demande le consentement de ses clients afin de permettre à de tierces parties d'utiliser leurs informations de paiement à des fins de commercialisation directe. Ce traitement n'est pas nécessaire à l'exécution du contrat avec le client et à la fourniture de services de compte bancaire ordinaires. Si le refus du client de donner son consentement à cette finalité de traitement entraînerait le déni de services bancaires, la fermeture du compte bancaire, ou, selon le cas, une augmentation des frais, le consentement ne peut être donné librement.

Le choix du législateur de souligner, entre autres, la conditionnalité en tant que présomption de l'absence de liberté de consentement démontre qu'il convient d'évaluer soigneusement l'existence d'une telle conditionnalité. La locution «tenir le plus grand compte» utilisée dans l'article 7, paragraphe 4, suggère que le responsable du traitement doit être particulièrement prudent lorsqu'un contrat (qui pourrait inclure la fourniture d'un service) intègre une sollicitation de consentement au traitement de données à caractère personnel.

Dès lors que la formulation de l'article 7, paragraphe 4, n'est pas absolue, il pourrait exister un nombre très limité de cas où cette conditionnalité ne rendrait pas le consentement non valable. Toutefois, le terme «préssumé» du considérant 43 indique clairement que de tels cas seront hautement exceptionnels.

En tout état de cause, la charge de la preuve repose sur le responsable du traitement en vertu de l'article 7, paragraphe 4²⁴. Cette règle spécifique reflète le principe général de responsabilité omniprésent dans le RGPD. Toutefois, lorsque l'article 7, paragraphe 4, s'applique, il sera plus difficile pour le responsable du traitement de prouver que le consentement a été donné librement par la personne concernée²⁵.

²³ La base juridique appropriée pourrait alors être l'article 6, paragraphe 1, point b) (contrat).

²⁴ Voir également l'article 7, paragraphe 1, du RGPD qui stipule que le responsable du traitement doit démontrer que le consentement de la personne concernée a été donné librement.

²⁵ Dans une certaine mesure, l'introduction de ce paragraphe est une codification des orientations existantes du G29. Comme décrit dans l'avis 15/2011, lorsqu'une personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement – en raison de la nature de la relation ou de circonstances particulières – l'on peut être porté à croire que la liberté de consentement est limitée (par ex. dans une relation de travail ou si la collecte des données est effectuée par une autorité publique). Avec l'entrée en vigueur de l'article 7, paragraphe 4, il sera plus difficile pour le responsable du traitement de prouver que le consentement a été donné librement par la personne concernée. Cf. avis 15/2011 sur la définition du consentement (WP 187), p. 14-18.

Le responsable du traitement pourrait avancer que son organisation offre un véritable choix aux personnes concernées si celles-ci peuvent choisir entre un service qui inclut le consentement à l'utilisation de données à caractère personnel à des fins complémentaires et un service équivalent proposé par le même responsable du traitement n'impliquant pas de consentir au traitement de données à caractère personnel à des fins complémentaires. Dans la mesure où il existe la possibilité que le responsable du traitement exécute le contrat ou fournisse le service sans que la personne concernée ne consente aux autres utilisations des données en question, le service n'est pas conditionné. Les deux services doivent cependant être réellement équivalents.

Le G29 considère que le consentement ne peut pas être considéré comme donné librement si un responsable du traitement avance qu'il existe un choix entre son service comprenant le consentement à l'utilisation de données à caractère personnel à des fins complémentaires et un service équivalent proposé par un autre responsable du traitement. Dans un tel cas, la liberté de choix dépendrait de ce que d'autres acteurs du marché font et de si la personne concernée trouve les services de l'autre responsable du traitement réellement équivalents. Cela impliquerait en outre une obligation pour les responsables du traitement de surveiller l'évolution du marché afin de s'assurer que le consentement à leurs activités de traitement est toujours valable, dès lors qu'un concurrent pourrait modifier ultérieurement ses services. Aussi le recours à cet argument implique-t-il que le consentement n'est pas conforme au RGPD.

3.1.3. Nécessité de détailler le consentement

Un service peut impliquer de multiples opérations de traitement à différentes fins. Dans de tels cas, les personnes concernées devraient être libres de choisir quelles finalités elles acceptent, plutôt que de devoir consentir à un ensemble de finalités de traitement. En vertu du RGPD, plusieurs consentements pourraient être nécessaires avant de pouvoir fournir un service dans un cas donné.

Le considérant 43 précise que le consentement est présumé ne pas avoir été donné librement si le processus/la procédure d'obtention du consentement ne permet pas aux personnes concernées de donner un consentement distinct à différentes opérations de traitement des données à caractère personnel (par ex. uniquement pour certaines opérations de traitement et pas pour d'autres) bien que cela soit approprié dans le cas d'espèce. Le considérant 32 stipule que *«Le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles»*.

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. Cette nécessité de détailler le consentement est étroitement liée à la nécessité que le consentement soit spécifique, comme décrit à la rubrique 3.2 ci-après. Afin de se conformer aux conditions d'obtention d'un consentement valable lorsque le traitement des données est effectué pour différentes finalités, il convient de détailler le consentement, c.-à-d. de différencier ses différentes finalités et d'obtenir un consentement pour chacune d'entre elles.

[Exemple 7]

Dans la même demande de consentement, un détaillant demande le consentement de ses clients à l'utilisation de leurs données afin de leur envoyer des communications commerciales par courrier électronique et de

partager leurs informations avec d'autres entreprises au sein du même groupe. Ce consentement n'est pas détaillé dès lors qu'il n'y a pas de consentement différencié pour ces deux finalités distinctes et le consentement ne sera donc pas valable. Dans ce cas, un consentement spécifique devrait être obtenu pour envoyer les coordonnées de la personne concernée aux partenaires commerciaux. Un tel consentement spécifique sera jugé valable pour chaque partenaire (voir également la rubrique 3.3.1) dont l'identité a été fournie à la personne concernée au moment de l'obtention de son consentement, à condition que les données leur soient envoyées pour la même finalité (dans cet exemple: une finalité commerciale).

3.1.4. Préjudice

Le responsable du traitement doit démontrer qu'il est possible de refuser ou de retirer son consentement sans subir de préjudice (considérant 42). Par exemple, le responsable du traitement doit prouver que le retrait du consentement n'engendre pas de frais pour la personne concernée et qu'il n'y a donc pas de désavantage évident pour ceux qui retirent leur consentement.

D'autres exemples de préjudice sont la tromperie, l'intimidation, la coercition ou toute conséquence négative importante si la personne concernée refuse de donner son consentement. Le responsable du traitement devrait être en mesure de prouver que la personne concernée dispose d'une véritable liberté de choix concernant la décision de donner ou non son consentement et qu'il est possible de retirer son consentement sans subir de préjudice.

Si un responsable du traitement est en mesure de démontrer qu'un service inclut la possibilité de retirer son consentement sans subir de conséquences négatives, c'est-à-dire sans que la qualité du service ne soit amoindrie au détriment de l'utilisateur, cela peut constituer la preuve que le consentement a été donné librement. Le RGPD n'exclut pas tous les incitants, mais il appartiendra au responsable du traitement de démontrer que le consentement a bien été donné librement en toutes circonstances.

[Exemple 8]

Lorsqu'une utilisatrice télécharge une application mobile de la catégorie «mode de vie», celle-ci sollicite son consentement pour accéder à l'accéléromètre du téléphone. Cet accès n'est pas nécessaire au fonctionnement de l'application, mais est utile pour le responsable du traitement qui souhaite en savoir plus sur les mouvements et les niveaux d'activité de ses utilisateurs. Lorsque l'utilisatrice retire ultérieurement son consentement, elle découvre que l'application ne fonctionne plus que de manière restreinte. Il s'agit d'un exemple de préjudice au sens du considérant 42, ce qui signifie que le consentement n'a jamais été obtenu de façon valable (et le responsable doit de ce fait supprimer toutes les données à caractère personnel concernant les mouvements des utilisateurs collectées de cette manière).

[Exemple 9]

Une personne concernée s'inscrit à un bulletin d'informations d'une enseigne de mode avec des réductions générales. Le détaillant demande le consentement de la personne concernée pour collecter davantage de données sur ses préférences en matière de shopping afin d'adapter ses offres à ses préférences en fonction de son historique d'achat ou d'un questionnaire rempli sur une base volontaire. Si la personne concernée retire ultérieurement son consentement, elle recevra à nouveau des réductions non personnalisées. Il ne s'agit pas ici d'un préjudice, dès lors que seul l'incitant autorisé aura été perdu.

[Exemple 10]

Une revue de mode donne la possibilité à ses lecteurs d'acheter de nouveaux produits de maquillage avant leur lancement officiel.

Les produits seront bientôt disponibles sur le marché, mais les lecteurs de cette revue bénéficient d'une avant-première exclusive sur ces produits. Afin de profiter de cet avantage, les lecteurs doivent donner leur adresse postale et consentir à leur inscription sur la liste de diffusion de la revue. L'adresse postale est nécessaire pour l'expédition et la liste de diffusion est utilisée pour l'envoi d'offres commerciales pour des produits tels que des cosmétiques ou des t-shirts tout au long de l'année.

L'entreprise explique que les données sur la liste de diffusion ne seront utilisées que pour l'envoi de produits et de dépliants publicitaires par la revue elle-même et ne seront en aucun cas partagées avec d'autres organisations.

Si le lecteur ne souhaite pas révéler son adresse à cette fin, il ne subira aucun préjudice dès lors que les produits lui seront toujours accessibles.

3.2. Spécifique

L'article 6, paragraphe 1, point a), confirme que le consentement de la personne concernée doit être donné en lien avec «une ou plusieurs finalités spécifiques» et que la personne concernée a un choix concernant chacune de ces finalités²⁶. L'exigence selon laquelle le consentement doit être «spécifique» vise à garantir un certain degré de contrôle utilisateur et de transparence pour la personne concernée. Cette exigence n'a pas été modifiée par le RGPD et reste étroitement liée à l'exigence selon laquelle le consentement doit être «éclairé». Parallèlement, elle doit être interprétée conformément à l'exigence selon laquelle le consentement doit être «détaillé» pour être considéré comme étant «libre»²⁷. Pour résumer, afin de se conformer au caractère «spécifique» du consentement, le responsable du traitement doit garantir:

- (i) la spécification des finalités en tant que garantie contre tout détournement d'usage,
- (ii) le caractère détaillé des demandes de consentement, et
- (iii) la séparation claire des informations liées à l'obtention du consentement au traitement des données et des informations concernant d'autres sujets.

Ad. i): Conformément à l'article 5, paragraphe 1, point b), du RGPD, l'obtention d'un consentement valable est toujours précédée de la détermination d'une finalité déterminée, explicite et légitime pour l'activité de traitement envisagée²⁸. Combinée à la notion de limitation de la finalité de l'article 5, paragraphe 1, point b), la nécessité d'obtenir un consentement spécifique sert de garantie contre l'élargissement ou l'estompement progressif des fins auxquelles les données sont traitées après qu'une personne concernée a donné son consentement à la collecte initiale de ses données. Ce phénomène, également connu sous le terme de détournement d'usage, constitue un risque pour les personnes concernées dès lors qu'il peut entraîner une utilisation imprévue de leurs données à caractère personnel par le responsable du traitement ou par de tierces parties ainsi que l'affaiblissement du contrôle exercé par la personne concernée.

²⁶ Des orientations complémentaires concernant la détermination des «finalités» peuvent être trouvées dans l'avis 3/2013 sur la limitation de la finalité (WP 203).

²⁷ Le considérant 43 du RGPD prévoit qu'un consentement distinct pour différentes opérations de traitement sera nécessaire chaque fois que cela est approprié. Des possibilités de consentement détaillé devraient être prévues afin de permettre aux personnes concernées de donner un consentement distinct à des fins distinctes.

²⁸ Voir l'avis 3/2013 du G29 sur la limitation de la finalité (WP 203), p. 16: «Pour ces raisons, les finalités vagues ou générales, telles que des fins d'«amélioration de l'expérience utilisateur», des «fins commerciales», des «fins de sécurité informatique» ou des fins de «recherches futures», ne satisferont généralement pas – si pas davantage détaillées – au critère d'être «spécifiques».»

Si le responsable du traitement se fonde sur l'article 6, paragraphe 1, point a), la personne concernée doit toujours donner son consentement pour une finalité de traitement spécifique²⁹. Conformément au concept de *limitation de la finalité*, à l'article 5, paragraphe 1, point b) et au considérant 32, le consentement peut couvrir différentes opérations dans la mesure où ces opérations partagent la même finalité. Il va sans dire qu'un consentement spécifique ne peut être obtenu que lorsque les personnes concernées sont spécifiquement informées des finalités prévues du traitement des données les concernant.

Sans préjudice des dispositions relatives à la compatibilité des finalités, le consentement doit être spécifique à la finalité. Les personnes concernées donneront leur consentement en sachant qu'elles en possèdent le contrôle et que leurs données ne seront traitées qu'à ces fins spécifiques. Si un responsable du traitement traite des données en se fondant sur le consentement et souhaite traiter les données à une autre finalité, il doit solliciter un consentement complémentaire pour cette autre finalité à moins qu'une autre base juridique ne reflète mieux la situation.

[Exemple 11] Un réseau de télévision par câble collecte les données à caractère personnel de ses abonnés en se fondant sur leur consentement afin de leur proposer, en fonction de leurs habitudes de visionnement, des suggestions personnalisées de nouveaux films qui pourraient les intéresser. Après un certain temps, le réseau décide qu'il souhaiterait permettre à de tierces parties d'envoyer (ou d'afficher) des publicités ciblées en fonction des habitudes de visionnement des abonnés. Au vu de cette nouvelle finalité, un nouveau consentement sera nécessaire.

Ad. ii): Les mécanismes de consentement ne doivent pas être détaillés uniquement afin de satisfaire à l'exigence selon laquelle le consentement doit être «libre», mais également à l'exigence selon laquelle il doit être «spécifique». Cela signifie qu'un responsable du traitement qui sollicite le consentement pour diverses finalités spécifiques devrait prévoir un consentement distinct pour chaque finalité afin que les utilisateurs puissent donner un consentement spécifique à des finalités spécifiques.

Ad. iii): Enfin, le responsable des données devrait accompagner chacune des demandes de consentement distinctes d'informations spécifiques concernant les données traitées pour chaque finalité afin que les personnes concernées soient conscientes de l'incidence de leur choix. Les personnes concernées pourront ainsi donner leur consentement spécifique. Cette problématique est liée à l'exigence selon laquelle les responsables du traitement doivent fournir des informations claires, telle que décrite à la rubrique 3.3 ci-après.

3.3. Éclairée

Le RGPD renforce l'exigence selon laquelle le consentement doit être éclairé. Conformément à l'article 5 du RGPD, l'exigence de transparence, étroitement liée aux principes de loyauté et de licéité, en est l'un des principes fondamentaux. Fournir des informations aux personnes concernées avant d'obtenir leur consentement est indispensable afin de leur permettre de prendre des décisions en toute connaissance de cause, de comprendre ce à quoi ils consentent et, par exemple, d'exercer leur droit de retirer leur consentement. Si le responsable du traitement ne fournit pas d'informations

²⁹ Ceci est conforme à l'avis 15/2011 du G29 sur la définition du consentement (WP 187), par exemple p. 19.

accessibles, le contrôle utilisateur devient illusoire et le consentement ne constituera pas une base valable pour le traitement.

Si un responsable du traitement ne respecte pas les exigences relatives à l'obtention d'un consentement éclairé, ce consentement ne sera pas valable et ledit responsable du traitement pourrait se trouver dans une situation d'infraction à l'article 6 du RGPD.

3.3.1. Exigences minimales de contenu pour que le consentement soit «éclairé»

Pour que le consentement soit éclairé, il est nécessaire d'informer la personne concernée de certains éléments cruciaux pour opérer un choix. Aussi le G29 est-il d'avis qu'au moins les informations suivantes sont nécessaires afin d'obtenir un consentement valable:

- (i) l'identité du responsable du traitement,³⁰
- (ii) la finalité de chacune des opérations de traitement pour lesquelles le consentement est sollicité³¹,
- (iii) les (types de) données collectées et utilisées,³²
- (iv) l'existence du droit de retirer son consentement³³,
- (v) des informations concernant l'utilisation des données pour la prise de décision automatisée conformément à l'article 22, paragraphe 2, point c)³⁴, le cas échéant, et
- (vi) des informations sur les risques éventuels liés à la transmission des données en raison de l'absence de décision d'adéquation et de garanties appropriées telles que décrites à l'article 46³⁵.

Concernant les points (i) et (iii), le G29 signale que si le consentement sollicité servira de base à plusieurs responsables (conjoints) du traitement ou si les données seront transférées à, ou traitées par, d'autres responsables qui souhaitent se fonder sur le consentement original, ces organisations devraient toutes être nommées. Les sous-traitants ne doivent pas impérativement être nommés en vertu des exigences en matière de consentement, bien que pour se conformer aux articles 13 et 14 du RGPD, les responsables du traitement devront fournir une liste complète des destinataires ou des catégories de destinataires, y compris des sous-traitants. Pour conclure, le G29 signale qu'en fonction des circonstances et du contexte de chaque cas, plus d'informations peuvent être nécessaires afin que la personne concernée puisse réellement comprendre les opérations de traitement envisagées.

3.3.2. Comment fournir des informations

³⁰ Voir également le considérant 42 du RGPD: «[...] Pour que le consentement soit éclairé, la personne concernée devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel. [...]».

³¹ Voir à nouveau le considérant 42 du RGPD.

³² Voir également l'avis 15/2011 du G29 sur la définition du consentement (WP 187), p. 21-22.

³³ Voir l'article 7, paragraphe 3, du RGPD.

³⁴ Voir également les lignes directrices du G29 sur les décisions individuelles automatisées et le profilage au titre du règlement 2016/679 (WP 251), paragraphe IV.B, p. 20 et suivantes.

³⁵ Conformément à l'article 49, paragraphe 1, point a), des informations spécifiques relatives à l'absence des garanties décrites à l'article 46 sont requises lorsqu'un consentement explicite est sollicité. Voir également l'avis 15/2011 du G29 sur la définition du consentement (WP 187), p. 21.

Le RGPD ne stipule pas la forme sous laquelle les informations doivent être fournies afin de satisfaire à l'exigence du consentement éclairé. Cela signifie que les informations valables peuvent être présentées de diverses façons, par exemple sous la forme de communications écrites ou verbales ou de messages audio ou vidéo. Le RGPD fixe toutefois différentes exigences en matière de consentement éclairé, notamment dans son article 7, paragraphe 2, et dans son considérant 32. Cela entraîne une amélioration du niveau de clarté et d'accessibilité des informations.

En 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. Les responsables du traitement ne peuvent pas utiliser de longues politiques de confidentialité difficiles à comprendre ou des énoncés riches en jargon juridique. Le consentement doit être clair et se distinguer des autres questions, et doit être présenté sous une forme compréhensible et aisément accessible. Cette exigence signifie essentiellement que les informations nécessaires à une prise de décision éclairée concernant le consentement ne peuvent être cachées dans des conditions générales³⁶.

Un responsable du traitement doit s'assurer que le consentement est fourni sur la base d'informations qui permettent aux personnes concernées d'identifier facilement qui est le responsable des données et de comprendre ce à quoi elles consentent. Le responsable du traitement doit clairement décrire la finalité du traitement des données pour lequel le consentement est sollicité³⁷.

D'autres orientations spécifiques sur l'accessibilité ont été fournies dans les lignes directrices du G29 sur la transparence. Si le consentement doit être donné par voie électronique, la sollicitation doit être claire et concise. Des informations superposées ou détaillées peuvent être un moyen adéquat de gérer la double obligation que celles-ci soient précises et complètes d'un côté, et compréhensibles d'un autre.

Un responsable du traitement doit évaluer quel type de public fournit des données à caractère personnel à son organisation. Par exemple, si le public cible comprend des mineurs, il convient que le responsable du traitement s'assure que les informations soient compréhensibles pour ceux-ci³⁸. Après avoir identifié leur public, les responsables du traitement doivent déterminer quelles informations devraient être fournies et, consécutivement, comment lesdites informations seront présentées aux personnes concernées.

L'article 7, paragraphe 2, traite des déclarations de consentement écrites préformulées concernant également d'autres questions. Lorsque le consentement est requis dans le cadre d'un contrat (papier), la demande de consentement devrait être présentée sous une forme qui la distingue clairement des autres questions. Si le contrat papier comprend de nombreux aspects qui ne sont pas

³⁶ La déclaration de consentement doit être désignée comme telle. Les énoncés de type «Je suis conscient(e) que...» ne satisfont pas à l'exigence selon laquelle les termes utilisés doivent être clairs.

³⁷ Voir l'article 4, paragraphe 11, et l'article 7, paragraphe 2, du RGPD.

³⁸ Voir également le considérant 58 concernant les informations compréhensibles pour les enfants.

liés à la question du consentement à l'utilisation de données à caractère personnel, la question du consentement devrait être traitée sous une forme qui se distingue clairement, ou dans le cadre d'un document distinct. De même, si le consentement est sollicité par voie électronique, la demande de consentement doit être séparée et distincte, elle ne peut être simplement un paragraphe dans les conditions générales, conformément au considérant 32³⁹. Afin de s'adapter à de petits écrans ou à des situations où il y a peu d'espace pour les informations, une présentation superposée des informations peut être envisagée, le cas échéant, afin d'éviter toute perturbation excessive de l'expérience utilisateur ou de la conception du produit.

Un responsable du traitement qui se fonde sur le consentement de la personne concernée doit également respecter les différentes obligations en matière d'information énoncées aux articles 13 et 14 afin d'être conforme au RGPD. En pratique, le respect des obligations en matière d'information et de l'exigence selon laquelle le consentement doit être éclairé pourrait entraîner une approche intégrée dans de nombreux cas. Toutefois, cette rubrique est rédigée étant entendu qu'un consentement «éclairé» valable est possible même lorsque tous les éléments des articles 13 et/ou 14 ne sont pas mentionnés lors du processus d'obtention du consentement (ces points devraient bien évidemment être mentionnés ailleurs, par exemple dans l'avis de confidentialité d'une entreprise). Le G29 a publié d'autres lignes directrices sur l'exigence de la transparence.

[Exemple 12]

L'entreprise X est un responsable du traitement qui a reçu des plaintes concernant le manque de clarté des finalités du traitement des données pour lesquelles le consentement a été demandé aux personnes concernées. L'entreprise considère nécessaire de vérifier si les informations de sa demande de consentement sont compréhensibles pour les personnes concernées. X organise des panels volontaires constitués de catégories spécifiques de clients et présente de nouvelles mises à jour de ses informations de consentement à ces audiences tests avant de les communiquer à l'extérieur. La sélection du panel respecte le principe d'indépendance et se fait sur la base de critères assurant un résultat représentatif et non biaisé. Les membres du panel reçoivent un questionnaire et indiquent ce qu'ils ont compris de ces informations et comment ils les évalueraient sur les plans de l'intelligibilité et de la pertinence. Le responsable du traitement poursuit ces tests jusqu'à ce que le panel indique que les informations sont compréhensibles. X établit un rapport du test et le tient à disposition à des fins de référence ultérieure. Cet exemple montre l'une des possibilités dont dispose X pour démontrer que les personnes concernées reçoivent des informations claires avant de consentir au traitement de leurs données à caractère personnel par ses soins.

[Exemple 13]

Une entreprise procède au traitement de données en se fondant sur le consentement. L'entreprise utilise un avis de confidentialité superposé qui inclut une demande de consentement. L'entreprise communique toutes les informations de base concernant le responsable du traitement et les activités de traitement des données envisagées⁴⁰. Toutefois, l'entreprise n'indique pas comment son délégué à la protection des données peut être contacté dans le premier niveau d'informations de son avis de confidentialité. Afin de disposer d'une base

³⁹ Voir également le considérant 42 et la directive 93/13/CE, notamment son article 5 (termes clairs et compréhensibles et en cas de doute, l'interprétation la plus favorable au consommateur prévaudra) et son article 6 (invalidité des clauses abusives, le contrat continue à exister sans ces clauses s'il reste pertinent, faute de quoi le contrat ne sera plus valable).

⁴⁰ Il convient de noter que lorsque l'identité du responsable du traitement ou les finalités du traitement ne sont pas apparentes dans le premier niveau d'informations de l'avis de confidentialité superposé (et se trouvent dans des niveaux inférieurs), il sera difficile pour le responsable du traitement de démontrer que la personne concernée a donné un consentement éclairé, à moins que le responsable du traitement ne soit en mesure de démontrer que la personne concernée en question a accédé à ces informations avant de donner son consentement.

juridique valable au sens de l'article 6, ce responsable du traitement a obtenu un consentement «éclairé» valable, même si les coordonnées du délégué à la protection des données n'ont pas été communiquées à la personne concernée (dans le premier niveau d'informations) conformément à l'article 13, paragraphe 1, point b) ou à l'article 14, paragraphe 1, point b) du RGPD.

3.4. Univoque

Le RGPD établit clairement que le consentement nécessite une déclaration de la part de la personne concernée ou un acte positif clair, ce qui signifie qu'il doit toujours être donné par une déclaration ou un geste actif. Il doit être évident que la personne concernée a consenti au traitement en question.

L'article 2, point h), de la directive 95/46/CE décrit le consentement comme une «manifestation de volonté par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement». L'article 4, paragraphe 11, du RGPD développe cette définition en précisant qu'un consentement valable nécessite une manifestation de volonté *univoque*, par une *déclaration ou par un acte positif clair*, conformément à de précédentes orientations publiées par le G29.

Un «acte positif clair» signifie que la personne concernée doit avoir posé un acte délibéré afin de donner son consentement au traitement spécifique⁴¹. Le considérant 32 établit des orientations complémentaires à cet égard. Le consentement peut être recueilli au moyen d'une déclaration écrite ou orale (enregistrée), y compris par voie électronique.

Peut-être la façon la plus littérale de satisfaire au critère d'une «déclaration écrite» est-elle de s'assurer que la personne concernée rédige une lettre ou un courrier électronique expliquant au responsable du traitement ce à quoi elle consent. Cela est cependant rarement réaliste. Les déclarations écrites peuvent adopter de nombreuses tailles et formes qui pourraient être conformes au RGPD.

Sans préjudice du droit des contrats (national) existant, le consentement peut être obtenu moyennant une déclaration orale enregistrée, bien qu'il convienne que la personne concernée ait pris bonne note des informations à sa disposition avant sa déclaration de consentement. 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.

⁴¹ Voir le document de travail des services de la Commission, analyse d'impact, annexe 2, p. 20 et p. 105-106: «*Comme le souligne également l'avis du G29 sur le consentement, il semble essentiel de préciser que l'obtention d'un consentement valable impose de recourir à des mécanismes qui ne laissent aucun doute sur l'intention de la personne concernée de consentir au traitement, tout en expliquant que – dans le contexte de l'environnement en ligne – l'utilisation d'options par défaut, que la personne concernée doit modifier pour refuser le traitement («consentement fondé sur le silence»), ne constitue pas, en soi, un consentement indubitable. Cela conférerait aux individus un plus grand contrôle sur leurs propres données lorsque le traitement est fondé sur leur consentement. Quant à l'incidence sur le responsable du traitement, celle-ci serait faible dès lors que cette mesure ne fait que clarifier et expliciter les implications de l'actuelle directive concernant les conditions d'un consentement valable de la part de la personne concernée. Dans la mesure où la notion de consentement «explicite» clarifierait – en remplaçant la notion de consentement «indubitable» – les modalités et la qualité du consentement et où elle ne vise pas à accroître le nombre de cas et de situations où le consentement (explicite) devrait être utilisé comme base du traitement, l'incidence de cette mesure sur les responsables du traitement ne devrait pas être majeure.»*

[Exemple 14]

Lors de l'installation d'un logiciel, celui-ci demande le consentement de la personne concernée afin d'utiliser des rapports d'erreur non anonymes afin d'améliorer le logiciel. Un avis de confidentialité superposé fournissant les informations nécessaires accompagne la demande de consentement. En cochant activement la case stipulant «Je consens», l'utilisateur est en mesure de poser un «acte positif clair» afin de donner son consentement au traitement.

Un responsable du traitement doit également être conscient que le consentement ne peut être obtenu moyennant la même action que lorsqu'une personne concernée accepte un contrat ou les conditions générales d'un service. L'acceptation globale des conditions générales ne peut être considérée comme un acte positif clair visant à donner son consentement à l'utilisation de données à caractère personnel. Le RGPD n'autorise pas les responsables du traitement à proposer des cases cochées par défaut ou des options de refus nécessitant une action de la personne concernée pour signaler son refus (par exemple des «cases de refus»)⁴².

Lorsque le consentement est donné à la suite d'une demande introduite par voie électronique, la demande de consentement ne devrait pas *inutilement* perturber l'utilisation du service pour lequel il est accordé⁴³. Un acte positif clair par lequel une personne concernée donne son consentement peut être nécessaire lorsqu'une méthode moins perturbante ou dérangeante entraînerait une certaine ambiguïté. Il peut ainsi être nécessaire qu'une demande de consentement interrompe l'expérience d'utilisation jusqu'à un certain point afin que cette demande soit effective.

Toutefois, les responsables du traitement conservent la liberté de développer un mode de consentement qui convienne à leur organisation dans le respect des exigences du RGPD. À cet égard, les mouvements physiques peuvent être qualifiés d'actes positifs clairs conformes au RGPD.

Les responsables du traitement devraient élaborer des mécanismes de consentement clairs pour les personnes concernées. Ils doivent éviter toute ambiguïté et s'assurer que l'acte par lequel le consentement est accordé puisse se distinguer de tout autre acte. Aussi la simple poursuite de l'utilisation ordinaire d'un site Internet n'est-elle pas un comportement qui permet de supposer une manifestation de volonté de la part de la personne concernée visant à donner son accord à une opération de traitement envisagée.

[Exemple 15]

Faire glisser une barre sur un écran, agiter la main devant une caméra intelligente, faire tourner un smartphone dans le sens des aiguilles d'une montre ou pour former un huit sont différentes possibilités permettant d'indiquer son consentement, pour autant que des informations claires soient fournies et qu'il soit clair que le mouvement en question signifie que la personne concernée accepte une demande spécifique (par ex. «En faisant glisser cette barre vers la gauche, vous consentez à l'utilisation de l'information X à une fin Y. Veuillez répéter le mouvement pour confirmer»). Le responsable du traitement doit être en mesure de démontrer que le consentement a été obtenu de cette façon et les personnes concernées doivent être en mesure de retirer leur consentement aussi facilement qu'elles l'ont donné.

⁴² Voir l'article 7, paragraphe 2. Voir également le document de travail n° 02/2013 sur le recueil du consentement pour le dépôt de cookies (WP 208), p. 4-7.

⁴³ Voir le considérant 32 du RGPD.

[Exemple 16]

Faire défiler une page ou naviguer sur un site Internet ne satisfait pas à l'exigence d'un acte positif clair. La raison en est que la notification indiquant qu'en continuant à faire défiler la page, l'utilisateur donne son consentement peut être difficile à distinguer et/ou peut être manquée lorsqu'une personne concernée fait rapidement défiler de longs textes, et qu'une telle action n'est pas suffisamment univoque.

Dans le contexte numérique, de nombreux services nécessitent des données à caractère personnel afin de fonctionner. Les utilisateurs reçoivent ainsi chaque jour de nombreuses demandes de consentement auxquelles elles doivent répondre par un clic ou en balayant leur écran. Cela peut mener à une certaine lassitude: lorsque trop souvent rencontré, l'effet d'avertissement des mécanismes de consentement diminue.

Il en résulte une situation où les informations de consentement cessent d'être lues. Cela constitue un grand risque pour les personnes concernées, dès lors que le consentement est généralement demandé pour des actions qui seraient illicites sans ce consentement. Le RGPD impose aux responsables du traitement de développer des solutions à ce problème.

Un exemple fréquemment mentionné de solution à ce problème dans un environnement en ligne est l'obtention du consentement des utilisateurs d'Internet moyennant les paramètres de leur navigateur. De tels paramètres devraient être développés conformément aux conditions d'un consentement valable établies par le RGPD, telles que la nécessité que le consentement soit distinct pour chacune des finalités envisagées et que les informations fournies nomment les responsables du traitement.

En tout état de cause, le consentement doit toujours être obtenu avant que le responsable du traitement ne commence à traiter les données à caractère personnel pour lesquelles un consentement est nécessaire. Le G29 a à maintes reprises considéré dans ses avis précédents que le consentement devrait être donné préalablement à l'activité de traitement⁴⁴. Bien que le RGPD n'indique pas littéralement dans son article 4, paragraphe 11, que le consentement doit être donné préalablement à l'activité de traitement, il le laisse cependant clairement entendre. Le titre de l'article 6, paragraphe 1, et la formule «a consenti» utilisée dans l'article 6, paragraphe 1, point a), étayent cette interprétation. Il ressort logiquement de l'article 6 et du considérant 40 qu'une base juridique valable doit exister avant le début du traitement des données. Le consentement devrait donc être donné préalablement à l'activité de traitement. En principe, il peut être suffisant de ne demander le consentement de la personne concernée qu'une seule fois. Les responsables du traitement doivent toutefois obtenir un nouveau consentement spécifique si les finalités du traitement des données changent après l'obtention du consentement ou si une finalité supplémentaire est envisagée.

4. Obtention d'un consentement explicite

Le consentement explicite est requis dans certaines situations où un risque sérieux lié à la protection des données survient, et où un niveau élevé de contrôle sur les données à caractère personnel par la

⁴⁴ Le G29 a constamment défendu cette position depuis son avis 15/2011 sur la définition du consentement (WP 187), p. 34-36.

personne concernée est de ce fait jugé approprié. En vertu du RGPD, le consentement explicite joue un rôle dans l'article 9 relatif au traitement portant sur des catégories particulières de données, dans les dispositions relatives aux transferts de données vers des pays tiers ou des organisations internationales de l'article 49⁴⁵ ainsi que dans l'article 22 sur la décision individuelle automatisée, y compris le profilage⁴⁶.

Le RGPD stipule qu'une «déclaration ou un acte positif clair» est une condition *sine qua non* d'un consentement «standard». Dès lors que les exigences pour un consentement «standard» dans le RGPD sont déjà portées à un niveau supérieur à celles de la directive 95/46/CE, il convient de préciser quels efforts complémentaires un responsable du traitement devrait entreprendre afin d'obtenir le consentement *explicite* d'une personne concernée conformément au RGPD.

Le terme *explicite* se rapporte à la façon dont le consentement est exprimé par la personne concernée. Il implique que la personne concernée doit formuler une déclaration de consentement exprès. Une manière évidente de s'assurer que le consentement est explicite serait de confirmer expressément le consentement dans une déclaration écrite. Le cas échéant, le responsable du traitement pourrait s'assurer que la déclaration écrite est signée par la personne concernée afin de prévenir tout doute potentiel et toute absence potentielle de preuve à l'avenir⁴⁷.

Une telle déclaration signée n'est toutefois pas la seule façon d'obtenir le consentement explicite, et on ne peut affirmer que le RGPD préconise des déclarations écrites et signées dans toutes les situations où un consentement explicite valable est nécessaire. Par exemple, dans un contexte numérique ou en ligne, une personne concernée peut être en mesure de fournir la déclaration nécessaire en remplissant un formulaire électronique, en envoyant un courrier électronique, en téléchargeant un document scanné porteur de la signature de la personne concernée ou en utilisant une signature électronique. En théorie, le recours à des déclarations orales peut également être suffisamment explicite pour que le consentement soit valable, bien qu'il puisse être difficile pour le responsable du traitement de prouver que toutes les conditions d'un consentement explicite valable étaient remplies lorsque la déclaration a été enregistrée.

Une organisation peut également obtenir un consentement explicite moyennant une conversation téléphonique, à condition que les informations relatives au choix soient loyales, compréhensibles et

⁴⁵ Selon l'article 49, paragraphe 1, point a), du RGPD, un consentement explicite peut lever l'interdiction portant sur les transferts de données vers des pays ne disposant pas d'un niveau adéquat de droit relatif à la protection des données. Voir également le document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive

95/46/CE du 24 octobre 1995 (WP 114), p. 13, où le G29 a indiqué que le recours au consentement pour les transferts de données périodiques ou permanents n'est pas approprié.

⁴⁶ Dans son article 22, le RGPD introduit des dispositions visant à protéger les personnes concernées contre les prises de décision uniquement fondées sur un traitement automatisé, y compris le profilage. Les décisions prises sur cette base sont autorisées sous certaines conditions légales. Le consentement joue un rôle clé dans ce mécanisme de protection, dès lors que l'article 22, paragraphe 2, point c) du RGPD stipule clairement qu'un responsable du traitement peut procéder à des prises de décision automatisées, y compris à un profilage, qui pourraient affecter la personne concernée de manière significative s'il dispose du consentement explicite de celle-ci. Le G29 a publié d'autres lignes directrices à cet égard: lignes directrices du G29 sur les décisions individuelles automatisées et le profilage au titre du règlement 2016/679 du G29, 3 octobre 2017 (WP 251).

⁴⁷ Voir également l'avis 15/2011 du G29 sur la définition du consentement (WP 187), p. 28.

claires et qu'elle demande une confirmation spécifique de la part de la personne concernée (par ex. appuyer sur un bouton ou donner une conformation orale).

[Exemple 17] Un responsable du traitement peut également obtenir le consentement explicite d'un visiteur de son site Internet en affichant un écran de consentement explicite qui contient des cases à cocher avec les mentions «Oui» et «Non», à condition que le texte indique clairement qu'il s'agit d'un consentement, par exemple moyennant une formulation telle que «Je consens par la présente au traitement de mes données» et non «Je suis conscient(e) que mes données seront traitées». Il va sans dire que les conditions d'obtention d'un consentement éclairé ainsi que les autres conditions d'obtention d'un consentement valable doivent être satisfaites.

[Exemple 18] Une clinique de chirurgie esthétique demande le consentement explicite d'un patient afin de transférer son dossier médical à un expert consulté dans le but d'obtenir une deuxième opinion sur l'état du patient. Le dossier médical se présente sous la forme d'un fichier numérique. Au vu de la nature spécifique des informations concernées, la clinique demande la signature électronique de la personne concernée afin d'obtenir un consentement explicite valable et d'être en mesure de démontrer qu'un consentement valable a été obtenu⁴⁸.

Une vérification en deux étapes du consentement peut également être une façon de s'assurer que le consentement explicite est valable. Par exemple, une personne concernée reçoit un courrier électronique l'informant de l'intention du responsable du traitement de traiter un dossier contenant des informations médicales. Le responsable du traitement explique dans le courrier électronique qu'il lui demande son consentement pour utiliser un ensemble spécifique d'informations à une fin spécifique. Si la personne concernée consent à l'utilisation de ces données, le responsable du traitement lui demande une réponse par courrier électronique contenant la formule «Je consens». Une fois la réponse envoyée, la personne concernée reçoit un lien de vérification qu'elle doit ouvrir ou un SMS avec un code de vérification afin de confirmer le consentement.

L'article 9, paragraphe 2, ne reconnaît pas le caractère «nécessaire à l'exécution d'un contrat» comme une exception à l'interdiction générale de traiter des catégories particulières de données. Les responsables du traitement et les États membres se trouvant dans cette situation devraient se pencher sur les exceptions spécifiques des points b) à j) de l'article 9, paragraphe 2. Si aucune des exceptions listées aux points b) à j) ne s'applique, l'obtention d'un consentement explicite conforme aux conditions d'un consentement valable définies par le RGPD reste la seule exception licite permettant de traiter de telles données.

[Exemple 19]

Une compagnie aérienne, Holiday Airways, propose un service de voyage assisté pour les passagers qui ne peuvent voyager sans assistance, par exemple en raison d'un handicap. Une cliente réserve un vol d'Amsterdam à Budapest et demande une assistance voyage afin de pouvoir monter dans l'avion. Holiday Airways lui demande de fournir des informations sur son état de santé afin de mettre en place les services appropriés (il existe donc de nombreuses possibilités, par ex. un fauteuil roulant à la porte d'arrivée, ou un assistant voyageant avec elle de A à B). Holiday Airways lui demande son consentement explicite pour traiter ses données de santé dans l'objectif d'organiser l'assistance voyage requise. Les données traitées sur la base du consentement sont nécessaires au service requis. En outre, les vols vers Budapest sont toujours disponibles

⁴⁸ Cet exemple est sans préjudice du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

sans assistance voyage. Il convient de noter que dès lors que les données sont nécessaires à la fourniture du service requis, l'article 7, paragraphe 4, ne s'applique pas.

[Exemple 20]

Une entreprise prospère est spécialisée dans la fourniture de lunettes de snowboard et de ski personnalisées et d'autres types de lunettes personnalisées pour les sports en extérieur. L'idée est que les clients puissent les porter sans avoir à porter leurs propres lunettes. L'entreprise reçoit les commandes à un point central et livre ses produits à travers l'UE à partir d'un lieu unique. Afin de pouvoir fournir ses produits personnalisés aux clients souffrant de myopie, ce responsable du traitement demande leur consentement pour utiliser des informations sur leurs problèmes oculaires. Les clients fournissent les informations de santé nécessaires, telles que des données concernant leurs ordonnances, lorsqu'ils passent commande en ligne. Sans ces données, il est impossible pour l'entreprise de fournir les lunettes personnalisées demandées. L'entreprise propose également une gamme de lunettes avec des corrections standards. Les clients qui ne souhaitent pas partager leurs données de santé pourraient opter pour ces modèles standards. Aussi un consentement explicite est-il nécessaire en vertu de l'article 9 et le consentement peut-il être considéré comme étant donné librement.

5. Conditions supplémentaires d'obtention d'un consentement valable

Le RGPD introduit des conditions exigeant des responsables du traitement qu'ils prennent des dispositions complémentaires afin de s'assurer d'obtenir, de conserver et d'être en mesure de démontrer un consentement valable. L'article 7 du RGPD établit ces conditions supplémentaires d'obtention d'un consentement valable, avec des dispositions spécifiques concernant l'archivage du consentement et le droit de retirer facilement son consentement. L'article 7 s'applique également au consentement auquel il est fait référence dans d'autres articles du RGPD, par ex. dans les articles 8 et 9. Des orientations sur les exigences complémentaires de démonstration d'un consentement valable et de retrait du consentement sont disponibles ci-après.

5.1. Démonstration du consentement

Dans son article 7, paragraphe 1, le RGPD souligne l'obligation explicite du responsable du traitement de démontrer que la personne concernée a donné son consentement. En vertu de l'article 7, paragraphe 1, la charge de la preuve reposera sur le responsable du traitement.

Le considérant 42 prévoit que: *«Lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement devrait être en mesure de prouver que ladite personne a consenti à l'opération de traitement».*

Les responsables du traitement sont libres de développer des méthodes adaptées à leurs opérations quotidiennes pour se conformer à cette disposition. Parallèlement, l'obligation qu'a le responsable du traitement de démontrer qu'un consentement valable a été obtenu ne devrait pas en elle-même entraîner des volumes de traitement supplémentaire excessifs. Cela signifie que les responsables du traitement devraient disposer de suffisamment de données pour établir un lien avec le traitement (afin de démontrer que le consentement a été obtenu), mais qu'ils ne devraient pas collecter plus d'informations que nécessaire.

Il incombe au responsable du traitement de prouver qu'un consentement valable a été obtenu de la part de la personne concernée. Le RGPD ne stipule pas précisément comment cela doit être fait. Le responsable du traitement doit toutefois être en mesure de prouver qu'une personne concernée a

donné son consentement dans un cas spécifique. L'obligation de démontrer le consentement s'applique tant que l'activité de traitement en question perdure. Une fois l'activité de traitement terminée, la preuve de consentement ne devrait pas être conservée plus longtemps que strictement nécessaire pour respecter une obligation légale ou à la constatation, à l'exercice ou à la défense de droits en justice, conformément à l'article 17, paragraphe 3, points b) et e).

Le responsable du traitement peut par exemple conserver une trace des déclarations de consentement reçues afin de pouvoir attester de la façon dont le consentement a été obtenu, du moment où il a été obtenu et des informations fournies à la personne concernée à l'époque. Le responsable du traitement doit être en mesure de démontrer que la personne concernée a été informée et que le flux de travail respectait tous les critères pertinents pour un consentement valable. La raison de cette obligation établie par le RGPD est que les responsables du traitement doivent répondre de l'obtention d'un consentement valable de la part des personnes concernées et des mécanismes de consentement qu'ils ont établis. Par exemple, dans l'environnement en ligne, un responsable du traitement pourrait conserver des informations sur la session lors de laquelle le consentement a été donné, parallèlement à la documentation sur le flux de travail relatif au consentement à l'époque de la session et à une copie des informations fournies à l'époque à la personne concernée. Il ne serait pas suffisant de simplement se référer à une configuration adéquate du site Internet en question.

[Exemple 21] Un hôpital met en place un programme de recherche scientifique, appelé projet X, pour lequel des dossiers dentaires de patients réels sont nécessaires. Les participants sont recrutés par le biais d'appels téléphoniques à des patients ayant volontairement accepté de figurer sur une liste de candidats pouvant être contactés à cette fin. Le responsable du traitement sollicite le consentement explicite des personnes concernées pour utiliser leur dossier dentaire. Le consentement est obtenu lors d'un appel téléphonique par l'enregistrement d'une déclaration orale de la personne concernée dans laquelle celle-ci confirme consentir à l'utilisation de ses données aux fins du projet X.

Le RGPD ne fixe pas de durée spécifique pendant laquelle le consentement restera valable. La durée de validité du consentement dépendra du contexte, de la portée du consentement initial et des attentes de la personne concernée. Si les opérations de traitement changent ou évoluent considérablement, le consentement initial n'est plus valable. Dans ce cas, un nouveau consentement devra être obtenu.

Le G29 recommande, à titre de meilleure pratique, que le consentement soit renouvelé à des intervalles appropriés, toujours à condition que toutes les informations permettent de garantir que la personne concernée reste bien informée de la façon dont ses données sont utilisées et dont elle peut exercer ses droits⁴⁹.

5.2. Retrait du consentement

⁴⁹ Voir les lignes directrices du G29 sur la transparence. [Citation à finaliser une fois disponible]

Le RGPD accorde une place importante au retrait du consentement. Les dispositions et considérants du RGPD sur le retrait du consentement peuvent être considérés comme la codification de l'interprétation existante de cette thématique dans les avis du G29⁵⁰.

L'article 7, paragraphe 3, du RGPD stipule que le responsable du traitement doit s'assurer qu'il soit aussi simple pour la personne concernée de retirer que de donner son consentement, et que cela puisse être fait à tout moment. Le RGPD ne précise pas que la personne concernée doit toujours pouvoir donner et retirer son consentement moyennant la même action.

Toutefois, lorsque le consentement est obtenu par voie électronique uniquement par un clic, une frappe ou en balayant l'écran, les personnes concernées doivent, en pratique, pouvoir retirer ce consentement par le même biais. Lorsque le consentement est obtenu au moyen d'une interface utilisateur spécifique au service (par exemple moyennant un site Internet, une application, un compte avec identifiant, l'interface d'un dispositif IdO ou par courrier électronique), 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. La personne concernée devrait également être en mesure de retirer son consentement sans subir de préjudice. Cela signifie, entre autres, qu'un responsable du traitement doit proposer la possibilité de retirer son consentement gratuitement ou sans entraîner la diminution du niveau de service⁵¹.

[Exemple 22] Un festival de musique vend des tickets par le biais d'une plateforme de vente de tickets en ligne. Pour chaque ticket vendu, il demande le consentement de l'acheteur pour utiliser ses coordonnées à des fins commerciales. Afin d'indiquer leur consentement à cette finalité, les clients peuvent sélectionner soit «Non», soit «Oui». Le responsable du traitement informe les clients qu'ils auront la possibilité de retirer leur consentement. Pour ce faire, ils peuvent contacter gratuitement un centre d'appel les jours ouvrables entre 8h et 17h. Dans cet exemple, le responsable du traitement ne respecte pas l'article 7, paragraphe 3, du RGPD. En effet, le retrait du consentement nécessite ici un appel téléphonique pendant les heures ouvrables, ce qui est plus fastidieux que le clic de souris nécessaire pour donner son consentement sur la plateforme de vente de tickets en ligne, accessible 24/7.

Le RGPD considère l'existence d'un retrait facile comme un aspect nécessaire à un consentement valable. Si le droit de retrait ne remplit pas les exigences du RGPD, le mécanisme de consentement du responsable du traitement n'est pas conforme au RGPD. Comme mentionné à la rubrique 3.1 sur la condition d'un consentement *éclairé*, le responsable du traitement doit informer la personne concernée du droit de retrait du consentement avant qu'elle ne donne son consentement, conformément à l'article 7, paragraphe 3 du RGPD. Dans le cadre de l'obligation de transparence,

⁵⁰ Le G29 a discuté de cette thématique dans son avis sur le consentement (voir l'avis 15/2011 sur la définition du consentement (WP 187), p. 10, 14-15, 22, 31 et 37-38) et, entre autres, dans son avis sur l'utilisation de données de localisation (voir l'avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée (WP 115), p. 7).

⁵¹ Voir également l'avis 4/2010 du G29 sur le code de conduite de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct (WP 174) et l'avis sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée (WP 115).

le responsable du traitement doit en outre informer les personnes concernées de la façon dont elles peuvent exercer leurs droits⁵².

En règle générale, si le consentement est retiré, toutes les opérations de traitement des données basées sur le consentement ayant eu lieu avant le retrait du consentement – et conformes au RGPD – restent licites, mais le responsable du traitement doit cesser les activités de traitement en question. Si aucune autre base juridique ne justifie le traitement des données (par ex. période de conservation), celles-ci devraient être supprimées par le responsable du traitement⁵³.

Comme mentionné précédemment dans les présentes lignes directrices, il est essentiel que les responsables des données évaluent les finalités pour lesquelles les données sont effectivement traitées ainsi que les bases juridiques sur lesquelles ce traitement se fonde avant que les données ne soient collectées. Les entreprises ont souvent besoin de données à caractère personnel pour différentes finalités, et le traitement se fonde sur plus d'une base juridique, par ex. les données client peuvent se fonder sur un contrat ainsi que sur le consentement. Le retrait du consentement ne signifie ainsi pas qu'un responsable du traitement doit effacer les données traitées à une fin fondée sur l'exécution d'un contrat avec la personne concernée. Aussi les responsables du traitement devraient-ils d'emblée préciser clairement quelles finalités s'appliquent à quel élément de données et quelle base juridique sert de fondement au traitement.

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 conservation⁵⁴.

Outre cette situation, couverte par l'article 17, paragraphe 1, point b), une personne concernée peut demander la suppression d'autres données la concernant traitées sur la base d'un autre fondement juridique, par ex. sur la base de l'article 6, paragraphe 1, point b)⁵⁵. Les responsables du traitement sont contraints d'évaluer si la poursuite du traitement des données en question est appropriée, même en l'absence d'une demande d'effacement par la personne concernée⁵⁶.

Dans les cas où la personne concernée retire son consentement et où le responsable du traitement souhaite continuer à traiter les données à caractère personnel sur la base d'un autre fondement juridique, il ne peut silencieusement passer du consentement (qui est retiré) à cet autre fondement juridique. Toute modification de la base juridique du traitement doit être notifiée à la personne concernée conformément aux exigences en matière d'information définies aux articles 13 et 14 et en vertu du principe général de transparence.

⁵² Le considérant 39 du RGPD, qui se réfère aux articles 13 et 14 du règlement, stipule que «*les personnes physiques devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement.*»

⁵³ Voir article 17, paragraphe 1, point b) et paragraphe 3 du RGPD.

⁵⁴ Dans un tel cas, l'autre finalité justifiant le traitement doit disposer de sa propre base juridique. Cela ne signifie pas que le responsable du traitement peut remplacer le consentement par une autre base juridique, voir rubrique 6 ci-après.

⁵⁵ Voir article 17, y compris les exceptions qui peuvent s'y appliquer, et le considérant 65 du RGPD.

⁵⁶ Voir l'article 5, paragraphe 1, point e), du RGPD.

6. Interactions entre le consentement et les autres bases juridiques définies par l'article 6 du RGPD

L'article 6 établit les conditions d'un traitement des données à caractère personnel licite et décrit six bases juridiques sur lesquelles un responsable du traitement peut se fonder. L'application de l'une de ces six bases juridiques doit être établie avant l'activité de traitement et en lien avec une finalité spécifique⁵⁷.

Il est important de noter que si un responsable du traitement choisit de se fonder sur le consentement pour une partie du traitement, il doit être prêt à respecter ce choix et à interrompre le traitement si un individu retire son consentement. Indiquer que les données seront traitées sur la base du consentement, alors que le traitement se fonde sur une autre base juridique, serait fondamentalement déloyal envers les personnes concernées.

Autrement dit, le responsable du traitement ne peut passer du consentement à une autre base juridique. Par exemple, il n'est pas autorisé d'utiliser rétrospectivement la base juridique des intérêts légitimes afin de justifier le traitement lorsque des problèmes ont été rencontrés concernant la validité du consentement. Dès lors que les responsables du traitement ont l'obligation de communiquer la base juridique sur laquelle ils se fondent au moment de la collecte des données, ils doivent avoir défini leur base juridique préalablement à ladite collecte.

7. Domaines critiques spécifiques dans le RGPD

7.1. Les enfants (article 8)

Par rapport à la directive actuelle, le RGPD établit un niveau de protection supplémentaire lorsque les données à caractère personnel de personnes vulnérables, notamment d'enfants, sont traitées. L'article 8 introduit des obligations complémentaires pour garantir un niveau de protection des données à caractère personnel amélioré pour les enfants en ce qui concerne les services de la société de l'information. Les raisons de cette protection améliorée sont précisées au considérant 38: *«[...] ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel [...]»*. Le considérant 38 indique également que *«Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant.»* Le mot «notamment» indique que cette protection spécifique ne se limite pas uniquement au marketing ou au profilage, mais inclut «la collecte de données à caractère personnel relatives aux enfants» au sens large.

L'article 8, paragraphe 1, dispose que lorsque le consentement s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans.

⁵⁷ Conformément aux articles 13, paragraphe 1, point c) et 14, paragraphe 1, point c), le responsable du traitement doit en informer la personne concernée.

Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant⁵⁸. Le RGPD est flexible en ce qui concerne l'âge minimum d'un consentement valable: les États membres peuvent prévoir par la loi un âge inférieur, mais il ne peut être inférieur à 13 ans.

Comme mentionné à la rubrique 3.1 sur le consentement éclairé, les informations devront être compréhensibles pour l'audience à laquelle s'adresse le responsable du traitement, avec une attention particulière pour la situation des enfants. Afin d'obtenir un «consentement éclairé» de la part d'un enfant, le responsable du traitement doit expliquer en termes clairs et simples pour les enfants comment il a l'intention d'utiliser les données qu'il collecte⁵⁹. S'il appartient au parent de donner son consentement, un certain nombre d'informations pourrait être nécessaire afin que l'adulte en question puisse prendre une décision éclairée.

Il ressort clairement de ce qui précède que l'article 8 s'appliquera uniquement lorsque les conditions suivantes sont remplies:

- Le traitement est lié à l'offre directe de services de la société de l'information à un enfant⁶⁰.
- Le traitement est fondé sur le consentement.

7.1.1. Service de la société de l'information

Afin de déterminer la portée du terme «service de la société de l'information» dans le RGPD, l'article 4, paragraphe 25, du RGPD fait référence à la directive 2015/1535.

Pour évaluer la portée de cette définition, le G29 se réfère également à la jurisprudence de la CJUE⁶². La CJUE a estimé que les *services de la société de l'information* couvrent les contrats et autres services conclus ou transmis en ligne. Lorsqu'un service a deux éléments économiquement

⁵⁸ Sans préjudice de la possibilité qu'ont les États membres de déroger par voie législative à la limite d'âge; voir l'article 8, paragraphe 1.

⁵⁹ Le considérant 58 du RGPD réaffirme cette obligation, en indiquant que, le cas échéant, un responsable du traitement devrait s'assurer que les informations fournies soient compréhensibles pour des enfants.

⁶⁰ Selon l'article 4, paragraphe 25 du RGPD, un service de la société de l'information est un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535: «b) "service", tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services. Aux fins de la présente définition, on entend par: i) "à distance", un service fourni sans que les parties soient simultanément présentes; ii) "par voie électronique", un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques; iii) "à la demande individuelle d'un destinataire de services", un service fourni par transmission de données sur demande individuelle.» Une liste indicative des services non visés par cette définition figure à l'annexe I de ladite directive. Voir aussi le considérant 18 de la directive 2000/31.

⁶¹ Selon l'article 1^{er} de la Convention des Nations unies relative aux droits de l'enfant, «[...] un enfant s'entend de tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable»; cf. Nations unies, résolution 44/25 du 20 novembre 1989 (Convention relative aux droits de l'enfant).

⁶² Cf. Cour de justice de l'Union européenne, 2 décembre 2010, affaire C-108/09 (*Ker-Optika*), paragraphes 22 et 28. Par rapport aux «services composites», le G29 se réfère également à l'affaire C-434/15 (*Asociación Profesional Elite Taxi contre Uber Systems Spain SL*), paragraphe 40, qui stipule qu'un service de la société de l'information faisant partie intégrante d'un service global dont l'élément principal n'est pas un service de la société de l'information (dans le cas d'espèce, un service de transport) ne répond pas à la qualification de «service de la société de l'information».

indépendants, l'un d'entre eux étant un élément en ligne, par exemple l'offre ou l'acceptation d'une offre dans le cadre de la conclusion d'un contrat, ou les informations liées aux produits ou services, y compris les activités de marketing, cet élément est considéré comme un service de la société de l'information, tandis que l'autre élément, qui serait la livraison ou la distribution physique de marchandises, n'est pas couvert par la notion de service de la société de l'information. La fourniture d'un service en ligne relèverait également du champ d'application du terme *service de la société de l'information* au sens de l'article 8 du RGPD.

7.1.2. Proposés directement à un enfant

L'inclusion de la formule «proposés directement à un enfant» indique que l'article 8 ne s'applique qu'à certains des services de la société de l'information, et non à tous. À cet égard, si un prestataire de services de la société de l'information indique clairement aux utilisateurs potentiels qu'il ne propose ses services qu'à des personnes âgées de 18 ans ou plus, et que cette affirmation n'est pas contredite par d'autres preuves (tels que le contenu du site Internet ou les plans de commercialisation), ces services ne seront pas considérés comme étant «proposés directement à un enfant» et l'article 8 ne s'appliquera pas.

7.1.3. Âge

Le RGPD stipule que *«Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans.»* Lorsqu'il évalue le public ciblé par ses services, le responsable du traitement doit être conscient des différentes lois nationales. Il convient de noter en particulier qu'un responsable du traitement fournissant un service transfrontalier ne peut pas toujours se contenter de respecter uniquement la législation de l'État membre dans lequel il est principalement établi, mais peut se voir dans l'obligation de respecter les législations nationales respectives de tous les États membres dans lesquels il propose son ou ses services de la société de l'information. Cela sera fonction de si l'État membre décide d'utiliser le lieu d'établissement principal du responsable du traitement comme point de référence dans sa législation nationale, ou bien la résidence de la personne concernée. Avant toute chose, les États membres doivent tenir compte de l'intérêt supérieur de l'enfant lorsqu'ils prennent leur décision. Le groupe de travail encourage les États membres à chercher une solution harmonisée à cet égard.

Lorsqu'ils fournissent des services de la société de l'information à des enfants en se fondant sur le consentement, les responsables du traitement devront s'efforcer raisonnablement de vérifier que l'utilisateur a dépassé l'âge minimum de consentement numérique; ces efforts devraient être proportionnels à la nature des activités de traitement et aux risques qui y sont liés.

Si les utilisateurs indiquent qu'ils ont bien l'âge minimum de consentement numérique, le responsable du traitement peut effectuer des vérifications appropriées pour s'assurer que cette affirmation est vraie. Bien que la nécessité de déployer des efforts raisonnables pour vérifier l'âge n'est pas explicite dans le RGPD, elle est sous-entendue de façon implicite, dès lors que si un enfant donne son consentement alors qu'il n'a pas atteint l'âge requis pour donner un consentement valable en son nom propre, le traitement des données sera illicite.

Si l'utilisateur déclare ne pas avoir atteint l'âge minimum de consentement numérique, le responsable du traitement peut accepter cette déclaration sans vérification complémentaire, mais devra s'assurer d'obtenir une autorisation parentale et de vérifier que la personne fournissant ce consentement est titulaire de la responsabilité parentale.

La vérification de l'âge de la personne concernée ne doit pas entraîner un traitement de données supplémentaire excessif. Le mécanisme choisi pour vérifier l'âge d'une personne concernée devrait comprendre une évaluation des risques liés au traitement envisagé. Dans certaines situations à faible risque, il pourrait être approprié de demander à un nouvel abonné à un service de révéler son année de naissance ou de remplir un formulaire stipulant qu'il est ou n'est pas mineur⁶³. En cas de doute, le responsable du traitement devrait réviser ses mécanismes de vérification de l'âge dans un cas donné et évaluer si des méthodes de vérification alternatives sont nécessaires⁶⁴.

7.1.4. Consentement des enfants et responsabilité parentale

Concernant l'autorisation d'un titulaire de la responsabilité parentale, le RGPD ne définit pas de méthode pratique d'obtention du consentement parental ou de vérification que la personne en question est habilitée à effectuer cette action⁶⁵. Aussi le G29 recommande-t-il l'adoption d'une approche proportionnée, conformément à l'article 8, paragraphe 2, du RGPD et à l'article 5, paragraphe 1, point c), du RGPD (minimisation des données). Une approche proportionnée pourrait être de se concentrer sur l'obtention d'une quantité limitée d'informations, telles que les coordonnées d'un parent ou d'un tuteur.

Le caractère raisonnable d'une mesure, à la fois pour ce qui est de vérifier qu'un utilisateur est suffisamment âgé pour donner son propre consentement et que la personne donnant son consentement au nom d'un enfant est titulaire de la responsabilité parentale, peut dépendre des risques liés au traitement ainsi que des technologies disponibles. Dans les cas présentant de faibles risques, la vérification de la responsabilité parentale par courrier électronique peut être suffisante. Inversement, dans les situations à risque élevé, il peut être approprié de demander davantage de preuves afin que le responsable du traitement soit en mesure de vérifier et de conserver les informations conformément à l'article 7, paragraphe 1, du RGPD⁶⁶. Des services de vérification tiers de confiance peuvent constituer une solution pour minimiser la quantité de données à caractère personnel traitées par le responsable du traitement.

⁶³ Bien qu'il ne s'agisse pas d'une solution infaillible dans tous les cas, il s'agit d'un exemple de méthode pour satisfaire à cette disposition.

⁶⁴ Voir l'avis 5/2009 du G29 sur les réseaux sociaux en ligne (WP 163).

⁶⁵ Le G29 remarque que le titulaire de la responsabilité parentale n'est pas toujours le parent biologique de l'enfant et que la responsabilité parentale peut être détenue par de multiples parties pouvant comprendre des personnes morales comme des personnes physiques.

⁶⁶ Par exemple, le responsable du traitement pourrait demander au parent ou tuteur d'effectuer un paiement de 0,01 € moyennant un virement bancaire, comprenant une brève confirmation, dans la communication associée à la transaction, que le titulaire du compte bancaire est le titulaire de la responsabilité parentale de l'utilisateur. Le cas échéant, une méthode alternative de vérification devrait être fournie afin d'éviter tout traitement discriminatoire indu de personnes ne disposant pas d'un compte bancaire.

[Exemple 23] Une plateforme de jeu en ligne souhaite s'assurer que les clients mineurs ne souscrivent ses services qu'avec le consentement de leurs parents ou tuteurs. Le responsable du traitement suit les étapes suivantes:

Étape n° 1: demander à l'utilisateur de préciser s'il a moins ou plus de 16 ans (ou tout autre âge de consentement numérique).

Si l'utilisateur indique ne pas avoir l'âge minimum de consentement numérique:

Étape n° 2: le service informe l'enfant qu'un parent ou tuteur doit donner son consentement ou autoriser le traitement avant que le service ne lui soit fourni. Il est demandé à l'utilisateur de communiquer l'adresse électronique d'un parent ou tuteur.

Étape n° 3: le service contacte le parent ou tuteur, obtient son consentement au traitement par courrier électronique et prend des mesures raisonnables pour confirmer que l'adulte en question est titulaire de la responsabilité parentale.

Étape n° 4: en cas de plainte, la plateforme prend des mesures complémentaires pour vérifier l'âge de l'abonné. Si la plateforme respecte les autres exigences en matière de consentement, elle peut se conformer aux critères complémentaires de l'article 8 du RGPD en suivant les étapes susmentionnées.

L'exemple montre que le responsable du traitement peut démontrer que des efforts raisonnables ont été entrepris afin de vérifier que le consentement valable a été obtenu pour les services fournis à un enfant. L'article 8, paragraphe 2, ajoute notamment que *«Le responsable du traitement s'efforce raisonnablement de vérifier que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.»*

Il incombe au responsable du traitement de déterminer quelles mesures sont appropriées dans un cas spécifique. En règle générale, les responsables du traitement doivent éviter les solutions de vérification qui impliquent en elles-mêmes une collecte excessive de données à caractère personnel.

Le G29 reconnaît qu'il peut exister des cas où une telle vérification est ardue (par exemple lorsque les enfants fournissant leur propre consentement n'ont pas encore établi une «empreinte identitaire», ou lorsque la responsabilité parentale n'est pas facilement vérifiable). Ces difficultés peuvent être prises en compte au moment de décider des efforts raisonnables, mais l'on s'attend également à ce que les responsables du traitement procèdent à une évaluation constante de leurs procédures et de la technologie disponible.

Pour ce qui est de l'autonomie d'une personne concernée à donner son consentement au traitement de ses données à caractère personnel et à avoir un contrôle total sur le traitement, le consentement donné ou autorisé par un titulaire de la responsabilité parentale quant au traitement des données à caractère personnel d'un enfant peut être confirmé, modifié ou retiré une fois que la personne concernée atteint l'âge minimum de consentement numérique.

En pratique, cela signifie que si l'enfant n'entreprend aucune action, le consentement donné ou autorisé par un titulaire de la responsabilité parentale quant au traitement de données à caractère personnel avant l'âge minimum de consentement numérique restera une base juridique valable pour ledit traitement.

Une fois l'âge minimum de consentement numérique atteint, l'enfant aura la possibilité de retirer son consentement par lui-même, conformément à l'article 7, paragraphe 3. Conformément aux

principes de loyauté et de responsabilité, le responsable du traitement doit informer l'enfant de cette possibilité⁶⁷.

Il est important de noter que conformément au considérant 38, le consentement par un parent ou un tuteur n'est pas nécessaire dans le cadre de services de prévention ou de conseil proposés directement à un enfant. Par exemple, la fourniture de services de protection de l'enfant proposés en ligne à un enfant au moyen d'un service de messagerie instantanée en ligne ne devrait pas nécessiter une autorisation parentale préalable.

Enfin, le RGPD stipule que les règles relatives aux exigences d'autorisation parentale par rapport aux mineurs ne devraient pas porter atteinte «au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant.» Aussi les exigences d'un consentement valable pour l'utilisation de données concernant des enfants font-elles partie d'un cadre juridique devant être considéré comme distinct du droit des contrats national. Ce document d'orientation ne traite par conséquent pas de la question de savoir s'il est licite pour un mineur de conclure des contrats en ligne. Ces deux régimes juridiques peuvent s'appliquer simultanément, mais le champ d'application du RGPD ne demande pas l'harmonisation des dispositions nationales du droit des contrats.

7.2. La recherche scientifique

La définition de ce que sont les fins de recherche scientifique a d'importantes répercussions sur le type d'activités de traitement des données qu'un responsable du traitement peut entreprendre. Le terme de «*recherche scientifique*» n'est pas défini par le RGPD. Le considérant 159 stipule que «(...) *Aux fins du présent règlement, le traitement de données à caractère personnel à des fins de recherche scientifique devrait être interprété au sens large (...).*» Toutefois, le G29 considère que cette notion peut être élargie au-delà de sa signification habituelle et estime que la «*recherche scientifique*» signifie dans ce contexte un projet de recherche établi conformément aux normes méthodologiques et éthiques du secteur en question, conformément aux bonnes pratiques.

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. Un exemple d'une telle obligation procédurale où le traitement n'est pas fondé sur le consentement, mais sur une autre base juridique peut être trouvé dans le règlement relatif aux essais cliniques. Dans le contexte de la législation relative à la protection des données, cette dernière forme de consentement pourrait être considérée comme une garantie complémentaire⁶⁸. Parallèlement, le RGPD ne restreint pas l'application de l'article 6 au seul consentement pour ce qui est du traitement de données à des fins de recherche. Du moment que des garanties appropriées existent, telles que celles énumérées à l'article 89, paragraphe 1, et que le traitement respecte les principes de loyauté, de licéité, de transparence et de minimisation des données ainsi que les droits individuels, d'autres bases juridiques, telles que l'article 6,

⁶⁷ Les personnes concernées devraient également être conscientes du droit à l'oubli prévu à l'article 17, particulièrement pertinent pour le consentement donné lorsque la personne concernée était encore un enfant, cf. considérant 63.

⁶⁸ Voir également le considérant 161 du RGPD.

paragraphe 1, point e) ou f), peuvent être envisageables⁶⁹. Ceci s'applique également aux catégories particulières de données en vertu de la dérogation définie par l'article 9, paragraphe 2, point j)⁷⁰.

Le considérant 33 semble apporter plus de flexibilité au niveau de précision et de détail du consentement dans le cadre de la recherche scientifique. Le considérant 33 prévoit 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. Par conséquent, les personnes concernées devraient pouvoir donner leur consentement en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique. Les personnes concernées devraient pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet.*»

Premièrement, il convient de noter que le considérant 33 n'annule pas les obligations liées à l'exigence d'obtention d'un consentement spécifique. Cela signifie qu'en principe, les projets de recherche scientifique ne peuvent inclure des données à caractère personnel sur la base du consentement de la personne concernée que si leur finalité est décrite avec précision. Dans les cas où les finalités du traitement de données dans le cadre d'un projet scientifique ne peuvent être précisées d'entrée de jeu, le considérant 33 admet, à titre d'exception, que la finalité soit décrite de façon plus générale.

Au vu des conditions strictes établies par l'article 9 du RGPD concernant le traitement portant sur des catégories particulières de données, le G29 observe que lorsque des catégories particulières de données sont traitées sur la base d'un consentement explicite, l'application de l'approche flexible décrite au considérant 33 devra être soumise à une interprétation plus stricte et nécessitera un contrôle minutieux.

Lorsque considéré dans son ensemble, le RGPD ne peut être interprété comme permettant à un responsable du traitement d'éluder le principe clé qu'est la spécification de la finalité pour laquelle le consentement de la personne concernée est sollicité.

Lorsque les finalités de recherche ne peuvent pas être spécifiées dans leur intégralité, le responsable du traitement doit trouver d'autres méthodes pour s'assurer que l'essence des exigences en matière de consentement soit respectée autant que possible, par exemple en faisant en sorte que les personnes concernées puissent donner leur consentement pour une finalité de recherche exprimée en termes plus généraux, ainsi que pour les éventuelles étapes spécifiques du projet de recherche connues à l'avance. Au fur et à mesure que le projet de recherche progresse, le consentement pour les étapes suivantes du projet peut être obtenu avant que lesdites étapes ne débutent. Un tel consentement devrait néanmoins toujours respecter les normes éthiques applicables à la recherche scientifique.

⁶⁹ L'article 6, paragraphe 1, point c), peut également s'appliquer aux opérations de traitement spécifiquement exigées par la loi, telles que la collecte de données fiables et solides en vertu du protocole approuvé par les États membres au titre du règlement relatif aux essais cliniques.

⁷⁰ En vertu de l'article 9, paragraphe 2, point i), l'essai spécifique de médicaments peut se fonder sur une réglementation européenne ou nationale.

Dans de tels cas, le responsable du traitement peut en outre appliquer des garanties complémentaires. L'article 89, paragraphe 1, souligne par exemple la nécessité d'établir des garanties dans le cadre des activités de traitement de données à des fins de recherche scientifique ou historique, ou à des fins statistiques. Le traitement à ces fins «*est soumis, conformément au présent règlement, à des garanties appropriées pour les droits et libertés de la personne concernée*». La minimisation, l'anonymisation et la sécurité des données sont citées comme garanties possibles⁷¹. L'anonymisation est la solution privilégiée dans tous les cas où la finalité de la recherche ne nécessite pas le traitement de données à caractère personnel.

La transparence constitue une garantie complémentaire lorsque les circonstances de la recherche ne permettent pas un consentement spécifique. Un manque de précision concernant la finalité peut être compensé par la communication régulière, par les responsables du traitement, d'informations sur l'évolution de la finalité à mesure que le projet progresse afin qu'avec le temps, le consentement soit aussi spécifique que possible. La personne concernée aura ainsi au moins une compréhension générale de l'état de la situation, ce qui lui permettra d'évaluer si elle souhaite ou non recourir à son droit de retrait du consentement conformément à l'article 7, paragraphe 3⁷².

L'établissement d'un plan de recherche exhaustif que les personnes concernées pourraient consulter avant de donner leur consentement pourrait également contribuer à compenser le manque de précision de la finalité⁷³. Ce plan de recherche devrait décrire les questions de recherche et les méthodes de travail envisagées aussi clairement que possible. Il pourrait également contribuer au respect de l'article 7, paragraphe 1, dès lors que les responsables du traitement doivent être en mesure de prouver que les informations étaient accessibles aux personnes concernées au moment du consentement afin de démontrer la validité du consentement.

Il est important de rappeler que lorsque le consentement est utilisé comme base juridique du traitement, la personne concernée doit avoir la possibilité de retirer ce consentement. Le G29 observe que le retrait du consentement pourrait compromettre les types de recherche scientifique nécessitant des données pouvant être reliées à des individus; le RGPD indique cependant clairement

⁷¹ Voir, par exemple, le considérant 156. Le traitement de données à caractère personnel à des fins scientifiques devrait également respecter d'autres dispositions législatives pertinentes, telles que celles relatives aux essais cliniques; cf. considérant 156, mentionnant le règlement (UE) n° 536/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain. Voir également l'avis 15/2011 du G29 sur la définition du consentement (WP 187), p. 8: «*En outre, l'obtention d'un consentement n'annule pas les obligations imposées au responsable du traitement par l'article 6 en termes d'équité, de nécessité, de proportionnalité ainsi que de qualité des données. Ainsi, même si le traitement de données à caractère personnel a reçu le consentement de l'utilisateur, cela ne justifie pas la collecte de données excessives au regard d'une fin particulière. [...] En principe, le consentement ne doit pas être considéré comme une dérogation à d'autres principes applicables à la protection des données, mais bien comme une garantie. Il s'agit en premier lieu d'une condition de licéité et non d'une renonciation à l'application d'autres principes.*»

⁷² D'autres mesures de transparence peuvent également être pertinentes. Lorsque des responsables du traitement procèdent au traitement de données à des fins scientifiques sans être en mesure de communiquer toutes les informations en début du projet, ils pourraient désigner une personne de contact spécifique à laquelle les personnes concernées peuvent adresser leurs questions.

⁷³ Une telle possibilité peut être trouvée dans l'article 14, paragraphe 1, de l'actuelle loi finlandaise relative à la protection des données (*Henkilötietolaki*, 523/1999).

que le consentement peut être retiré et que les responsables du traitement doivent s'y conformer – la recherche scientifique ne bénéficie d'aucune dérogation à cet égard. Si un responsable du traitement reçoit une demande de retrait du consentement, il doit en principe supprimer immédiatement les données à caractère personnel de la personne concernée s'il souhaite continuer à utiliser les données aux fins de sa recherche⁷⁴.

7.3. Les droits des personnes concernées

Si l'activité de traitement des données est fondée sur le consentement d'une personne concernée, cela aura une incidence sur les droits de cette personne. Lorsque le traitement est fondé sur le consentement, les personnes concernées bénéficient du droit à la portabilité des données (article 20). Le droit d'opposition (article 21) ne s'applique en revanche pas lorsque le traitement est fondé sur le consentement, bien que le droit de retrait du consentement puisse entraîner un résultat similaire.

Les articles 16 à 20 du RGPD indiquent que (lorsque le traitement est fondé sur le consentement) les personnes concernées disposent du droit à l'effacement lorsque le consentement a été retiré ainsi que du droit à la limitation, du droit de rectification et du droit d'accès⁷⁵.

8. Consentement obtenu en vertu de la directive 95/46/CE

Les responsables du traitement qui traitent actuellement des données sur la base du consentement conformément à la législation nationale relative à la protection des données ne sont pas automatiquement contraints de revoir entièrement leurs relations de consentement avec les personnes concernées en prévision du RGPD. Les consentements obtenus jusqu'ici restent valables dans la mesure où ils sont conformes aux conditions énoncées par le RGPD.

Il est essentiel que les responsables du traitement révisent en profondeur leurs processus de travail et leurs registres avant le 25 mai 2018 afin de s'assurer que les consentements existants sont conformes aux normes du RGPD (voir le considérant 171 du RGPD⁷⁶). En pratique, le RGPD relève la barre pour ce qui est de la mise en œuvre de mécanismes de consentement et introduit une série de nouvelles exigences qui astreignent les responsables du traitement à modifier leurs mécanismes de consentement plutôt que de simplement remanier leur politique de confidentialité⁷⁷.

⁷⁴ Voir également l'avis 05/2014 du G29 sur les techniques d'anonymisation (WP 216).

⁷⁵ Lorsque certaines activités de traitement des données sont restreintes conformément à l'article 18 du RGPD, le consentement de la personne concernée peut être nécessaire pour lever ces restrictions.

⁷⁶ Le considérant 171 du RGPD prévoit que: «*La directive 95/46/CE devrait être abrogée par le présent règlement. Les traitements déjà en cours à la date d'application du présent règlement devraient être mis en conformité avec celui-ci dans un délai de deux ans après son entrée en vigueur. Lorsque le traitement est fondé sur un consentement en vertu de la directive 95/46/CE, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la manière dont le consentement a été donné est conforme aux conditions énoncées dans le présent règlement, de manière à ce que le responsable du traitement puisse poursuivre le traitement après la date d'application du présent règlement. Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées.*»

⁷⁷ Comme indiqué dans l'introduction, le RGPD apporte des clarifications et des précisions complémentaires sur les conditions d'obtention et de démonstration d'un consentement valable. Nombre de ces nouvelles dispositions s'inspirent de l'avis 15/2011 sur le consentement.

Par exemple, dès lors que le RGPD stipule qu'un responsable du traitement doit être en mesure de démontrer qu'un consentement valable a été obtenu, tous les consentements présumés dont aucune trace n'est conservée seront automatiquement en deçà des normes de consentement établies par le RGPD et devront être renouvelés. De même, dès lors que le RGPD requiert une «déclaration ou un acte positif clair», tous les consentements présumés fondés sur une forme d'action plus implicite de la part de la personne concernée (par ex. une case cochée par défaut) ne seront pas conformes aux normes de consentement du RGPD.

En outre, afin d'être en mesure de démontrer qu'un consentement valable a été obtenu ou de permettre une indication plus détaillée des souhaits de la personne concernée, les opérations et les systèmes informatiques pourraient nécessiter une révision. Des mécanismes permettant aux personnes concernées de retirer facilement leur consentement doivent également être rendus disponibles, tout comme des informations sur la procédure de retrait du consentement. Si les procédures existantes d'obtention et de gestion du consentement ne sont pas conformes aux normes du RGPD, les responsables du traitement devront obtenir un nouveau consentement conforme au RGPD.

D'un autre côté, dès lors que tous les éléments énumérés aux articles 13 et 14 ne doivent pas nécessairement être présents pour que le consentement soit éclairé, les obligations d'information complémentaires fixées par le RGPD ne s'opposent pas nécessairement à la continuité de la validité du consentement obtenu avant l'entrée en vigueur du RGPD (voir page 17 ci-dessus). Il convient de signaler que la directive 95/46/CE n'établissait aucune nécessité d'informer les personnes concernées de la base sur laquelle se fondait le traitement de leurs données.

Si un responsable du traitement estime que le consentement obtenu en vertu de l'ancienne législation ne satisfera pas aux normes de consentement du RGPD, il doit prendre des mesures afin de se conformer auxdites normes, par exemple en renouvelant le consentement au moyen d'un mécanisme conforme au RGPD. En vertu du RGPD, il n'est pas possible de passer d'une base juridique à une autre. Si un responsable du traitement n'est pas en mesure de renouveler le consentement au moyen d'un mécanisme conforme au RGPD et n'est pas non plus en mesure de se conformer au nouveau règlement en fondant – à titre exceptionnel – son traitement des données sur une autre base juridique tout en s'assurant que le traitement ainsi poursuivi respecte les principes de loyauté et de responsabilité, les activités de traitement devront être interrompues. En tout état de cause, le responsable du traitement doit respecter les principes de licéité, de loyauté et de transparence du traitement.

._*._*._*._*._*._*._*._*._* **FIN DU DOCUMENT** *_*._*._*._*._*._*._*._*._*._*._*._*._*._*._*._*