

# RECOMMANDATION

n° 01/2020 du 17 janvier 2020

**relative aux traitements de données à caractère personnel à des fins de marketing direct**



Autorité de protection des données



|             |                                                                                                             |           |
|-------------|-------------------------------------------------------------------------------------------------------------|-----------|
| <b>I.</b>   | <b>INTRODUCTION.....</b>                                                                                    | <b>4</b>  |
| <b>A.</b>   | <b>Avant-propos .....</b>                                                                                   | <b>4</b>  |
| <b>B.</b>   | <b>Contexte et champ d’application de la recommandation .....</b>                                           | <b>5</b>  |
| <b>C.</b>   | <b>Cadre juridique.....</b>                                                                                 | <b>7</b>  |
| <b>II.</b>  | <b>Le marketing direct : de quoi parlons-nous ? .....</b>                                                   | <b>8</b>  |
| <b>A.</b>   | <b>Le marketing direct c’est .....</b>                                                                      | <b>8</b>  |
| 1.          | Définition.....                                                                                             | 8         |
| 2.          | Notions clés .....                                                                                          | 9         |
| <b>III.</b> | <b>Marketing direct et protection des données à caractère personnel : comment agir en conformité ?...16</b> |           |
| <b>A.</b>   | <b>Acteurs du marketing direct et rôles définis par le RGPD .....</b>                                       | <b>16</b> |
| 1.          | Responsable du traitement et responsables conjoints .....                                                   | 16        |
| 2.          | Sous-traitant.....                                                                                          | 19        |
| 3.          | Achat, location, enrichissement de données à caractère personnel .....                                      | 23        |
| 4.          | Filiales – Fusions, scissions et acquisitions .....                                                         | 27        |
| <b>B.</b>   | <b>Déterminez vos finalités de traitement .....</b>                                                         | <b>27</b> |
| 1.          | Finalité(s) initiale(s) .....                                                                               | 27        |
| 2.          | Finalité(s) ultérieure(s).....                                                                              | 29        |
| <b>C.</b>   | <b>Définissez vos opérations de traitement .....</b>                                                        | <b>31</b> |
| 1.          | Notion .....                                                                                                | 31        |
| 2.          | Profilage.....                                                                                              | 34        |
| <b>D.</b>   | <b>Identifiez les données nécessaires à la poursuite de vos finalités .....</b>                             | <b>37</b> |
| 1.          | Notion de « donnée à caractère personnel ».....                                                             | 37        |
| 2.          | Principe de minimisation des données .....                                                                  | 38        |
| 3.          | Maîtrisez votre gestion des données .....                                                                   | 40        |
| <b>E.</b>   | <b>Vérifiez que vous disposez d’une base juridique .....</b>                                                | <b>44</b> |
| 1.          | Pourquoi une base juridique ? .....                                                                         | 44        |
| 2.          | Est-il possible de changer de base juridique ? .....                                                        | 44        |
| 3.          | Quelle base juridique pour les traitements de marketing direct ?.....                                       | 46        |
| 4.          | Les intérêts légitimes .....                                                                                | 48        |
| 5.          | Le consentement.....                                                                                        | 58        |



**F. Soyez transparents .....74**

**IV. Conclusion .....77**



# I. INTRODUCTION

## A. Avant-propos

1. Adopté le 27 avril 2016, le Règlement (UE) 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « RGPD »), est entré en vigueur depuis le 25 mai 2018. Abrogeant la Directive du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « Directive 95/46/CE »), il en confirme et consolide les règles telles qu'appliquées par la Cour de Justice de l'Union européenne et par le Groupe de Travail Article 29<sup>1</sup> au travers de ses positions officielles et Lignes directrices. Passant d'une directive à un règlement, le législateur européen a entendu rendre la protection des données à caractère personnel, érigée au rang de droit fondamental par l'article 8 de la Charte des droits fondamentaux de l'Union européenne, directement et uniformément applicable eu sein des Etats-membres<sup>2</sup>.
2. L'un des objectifs principaux du RGPD est de renforcer les droits des personnes concernées. Le RGPD dote ainsi notamment les Autorités de contrôle de compétences importantes leur permettant, en outre, de prononcer des sanctions en cas de manquements aux règles qu'il établit. L'Eurobaromètre de mai 2019 sur le RGPD démontre que la connaissance qu'ont les personnes concernées des règles applicables en matière de protection des données et de leurs droits est en nette augmentation<sup>3</sup>. En outre, celles-ci exercent davantage leurs droits qu'auparavant<sup>4</sup>. Il en va notamment ainsi du retrait de leur consentement ou de l'opposition au traitement de leurs données pour des communications commerciales<sup>5</sup>.
3. C'est au regard de ces droits renforcés que de nombreuses associations de consommateurs et de droits civils s'accordent à dire que le RGPD contribue largement à une société digitale équitable, construite sur la confiance mutuelle entre personnes concernées et acteurs intervenant dans le traitement de leurs données<sup>6</sup>.

---

<sup>1</sup> Le Groupe de travail Article 29 a été remplacé par le Comité européen de protection des données (souvent désigné par son acronyme anglais « EDPB ») qui reprend à son compte les différentes positions adoptées par le Groupe de Travail Article 29. Il sera donc fait référence aux positions de l'EDPB dans la présente recommandation.

<sup>2</sup> Sous réserve de quelques exceptions laissant aux législateurs nationaux une marge de manœuvre que nous n'aborderons pas dans la présente recommandation.

<sup>3</sup> <https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222>; ou également [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_2956](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2956).

<sup>4</sup> [https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr\\_in\\_numbers\\_1.pdf](https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf)

<sup>5</sup> Voir le rapport du "Multi-stakeholder Group on the General Data Protection Regulation" établi auprès de la Commission européenne et impliquant la société civile et les représentants des secteurs professionnels, les académiques et les praticiens, disponible sur le lien suivant : <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537>

<sup>6</sup> Voir en ce sens la communication de la Commission européenne au Parlement européen et au Conseil du 24 juillet 2019 sur le lien suivant :

[https://ec.europa.eu/commission/sites/beta-political/files/gdpr\\_communication.pdf?utm\\_source=POLITICO\\_EU&utm\\_campaign=7a63680bad-EMAIL\\_CAMPAIGN\\_2019\\_07\\_24\\_10\\_41&utm\\_medium=email&utm\\_term=0\\_10959edeb5-7a63680bad-190036317](https://ec.europa.eu/commission/sites/beta-political/files/gdpr_communication.pdf?utm_source=POLITICO_EU&utm_campaign=7a63680bad-EMAIL_CAMPAIGN_2019_07_24_10_41&utm_medium=email&utm_term=0_10959edeb5-7a63680bad-190036317)



4. Afin de garantir cet objectif, le RGPD accentue la responsabilisation des différents acteurs du traitement des données à caractère personnel, qu'ils soient particuliers ou professionnels, personne morale ou administration publique, et ce à chaque étape du traitement, tant à un niveau national qu'euro-péen ou international.
5. De ce fait, les Autorités de contrôle n'ont pas pour seul rôle d'intervenir en aval à l'égard de ces derniers, en cas de violation par eux des règles du RGPD. Au vu des importantes sanctions encourues et du fait que les données à caractère personnel sont devenues indispensables à la poursuite de la majorité des activités socio-économiques, l'accompagnement des responsables de traitement par les Autorités de protection de données constitue une de leurs compétences les plus importantes.



Le marketing direct représente l'un des secteurs identifiés dans le plan stratégique de l'Autorité de protection des données (ci-après « APD » ou « Autorité ») comme étant une priorité dans les différentes actions que celle-ci entend mener. Fournir, par cette Recommandation, une interprétation des règles applicables aux traitements de données à caractère personnel réalisés à des fins de marketing direct et un cadre de bonnes pratiques constitue une de ces actions. Afin de garantir une approche harmonisée de cette interprétation et de ces bonnes pratiques, l'APD s'appuie notamment sur l'ensemble des lignes directrices pertinentes adoptées par le Contrôleur européen de protection des données (ci-après « EDPB »).

L'EDPB n'a toutefois pas adopté de lignes directrices générales relatives au marketing direct en tant que tel. Si tel devait être le cas, et tenant compte de toute position européenne future liée à la présente recommandation, l'APD en tiendra compte et adaptera si nécessaire le contenu de la présente recommandation.

## B. Contexte et champ d'application de la recommandation

6. De nombreux acteurs recourent aux communications de marketing direct, quotidiennement, à l'attention de millions de personnes concernées. Ces communications impliquent des traitements de données à caractère personnel. La régularité, la sophistication et la multiplication de ces traitements de données ainsi que des opérateurs actifs en la matière est un terrain propice à la répétition de certaines pratiques qui peuvent s'avérer parfois en contradiction avec les règles du RGPD. A l'adage du marketing « *adresser le bon message à la bonne personne au bon moment* », il vous faut ajouter « *de la bonne manière* », car le RGPD fait désormais partie intégrante de vos campagnes marketing.
7. Si celui-ci peut apparaître comme un cadre de règles contraignantes pour certains responsables de traitement dans le cadre du marketing direct, le RGPD est également un allié incontournable et utile dans votre relation avec les personnes concernées, que celles-ci soient clientes, prospects, membres, abonnés ou encore électeurs. C'est en communiquant avec ces dernières en toute transparence quant à vos



traitements de données à caractère personnel et en démontrant que vous mettez en place les mesures adéquates afin de garantir que ces traitements sont conformes que vous établirez une relation de confiance nécessaire à la réalisation et à la pérennité de vos objectifs. Le RGPD est dès lors également une véritable opportunité et un argument concurrentiel de premier ordre.

8. Afin de répondre au mieux aux questions soulevées dans ce domaine, l'APD a lancé en date du 12 juillet 2019 une consultation publique à l'attention des responsables de traitement actifs dans le marketing direct afin de les interroger sur les difficultés rencontrées depuis l'entrée en vigueur du RGPD.
9. Il en est ressorti principalement que la Recommandation n°02/2013 du 30 janvier 2013 relative au marketing direct et à la protection des données ne donnait pas de réponse à toutes les questions nées suite à l'adoption du RGPD et/ou de la sophistication des techniques de marketing direct, lesquelles sont principalement liées à la possibilité de trouver une base juridique pour légitimer les traitements de données à caractère personnel envisagés, à l'exercice des droits des personnes concernées, ou encore à l'appréhension de la notion même de marketing direct qui n'est pas définie par le RGPD.



La présente recommandation a pour objet d'aider les responsables de traitement recourant à des techniques de marketing direct (ou y participant) à acquérir les bons réflexes afin d'agir en conformité avec les règles du RGPD applicables. Elle examine dès lors les questions fréquemment posées relatives à la protection des données à caractère personnel dans le cadre du marketing direct. La Recommandation tient également compte, le cas échéant, de la multitude d'acteurs pouvant interagir avec les responsables de traitement mais s'adresse principalement à ces derniers.

La Recommandation ne se limite pas aux seules communications réalisées dans le cadre du marketing direct mais examine également l'ensemble des traitements de données à caractère personnel réalisés à cette fin et les règles qui s'y appliquent.

Les règles, concepts et principes développés dans cette Recommandation le sont sur la base du RGPD et ne tiennent pas compte d'autres législations applicables. La Recommandation n'a cependant pas non plus vocation à être une étude exhaustive du RGPD. Cela ne signifie pas que les responsables du traitement effectuant des traitements de données pour des finalités de marketing direct sont dispensés du respect de l'ensemble des règles qui leurs sont applicables, en ce compris celles édictées par le RGPD et qui ne font pas l'objet de l'examen fourni par cette recommandation, tel que le respect de l'ensemble des droits accordés aux personnes concernées prévus aux articles 12 à 22 du RGPD ou encore en matière de transferts internationaux tels qu'encadrés par le Chapitre V du RGPD.

Les points examinés sont illustrés par des situations propres au marketing direct. Chaque exemple n'implique pas pour autant un examen approfondi et exhaustif des différentes questions ou problèmes de conformité au RGPD.

La Recommandation fait également état de certaines sanctions adoptées par les Autorités de protection des données en la matière. Certaines de ces décisions sont toutefois susceptibles d'appel ou autres voies de recours au moment de l'adoption de la Recommandation. Ces décisions sont donc susceptibles d'être révisées, le cas échéant.



## C. Cadre juridique

10. Lorsque l'on aborde la thématique du marketing direct, différents textes de loi sont susceptibles de trouver à s'appliquer. Cette recommandation se concentre sur les questions de traitement de données à caractère personnel en marketing direct à l'aune du RGPD. Il n'y sera donc fait référence qu'aux règles de ce dernier.
11. L'analyse des règles du RGPD est faite à l'appui, le cas échéant, des positions du Comité européen pour la protection des données (ci-après « EDPB »<sup>7</sup>) et de celles de son prédécesseur, le Groupe de travail Article 29 (ci-après « Groupe 29 »). Certaines des Lignes Directrices de ce dernier ont été revues et actualisées par l'EDPB et d'autres adoptées en tant que telles<sup>8</sup>. D'autres sont actuellement soumises à révision mais sont, au jour de l'adoption de cette Recommandation, toujours d'application. D'éventuelles mises à jour seront apportées à la présente, le cas échéant. L'EDPB est également amené à adopter des prises de position concernant des questions ou thématiques qui n'ont pas encore fait l'objet de prises de position précédentes. Il en va notamment ainsi d'une position attendue et en cours de préparation sur le ciblage des utilisateurs de réseaux sociaux. Les prises de position de l'APD le sont sans préjudice des prises de position à venir de l'EDPB qui impliqueraient, le cas échéant, certaines adaptations de cette Recommandation (l'APD étant partie de l'EDPB et lié par ses prises de position). Veuillez donc rester attentifs aux versions qui pourraient être successivement publiées sur le site Internet de l'APD.
12. A toutes fins utiles et dans la mesure où celle-ci permet d'apporter des éclaircissements quant à ces questions, la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002<sup>9</sup> *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques* (ci-après « e-Privacy Directive ») sera abordée. Il est à ce propos essentiel de garder à l'esprit que cette Directive est actuellement soumise à révision. Le Règlement appelé à remplacer celle-ci étant toujours en discussion à la date de publication de cette Recommandation, il est renvoyé, lorsqu'elle est abordée, aux articles actuellement en vigueur et il n'est pas pris position sur les éventuelles interactions entre ce futur Règlement et le RGPD. Au besoin, la présente Recommandation sera complétée après l'entrée en vigueur dudit Règlement. Pour plus d'informations quant aux interactions qui se nouent entre le RGPD et la e-Privacy, l'Autorité renvoie le lecteur à l'opinion 5/2019 de l'EDPB adoptée à ce sujet en date du 12 mars 2019<sup>10</sup>.

---

<sup>7</sup> le Contrôleur européen est généralement désigné par son nom anglais « European Data Protection Board » ainsi que par l'acronyme y attaché « EDPB ».

<sup>8</sup> Pour une liste complète des différentes décisions prises, adaptées ou confirmées par l'EDPB : [https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices\\_en](https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en).

<sup>9</sup> Cette Directive, revue en 2006, est transposée dans notre droit national par la loi du 13 juin 2005 relative aux communications électroniques, et telle qu'inscrite au livre VI du Code de droit économique par la loi du 21 décembre 2013 portant insertion du titre VI " Pratiques du marché et protection du consommateur " dans le Code de droit économique et portant insertion des définitions propres au livre VI, et des dispositions d'application de la loi propres au livre VI, dans les Livres Ier et XV du Code de droit économique

<sup>10</sup> Opinion 5/2019 *on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*, disponible via le lien suivant :

[https://edpb.europa.eu/sites/edpb/files/files/file1/201905\\_edpb\\_opinion\\_eprivacydir\\_gdpr\\_interplay\\_en\\_0.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf)



## II. Le marketing direct : de quoi parlons-nous ?

### A. Le marketing direct c'est

#### 1. Définition

13. L'APD retient la notion de « marketing direct » dès lors que le terme « prospection » mentionné au considérant 47, ou encore à l'article 21.2 du RGPD au terme de « prospection », est généralement comprise comme visant uniquement l'action de démarcher de nouveaux clients, distinguant ainsi entre les prospects et les clients existants. Or, les règles du RGPD applicables au marketing direct le sont tant aux communications adressées aux « prospects » qu'à celles adressées aux anciens et actuels clients, membres ou abonnés. En outre, ces règles ne se limitent pas au domaine de l'activité commerciale mais s'étendent, plus largement, à toute forme de promotion, dans son acceptation commerciale (incluant la promotion à des fins de vente, à des fins publicitaires, électorales ou d'accroissement de la visibilité mais excluant la promotion non lucrative de la santé publique ou d'autres formes de comportements et pratiques encouragés par les autorités publiques dans le cadre de l'exercice de leurs missions). Enfin, elles ne visent pas uniquement la communication en tant que telle mais également l'ensemble des traitements réalisés dans le cadre d'opérations de marketing. Les traitements de données personnelles effectués afin d'adapter (automatiquement) le prix d'un produit ou d'un service sur la base d'un profil client constituent des opérations de marketing direct<sup>11</sup>

14. Le RGPD ne définit pas ce qu'il y a lieu d'entendre par « marketing direct ». Il n'existe pas à ce jour de définition légale, officielle ou communément admise à l'échelon européen de cette notion. En prenant appui sur la Recommandation n°02/2013 du 30 janvier 2013 de notre prédécesseur relative au marketing direct et à la protection des données d'une part, et à la Proposition de règlement du Parlement européen et du Conseil du 18 septembre 2019 concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE<sup>12</sup> l'Autorité propose de définir ce qu'il y a lieu de comprendre par marketing direct comme suit :



Toute communication, sollicitée ou non sollicitée, visant la promotion d'une organisation ou d'une personne, de services, de produits, que ceux-ci soient payants ou gratuits, ainsi que de marques ou d'idées, adressée par une organisation ou une personne agissant dans un cadre commercial ou non commercial, directement à une ou plusieurs personnes physiques dans un cadre privé ou professionnel, par n'importe quel moyen, impliquant le traitement de données à caractère personnel.

<sup>11</sup> Joseph Turow, Lauren Feldman et Kimberly Meltzer, Open to exploitation: American shoppers online and offline, Annenberg Public Policy Center of the University of Pennsylvania, s.l., 2005, p.36.

<sup>12</sup> Le texte est disponible via le lien suivant :

[https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST\\_12293\\_2019\\_INIT&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_12293_2019_INIT&from=EN)





## 2. Notions clés

### ♦ Toute communication, sollicitée ou non sollicitée

15. Cette définition recouvre tout type de communication, que celles-ci visent la promotion de produits ou services, la promotion d'idées, proposées ou soutenues par une personne ou une organisation, mais également la promotion de cette personne ou organisation elle-même, en ce compris de son image de marque ou des marques dont elle est titulaire ou qu'elle exploite, à l'exclusion de la promotion effectuée à l'initiative des autorités publiques agissant strictement dans le cadre de leurs obligations légales ou missions de service publique pour les services dont elles sont seules en charge.

#### Exemple 1

Une société qui vend des produits d'entretien contacte les clients référencés dans son listing afin de leur faire savoir que ses produits sont écoresponsables.

#### Exemple 2

Une ONG envoie un courrier postal de mobilisation pour une nouvelle campagne à sa liste d'adhérents et donateurs.

#### Exemple 3

Un parti politique adresse une invitation à ses contacts pour les inviter à participer à une journée de rencontres et d'animations pour fêter la rentrée.

16. Il est donc important de garder à l'esprit que la notion de « marketing » ne doit pas être nécessairement entendue comme une communication poursuivant un but commercial ou à finalités lucratives.

17. En outre, la notion de communication de marketing direct vise autant les communications sollicitées que les non sollicitées.

#### Exemple 4

Madame Verdura contacte le collectif « Raconte-moi des salades », qui met gratuitement à disposition des informations variées relatives au jardinage et vend, sur sa plateforme en ligne, des produits naturels pour aider les plantes à pousser. Madame Verdura remplit le formulaire mis en ligne de contact simplifié pour leur demander quel produit utiliser pour se débarrasser naturellement des limaces qu'elle a dans son jardin. Afin de recevoir une réponse à sa demande, elle doit indiquer son adresse e-mail.

Madame Verdura reçoit rapidement une réponse « technique » à sa question (le nom générique de la substance généralement utilisée pour combattre les limaces) avec une offre relative à leur produit miracle pour venir à bout de ces indésirables. Et quelques jours plus tard, elle reçoit la newsletter de « Raconte-moi des salades ».



#### Exemple 4 (suite)

- ✓ La réponse technique n'aurait pas constitué du « marketing direct » sans l'addition d'un message vantant les mérites du produit-miracle du vendeur.
- ✓ L'envoi de la newsletter implique plusieurs traitements de données à des fins de marketing direct.

18. Enfin, la notion de marketing direct ne vise pas les publicités apparaissant de façon aléatoire sur Internet, telles que des bannières de publicité pour autant que celles-ci apparaissent à tout visiteur du site en question, sans aucun lien avec une collecte/utilisation de données à caractère personnel. Si une bannière publicitaire apparaît à l'écran de manière ciblée, par exemple en raison de l'historique de navigation du visiteur, il s'agit de marketing direct. Il en va de même pour les tracts distribués dans toutes les boîtes aux lettres du Royaume, d'une Région ou d'une commune. Le « toute boîte » n'est a priori pas un outil de marketing direct. Néanmoins, si par exemple des tracts publicitaires sont distribués spécifiquement dans les boîtes aux lettres **des personnes qui ne sont pas encore clientes** d'une enseigne établie dans leur quartier, pour les inviter à venir tester ses produits, il s'agira de marketing direct.

19. Toute communication de marketing qui n'implique pas le moindre traitement de données à caractère personnel est exclue de la notion de marketing direct et donc du champ d'application des règles issues du RGPD.

♦ **Visant la promotion d'une organisation ou d'une personne, de services, de produits, que ceux-ci soient payants ou gratuits, ainsi que de marques ou d'idées**

20. Les communications de marketing direct ont pour but de promouvoir quelque chose, sans pour autant que cette promotion doive nécessairement porter sur des biens ou sur des services.

#### Exemple 5

Monsieur Engagé reçoit régulièrement des e-mails d'une association de lutte contre la pollution. Cette association informe ses membres des différentes actions menées à travers le monde. Elle ne demande ni support financier, ni ne propose de services ou de biens.

- ✓ Les e-mails envoyés sont toutefois soumis aux règles du marketing direct car il font la promotion des actions menées par l'ONG et promeuvent son image envers le public.

21. En revanche, les règles relatives au marketing direct ne s'appliquent pas lorsqu'il est pris contact avec des personnes, par exemple des consommateurs, pour réaliser une **étude de marché, un sondage ou une enquête de satisfaction**, pour autant que la communication soit réalisée dans cet unique but.

22. Cette exception ne s'applique pas dans le cas où l'étude de marché ou le sondage a également pour but de vendre ou de promouvoir des biens ou des services, ou encore s'il permet de collecter des données à caractère personnel qui seront ultérieurement utilisées pour des finalités de marketing. Si telle est



l'intention, celle-ci doit être claire et les personnes auxquelles l'étude, l'enquête ou le sondage est envoyé doivent en être clairement informées. En conséquence également, les règles encadrant le marketing direct s'appliqueront.



Si une communication est adressée aux personnes concernées sous couvert de sondage ou d'étude de marché sans dévoiler que les finalités réelles ou, à tout le moins, l'une d'elles est une finalité de marketing direct, il y a détournement de finalité et donc violation des règles du RGPD. Cela pourrait également constituer une violation de la ePrivacy Directive si la communication est faite sans le consentement de la personne alors qu'il y avait lieu de le demander.

23. Enfin, des communications adressées par les administrations publiques promouvant certaines campagnes (par exemple de vaccination), ou services (par exemple les centres téléphoniques d'aide aux personnes en difficulté) dont elles sont en charge légalement ou par mission de service public, ne sont pas considérées comme des communications de marketing direct à moins qu'elles ne fassent en parallèle la promotion de services ou de produits spécifiques, proposés par des prestataires privés.

#### Exemple 6

Une administration publique en charge des tâches relatives à la santé adresse directement aux personnes concernées selon des critères d'âge et/ou de sexe, des messages de sensibilisation à certaines maladies comme le papillomavirus pour les personnes de sexe féminin d'une certaine tranche d'âge, ou les oreillons en cas d'épidémie pour prévenir les parents d'enfants en bas âge ou encore la grippe, pour les personnes les plus vulnérables en raison de leur âge plus avancé.

Ce type de communication n'est pas une communication de marketing direct.

Par contre, si dans cette communication, il est fait mention du nom du vaccin XX développé par la société pharmaceutique XY, cette communication sera considérée comme du marketing direct et devra dès lors répondre aux règles qui l'encadre.

#### ♦ Par qui ?

24. Les communications visées par les règles de marketing direct peuvent être adressées par tout type d'organisations poursuivant ou non un but commercial. Il peut donc s'agir de communications réalisées par des sociétés poursuivant des buts lucratifs mais également par des ASBL, des fondations, des autorités publiques. Il peut également s'agir de personnes ne poursuivant aucun but de profit, pour autant que leurs communications visent à promouvoir quelque chose comme des actions menées par elles (par exemple l'administration publique qui fait la promotion du vaccin de la société XY), des idées ou positions, à moins que celles-ci ne soient effectuées dans le cadre d'activités purement et strictement privées et domestiques.



### Exemple 7

« Natura First », une ONG de protection de la nature contacte les personnes ayant accepté de faire une donation pour pouvoir confirmer leurs coordonnées bancaires. Si la prise de contact se limite à cette vérification, les règles en matière de marketing direct ne s'appliquent pas car elle ne fait pas de promotion d'idées, de services ou de produits.

Si à cette occasion, les personnes sont encouragées à faire d'autres donations ou s'il est fait mention de toute information quant aux campagnes menées, il s'agira de marketing direct et les règles en la matière seront d'application.

### Exemple 8

Un mandataire politique adresse ses vœux de bonne année à plusieurs de ses contacts issus de son compte privé de média social, par message privé depuis son compte privé. Limité aux vœux, le message envoyé n'est pas une communication de marketing direct.

- ✓ S'il ajoute à son message des informations relatives aux différentes actions et campagnes menées au cours de l'année écoulée et sur celles à venir, il s'agira de marketing direct.
- ✓ S'il utilise sa liste de contacts issue de son compte public de média social ou de toute autre source dont il ne dispose pas à titre purement privé, pour envoyer des messages privés de bons vœux, il s'agit de marketing direct.

25. Le raisonnement tenu dans l'exemple ci-dessus est également applicable aux organisations non commerciales, telles que celles actives dans les activités de charité.

26. En revanche, le marketing direct n'inclut a priori pas les communications réalisées par des autorités publiques agissant dans le cadre de leurs obligations légales ou exerçant leurs missions de service public. Si toutefois celles-ci adressent directement à certains administrés des communications faisant la promotion d'un service ou d'une organisation privé(e) et spécifique, les règles du marketing direct trouvent à s'appliquer.

27. Enfin, les communications de marketing direct ne visent pas les communications adressées par des personnes physiques dans le cadre d'activités purement domestiques, au sens de l'article 2 et du considérant 18 du RGPD qui exclut de son champ d'application les traitements de données à caractère personnel effectués par une personne physique dans le cadre d'activités strictement personnelles ou domestiques (par exemple l'envoi d'un faire-part de mariage pour venir assister à l'évènement et la tenue d'une base de données reprenant les réponses), et donc sans lien avec une activité professionnelle ou commerciale.

### Exemple 9

Lucie va fêter ses 18 ans. Pour l'occasion, ses parents invitent tous ses amis à venir la fêter et à faire du karting. Pour autant que l'anniversaire ne soit pas sponsorisé par l'établissement qui gère le karting et que les parents ne fassent pas gagner des T-shirts et Pass gratuits offerts par cet établissement pour toutes les personnes qui viendront à l'anniversaire, l'invitation ne constitue évidemment pas une action de marketing direct.



### ♦ Vers qui ?

28. La communication doit être dirigée vers une ou plusieurs personne(s) physique(s), identifiée(s) ou identifiable(s).
29. La notion de « personne physique identifiée ou identifiable » est intrinsèquement liée à la définition de la donnée à caractère personnel qui conditionne l'application du RGPD.
30. Dès que la communication faite est adressée à une personne, nominativement ou à partir d'informations relatives à cette personne (telle que son adresse IP par exemple), permettant d'entrer en communication avec elle, on parle de marketing direct, pour autant que soient rencontrés les autres critères de la définition.

#### Exemple 10

En visitant le site Internet « Cherry on the cake », une enseigne de matériel de cuisine, Monsieur Sosweet passe quelques minutes à regarder les différents modèles de moules à gâteaux proposés à la vente. Pas décidé à acheter, il quitte le site Internet et se connecte à sa boîte mail. Il voit alors apparaître, à la droite de son écran, une fenêtre pop-up qui lui montre les différents modèles de moules à gâteaux consultés, avec la mention « Une envie de cuisiner ? Cliquez ici ! ».

- ✓ Cherry on the cake a installé des cookies sur l'ordinateur de Monsieur Sosweet, permettant de collecter des informations telles que son adresse IP et les produits sur lesquels il a cliqué. Sur la base de ces données, Cherry on the cake a pu tracer la navigation de Monsieur Sosweet et faire apparaître en pop-up des communications de marketing direct ciblées qui apparaissent dans l'espace d'affichage mis à disposition sur la page de l'hébergeur du compte e-mail de Monsieur Sosweet.
- ✓ Le message apparaissant dans la fenêtre pop-up est encadré par les règles du marketing direct.
- ✓ L'utilisation de cookies par Cherry on the cake à des fins de marketing direct doit répondre aux règles du RGPD mais également de la e-Privacy Directive que nous n'examinons pas dans la présente Recommandation.

31. En outre, que la communication soit faite à une personne dans le cadre de sa vie « privée », par exemple via son adresse e-mail personnelle, ou dans le cadre de ses activités professionnelles, via son adresse e-mail professionnelle, cela reste du marketing direct pour autant que les autres critères de la définition soient rencontrés.



### Exemple 11

La société « Hi Tech » envoie l'un de ses collaborateurs visiter un salon organisé par « Technologia » dédié aux nouvelles technologies. Plusieurs enseignes y sont présentes à des stands de présentation, des conférences et workshops y sont également organisés. Après avoir participé à l'un de ces workshop, le collaborateur remplit un formulaire de satisfaction sur le workshop mais également, plus généralement, relatif à l'ensemble de l'organisation du salon. Il est invité à y indiquer ses coordonnées ainsi que le nom de sa société dès lors qu'il serait venu à titre professionnel. Le formulaire précise « *vous nous autorisez à faire usage de vos données afin de communiquer sur nos prochains évènements et salons* ». Afin d'aller plus rapidement, les participants sont également invités à laisser leurs cartes de visites au lieu de remplir le formulaire. Ils doivent, pour cela, déposer leurs cartes dans la boîte dédiée à cet effet. Le collaborateur est pressé, il laisse une carte de visite qui mentionne ses nom, prénom et adresse e-mail ainsi que l'ensemble des coordonnées de la société Hi Tech.

- ✓ Si les organisateurs du salon adressent ultérieurement des communications sur leurs prochains évènements à la société Hi Tech, sur la base des données générale de contact fournies (sans indication des nom et prénom du collaborateur ni de sa fonction spécifique) , il ne s'agit de marketing direct car il n'y a pas de traitement de données à caractère personnel ;
- ✓ Si ces mêmes communications sont adressées au collaborateur d'Hi Tech sur la base des coordonnées professionnelles indiquées sur sa carte de visite déposée au stand du workshop, les règles de protection des données applicables au traitement de données en matière de marketing direct sont d'application, même s'il s'agit de ses coordonnées professionnelles. Cela implique notamment que les coordonnées du collaborateurs ne peuvent pas être utilisées à d'autres fins que celles indiquées dans le formulaire et donc, qu'il n'est pas question de lui envoyer des communications de marketing direct sur autre chose que les évènements et salons organisés par Technologia elle-même.

### Exemple 11bis

Imaginons que le collaborateur de la société Hi Tech ait spontanément donné sa carte de visite à certains participants ou personnes rencontrées lors de cet évènement, que ce soit pour rester en contact si nécessaire ou simplement dans l'idée de se revoir à l'occasion.

L'une des personnes à qui il donne sa carte décide, de retour dans sa propre organisation, encode ses coordonnées, ainsi que toutes les autres coordonnées récupérées de la sorte, dans sa base de données, afin d'envoyer des communications relatives aux produits et services de sa société.

- ✓ En distribuant sa carte de visite, le collaborateur n'a pas consenti à ce que ses données soient traitées pour des finalités de marketing direct ;
- ✓ Un tel traitement des données à caractère personnel dépasse la finalité pour laquelle la carte de visite a été donnée au départ.

## 32. Enfin, **sans préjuger des conditions nécessaires en vue d'assurer la légalité des communications**

**adressées à ces personnes**, les communications adressées à un prospect, à une personne intéressée ou à un client/affilié/abonné/membre, sont tout autant des communications de marketing direct, pour autant qu'elles visent la promotion de vos produits, de vos services, de votre image de marque, de votre entreprise ou encore de vos idées.



33. Un prospect ou une personne intéressée (par exemple un client potentiel qui a demandé de nombreuses informations au sujet de vos produits ou services, ou de votre organisation) se distingue de vos clients, abonnés, affiliés, membres existants dès lors que les premiers n'ont pas encore acheté un produit auprès de votre organisation, convenu de la prestation de l'un de vos services, ou adhéré avec un engagement ferme à ce que vous proposez. Par contre, à la différence d'une personne intéressée, un prospect « pur » n'entretient aucune relation avec vous.

#### ♦ Par quels moyens ?

34. Les communications de marketing direct peuvent prendre plusieurs formes. La distinction la plus évidente consiste à séparer les communications électroniques des communications non électroniques.

35. Les communications non électroniques recouvrent les envois postaux ou les interactions humaines sans recours à des moyens techniques électroniques, tel que le porte à porte par exemple, lorsque celui-ci vise à conclure la prestation d'un service ou une vente et implique le traitement de données à caractère personnel **appelées à figurer dans un fichier**. La notion de fichier est importante car elle encadre le **champ d'application matériel du RGPD**.

#### Exemple 12

L'amicale des scouts fabrique chaque année des biscuits qu'ils vont vendre afin de récolter des sous pour préparer les camps d'été, acheter du matériel et améliorer leur locaux. Ils envoient pour les vendre certains scouts qui ont pour mission de faire du porte à porte avec les boîtes de biscuits. Ils sonnent aux portes d'un maximum de maisons et appartements en espérant récolter le plus d'argent possible pour les aider.

- ✓ Si les scouts sonnent aux portes de manière totalement aléatoire en se contentant de vendre les biscuits, il n'y a pas de marketing direct car aucune données à caractère personnel n'est contenues ou appelées à figurer dans un fichier organisé (telle qu'une liste de maisons précises ou un listing nominatif des personnes ayant acheté une boîte de biscuits) ;
- ✓ Si par contre le scouts sont envoyés par l'amicale à des maisons ou appartements bien spécifiques, pour y vendre des boîtes à des personnes identifiées sur la base, par exemple, d'une liste établie les années précédentes pour identifier les personnes ayant déjà acheté, il s'agira de marketing direct car la démarche implique un traitement de données à caractère personnel figurant dans un fichier.

36. Les communications électroniques visent quant à elles les communications textuelles, vidéos, photos, imagées ou sonores effectuées à l'aide de moyens issus de la technologie, tels que les appels téléphoniques, les SMS, les MMS, les e-mails, les chat-box, les pop-up ou autres encarts publicitaires dont le contenu est directement lié à un traitement de données à caractère personnel. Ces traitements peuvent se faire selon différentes techniques et/ou technologies telles que le ciblage<sup>13</sup> (en ce compris le microtargeting) ou le real

<sup>13</sup> Le ciblage (ou *targeting*) permet la sélection de clients potentiels en fonction de leurs données à caractère personnel, notamment de leur comportement de navigation sur Internet.



time bidding<sup>14</sup> et sur différents canaux tels que les plateformes de réseaux sociaux faisant apparaître du contenu personnalisé en fonction des préférences des titulaires de compte. A cet égard, l'Autorité attire l'attention sur l'élaboration en cours de lignes directrices par l'EDPB concernant spécifiquement la question du ciblage d'utilisateurs de réseaux sociaux. Toute position y relative développée dans la présente recommandation sera le cas échéant revue afin d'être conforme à la position qui sera adoptée sur ce point par l'EDPB.

### III. Marketing direct et protection des données à caractère personnel : comment agir en conformité ?

#### A. Acteurs du marketing direct et rôles définis par le RGPD

37. Les personnes, physiques ou morales, intervenant dans les traitements de données à caractère personnel nécessaires à vos activités de marketing peuvent être nombreuses et les relations nouées avec elles parfois complexes. Vous faites probablement appel, en tant que responsable de traitement, aux services de différents partenaires qui peuvent agir tantôt comme purs sous-traitants, tantôt comme responsables conjoints de traitement avec vous. Il est important que vous déterminiez les rôles de chacun afin d'appréhender correctement vos obligations et les leurs.

##### 1. Responsable du traitement et responsables conjoints

38. Vous êtes « responsable du traitement » lorsque, **seul ou conjointement**, vous déterminez les finalités et les moyens d'un traitement de données à caractère personnel.

39. Il est important de se rappeler qu'une organisation n'est pas responsable du traitement ou sous-traitant « par nature ». Tout dépend de la manière dont elle se comporte dans les faits. Vous devez vous demander, pour chaque opération que vous effectuez avec des données à caractère personnel, qui détermine les finalités de traitement et la manière dont le traitement de données en question est effectué.

40. Afin de clarifier votre rôle, et celui des autres intervenants (tels que vos fournisseurs de services techniques ou encore des tiers qui vous fournissent des données) demandez-vous :

- ✓ qui décide de collecter des données personnelles en premier lieu et le(s) type(s) de données personnelles à recueillir ;

---

<sup>14</sup> Le real time bidding est une technique publicitaire permettant aux régies publicitaires travaillant pour des annonceurs de remporter un espace publicitaire disponible sur une page Internet et mise aux enchères au plus offrant. Afin d'être intéressés à l'un de ces espaces publicitaires disponibles, les régies publicitaires examinent les informations disponibles quant à l'emplacement lui-même mais également sur les utilisateurs de la page Internet concernée, afin de savoir si le public cible de leur campagne de publicité correspond afin de favoriser un marketing encore plus ciblé.





- ✓ qui détermine les personnes ou catégories de personnes visées ;
- ✓ qui décide des données ou catégories de données à collecter ;
- ✓ qui détermine la ou les finalités pour lesquelles les données doivent être utilisées ;
- ✓ qui détermine et s'assurer de la base juridique pour le faire (consentement, obligation légale, intérêt légitime, etc) ;
- ✓ qui détermine s'il y a lieu de communiquer les données et, dans l'affirmative, à qui ;
- ✓ qui détermine le contenu de l'information à fournir aux personnes concernées au sujet du traitement ou des opérations de traitement appliqué(es) à leurs données ;
- ✓ qui détermine la durée de conservation des données ; et
- ✓ qui détermine la façon de répondre aux personnes concernées dans le cadre de l'exercice de leurs droits.

41. Toutes ces décisions ne peuvent être prises que par le responsable du traitement dans le cadre de son contrôle global du traitement des données. Si vous prenez l'une de ces décisions, vous êtes plus que probablement responsable du traitement.

42. L'article 26 du RGPD prévoit également la situation dans laquelle coexistent deux ou plusieurs responsables, dit « responsables conjoints » du traitement. Tel est le cas lorsque plusieurs opérateurs/organisations déterminent ensemble les finalités et les moyens du traitement. L'article 26 du RGPD prévoit que dans ce cas, les responsables conjoints doivent définir leurs obligations respectives de manière transparente par voie d'accord entre eux qui reflète dûment leurs rôles respectifs envers les personnes concernées.

### Exemple 13

L'enseigne des magasins « Bon prix » décide de mettre en place une plateforme Internet commune avec d'autres enseignes de magasins telles que « The Good one » et « Vous c'est Nous », afin d'améliorer leur collaboration en tant que partenaires commerciaux. Cette plateforme vise notamment à interagir avec leurs clientèles respectives et/ou communes. Ensemble, les partenaires se mettent d'accord sur des éléments importants, telles que les catégories de données collectées, qui peut accéder aux informations, l'information fournie aux personnes concernées ou encore les mesures de sécurité à prévoir. Par ailleurs, ils décident également de partager les données à caractère personnel de leurs clients afin de réaliser des actions de marketing plus pertinente.

- ✓ Dans ce cas, l'enseigne Bon prix et les autres enseignes participantes sont responsables conjoints puisqu'elles décident de la manière dont les données de leurs clientèles respectives vont être traitées, comment et pourquoi.

43. Si vous traitez des données à caractère personnel en collaboration avec certains partenaires qui eux-mêmes poursuivent leurs propres finalités et déterminent des moyens de traitement, vous devez impérativement vous conformer à l'article 26 du RGPD et prévoir par voie d'accord vos rôles respectifs afin, notamment d'agir en toute transparence envers les personnes concernées.



## CJUE, arrêt C-40/17 « Fashion ID » du 29 juillet 2019

La CJUE a décidé, dans son arrêt « *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV* » que le gestionnaire d'un site Internet équipé du bouton « j'aime » de Facebook peut être conjointement responsable avec Facebook de la collecte et de la transmission à Facebook des données à caractère personnel des visiteurs de son site.

Elle avait déjà pu décider qu'une personne morale ou physique qui influe, à des fins qui lui sont propres, sur le traitement de données à caractère personnel et **participe de ce fait** à la détermination des finalités et des moyens de ce traitement peut être considérée comme étant responsables du traitement (arrêt du 10 juillet 2018, *Jehova todistajat*, C-25/17, point 68). Elle avait également décidé que la responsabilité conjointe de plusieurs acteurs pour un même traitement **ne présuppose pas que chacun d'eux ait accès aux données** à caractère personnel concernées (arrêt du 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-201/16, point 38), **ni** que chacun de ces responsables de traitement ait **une responsabilité équivalente** mais qu'au contraire, ceux-ci peuvent être impliqués à **différents stades de ce traitements et selon différents degrés**, de telle sorte que le niveau de responsabilité de chacun d'eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce.

En insérant un bouton « j'aime » de Facebook sur son site Internet, Fashion ID offre consciemment à Facebook Ireland la possibilité d'obtenir des données à caractère personnel des visiteurs de son site Internet au moment où ceux-ci consultent ledit site Internet, indépendamment du fait que ces visiteurs aient ou non un compte Facebook ou même qu'ils aient cliqué sur le bouton « j'aime » et ce, sans qu'ils n'en soient tenus informés (points 75 et 77 de l'arrêt). En insérant un tel bouton, Fashion ID influe donc de manière déterminante sur la collecte et la transmission des données à caractère personnel des visiteurs de son site au profit du fournisseur de ce bouton, à savoir Facebook.

**Quant aux finalités**, la CJUE précise que l'insertion par Fashion ID du bouton « j'aime » sur son site Internet lui permet **d'optimiser la publicité pour ses produits en les rendant plus visibles sur le réseau social Facebook** lorsqu'un visiteur de son site Internet clique sur ledit bouton. Fashion ID a, à tout le moins implicitement, consenti à la collecte et à la communication par transmission des données à caractère personnel des visiteurs de son site Internet, afin de pouvoir bénéficier d'un avantage commercial consistant en une publicité accrue pour ses produits. Les opérations de traitements ainsi effectuées le sont dès lors tant dans l'intérêt économique de Facebook que de Fashion ID. Dans de telles circonstances, ces deux organisations déterminent donc conjointement les finalités des opérations de collecte et de communication des données à caractère personnel (points 80 et 81 de l'arrêt).

Notez également que lorsque vous faites usage de données à caractère personnel collectées via des médias sociaux, vous ne pouvez pas vous appuyer sur les conditions d'utilisation de ces réseaux sociaux pour informer les personnes concernées dont vous traitez les données à caractère personnel (ou dont les données sont traitées par votre intermédiaire), sur les différents traitements effectués et finalités poursuivies. Il vous appartient en effet, en tant que responsable du traitement, même conjoint, de fournir une information transparente aux personnes dont vous traitez les données à caractère personnel.



44. Notez également que lorsque vous faites usage de données à caractère personnel collectées via des médias sociaux, vous ne pouvez pas vous appuyer sur les conditions d'utilisation de ces réseaux sociaux pour informer les personnes concernées dont vous traitez les données à caractère personnel (ou dont les données sont traitées par votre intermédiaire), sur les différents traitements effectués et finalités poursuivies. Il vous appartient en effet, en tant que responsable du traitement, même conjoint, de fournir une information transparente aux personnes pour la partie des traitements de données à caractère personnel que vous mettez en œuvre.
45. Cette information porte sur vos traitements qui peuvent impliquer, le cas échéant, une communication de données à des tiers qui doivent être identifiés le plus précisément possible. En outre, les finalités de traitement auxquelles sont destinées les données collectées doivent aussi être clairement identifiées et précisées. Ceci implique dès lors que vous soyez également attentifs aux finalités poursuivies par les tiers avec lesquels vous collaborez et renseigniez également leurs finalités de traitement. Faire un simple renvoi aux politiques d'utilisation des données de ces tiers ne suffit pas toujours à rencontrer les exigences de transparence de l'article 12 du RGPD, au regard principalement de la complexité et de la longueur de ces politiques.

## 2. Sous-traitant

46. Lorsqu'un organisme public ou privé, ou une personne physique traite des données personnelles pour votre compte, sur la base de vos instructions, aux seules fins de vous permettre de réaliser vos finalités, il s'agit d'une situation de sous-traitance.
47. Cette situation de sous-traitance implique de respecter le prescrit de l'article 28 du RGPD.
48. Tout d'abord, retenez qu'en quelque situation que ce soit et face à quelque sous-traitant que ce soit, dès lors que vous agissez en tant que responsable du traitement vous demeurez tenus des obligations que met à votre charge le RGPD et **vous devez répondre, le cas échéant, des manquements à ces obligations**. C'est notamment la raison pour laquelle l'article 28.1 du RGPD vous impose de ne faire appel qu'à des sous-traitants présentant des **garanties suffisantes** quant à la mise en œuvre de mesures techniques et organisationnelles appropriées. Cela procède également de votre obligation prévue à l'article 24 du RGPD qui vous impose la mise en place de mesures techniques et organisationnelles appropriées pour vous assurer que votre traitement de données est effectué conformément au RGPD, et être en mesure de le démontrer. Le recours à un sous-traitant certifié ou ayant adhéré à un code de conduite approuvé peut servir d'élément attestant de l'existence de garanties suffisantes requises par l'article 28.1 et 4 du RGPD.
49. En cas de manquement aux obligations du RGPD, l'article 83 du RGPD prévoit que le responsable du traitement et son sous-traitant peuvent faire l'objet de différentes sanctions par l'Autorité. Une bonne



collaboration entre vous et votre sous-traitant est donc primordiale. Par exemple en cas de violation de données (data breach), l'article 33.2 du RGPD précise que le sous-traitant doit notifier au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. Dès lors que vous, en tant que responsable de traitement, ne disposez que d'un délai de 72 heures pour notifier à l'Autorité toutes violations susceptibles d'engendrer un risque pour les droits et libertés des personnes physiques, mieux vaut vous assurer de ce que votre sous-traitant respectera son obligation de notification.

50. Votre relation avec votre sous-traitant doit impérativement faire l'objet d'un **contrat ou d'un autre acte juridique**, et cet acte ou contrat doit impérativement être écrit, même sous format électronique, et ce afin de vous conformer à votre obligation de documentation et à l'article 30 du RGPD. Ce contrat ou acte juridique doit prévoir l'objet et la durée du ou des traitement(s) ainsi que la ou les finalités et la nature de ces traitements confiés au sous-traitant. Il doit également définir le type de données à caractère personnel traitées, et les catégories de personnes concernées et rappeler vos droits et obligations en tant que responsable de traitement. Enfin, cet acte doit au minimum contenir les précisions énumérées à l'article 28.3, a) à h) du RGPD, en ce compris le fait que le sous-traitant ne peut traiter les données à caractère personnel que sur instructions documentées du responsable de traitement.
51. Si vous n'êtes pas certain du contenu de cet acte qui doit être conclu avec votre sous-traitant, vous pouvez vous inspirer du modèle de clauses contractuelles types adoptées par l'Autorité de contrôle danoise en conformité avec l'article 28 du RGPD et ayant fait l'objet de l'avis 14/2019 du Comité européen de Protection des données<sup>15</sup>. Même si ce modèle de clauses a été adopté par une autre autorité nationale, le RGPD ne fait pas obstacle à ce que des responsables de traitement et sous-traitants ressortissant d'autres Etats-membres s'en inspirent (voir en ce sens le considérant 81 du RGPD)<sup>16</sup>.
52. Si la situation idéale est celle où le responsable du traitement fournit des instructions complètes concernant le traitement confié au sous-traitant, la réalité est parfois moins évidente et il se peut que certains éléments soient déterminés non pas par le responsable du traitement mais par son sous-traitant, au regard de l'expertise dont jouit ce dernier notamment quant aux technologies appliquées au traitement et/ou mesures de sécurisation des données les plus appropriées. Le fait qu'un sous-traitant dispose de plus d'expertise que vous quant aux moyens techniques à utiliser dans le cadre du traitement de données n'est pas, en soi, de nature à mener à une requalification de sa position de sous-traitant en une position de responsable de traitement. Certains sous-traitants proposent des solutions « clés en main » sans que cela n'interfère pour autant avec votre obligation de responsable du traitement de prendre les décisions requises quant aux données traitées, aux finalités poursuivies et/ou aux moyens à mettre en œuvre pour les atteindre.

---

<sup>15</sup> [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_opinion\\_201914\\_dk\\_scc\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf)

<sup>16</sup> Considérant 81 RGPD : « (...) le responsable du traitement et le sous-traitant peuvent choisir de recourir à un contrat particulier ou à des clauses contractuelles types, qui sont adoptées soit directement par la Commission soit par **une autorité de contrôle**(...). »



53. Dans le cadre du contrat à conclure avec vous, un sous-traitant peut prendre des décisions quant à des éléments accessoires relatifs aux moyens du traitements :

- ✓ des systèmes informatiques ou autres méthodes à utiliser pour collecter les données à caractère personnel ;
- ✓ des méthodes de stockage les données personnelles ;
- ✓ des détails des mesures de sécurité visant à protéger les données personnelles ;
- ✓ de la manière dont il transférera les données à caractère personnel d'une organisation à une autre ;
- ✓ de la façon dont il récupérera les données personnelles de certaines personnes ;
- ✓ de la façon dont il s'assurera du délai de conservation des données ; et
- ✓ de la façon dont il supprimera ou éliminera les données.

54. Quelle que soit l'expertise de votre sous-traitant, vous devez rester attentifs à ce qu'il vous propose et à garder la maîtrise de votre traitement. Dès lors que le sous-traitant doit toujours agir selon vos instructions, vous devez rester en mesure de refuser ce qu'il vous propose ou, à tout le moins, le renégocier avant de conclure votre contrat (ou autre acte juridique) avec lui<sup>17</sup>. Hors du cas où il en serait tenu par la loi, un sous-traitant agissant en dehors des instructions de son responsable du traitement est en infraction au RGPD et passibles des sanctions prévues par ce Règlement.

55. En outre, dans la mesure où vous êtes tenus de choisir un sous-traitant qui présente des garanties suffisantes de manière à ce que le traitement réponde aux exigences de conformité au RGPD, vous devez vous assurer de telles garanties avant la mise en place de la sous-traitance et pendant celle-ci. Vous êtes libre de choisir la manière dont vous souhaitez vous en assurer et pouvez, par exemple, prévoir que des contrôles et audits seront effectués à intervalles réguliers afin de vérifier le respect de ses obligations par votre sous-traitant. Le sous-traitant est quant à lui obligé de se conformer à ces audits et d'y contribuer (article 28.3, h) du RGPD).

56. Si un sous-traitant qui traite des données à caractère personnel détermine la/les finalité(s) et les moyens de(s) traitements, il doit être considéré comme responsable du traitement pour ce traitement et devra endosser les responsabilités et obligations qui s'attachent à ce rôle, pour le(s) traitement(s) concernés (article 28.10 du RGPD).

---

<sup>17</sup> Voir en ce sens la décision adoptée par le contrôleur européen (EDPS) concernant les conditions de Microsoft : [https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigation-it-contracts-stronger\\_en](https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigation-it-contracts-stronger_en)



#### Exemple 14

La société « Coconut Tree » fournit des services de communication de marketing et de publicité à différentes entreprises. L'entreprise « Incredible monkey » décide de recourir à ses services et conclut un contrat de sous-traitance avec Coconut Tree. Cette dernière fait toutefois également usage des données clients que lui confie Incredible Monkey pour les enrichir avec d'autres données dont elles disposent et les revendre à d'autres entreprises clientes auprès d'elle.

- ✓ Dans le cadre de cet autre traitement, Coconut Tree n'agit pas comme sous-traitant de Incredible Monkey mais comme responsable de traitement à part entière car elle poursuit ses propres finalités hors cadre des instructions reçues par Incredible Monkey. En outre, la question de la transparence de ces traitements ou encore celle de leur licéité se posent également.

57. **Un même organisme peut agir à la fois en tant que sous-traitant et responsable de traitement ; mais pas pour le même traitement de données à caractère personnel.** Un sous-traitant agissant de la sorte doit s'assurer que ses systèmes et procédures font la distinction entre les données à caractère personnel traitées en sa qualité de responsable du traitement et celles traitées en qualité de sous-traitant. Si certaines des données sont identiques, ces systèmes doivent pouvoir distinguer ces deux situations afin d'appliquer différents processus et mesures à chacune.

58. Sous réserve de la légalité des traitements concernés, **si une organisation agit, en parallèle, en tant que responsable de traitement et en tant que sous-traitant pour des traitements de données différents mais sur la base des mêmes données personnelles, les personnes concernées doivent en être dûment informées : tant par l'organisation qui agit en tant que sous-traitant que par l'organisation qui agit en tant que responsable de traitement.** Il en va notamment ainsi des entreprises qui vous proposent de recourir à leur système de cartes de fidélité et qui gèrent pour votre compte, une base de données reprenant, par exemple, les données des personnes titulaires d'une carte pour votre enseigne, les achats ou catégories d'achats effectués, la fréquence, les périodes et les montants, afin de vous aider à mieux cibler votre clientèle et leurs proposer des promotions plus adéquates. Il se peut que ces mêmes organisations exercent également des activités autre que de la pure sous-traitance en fournissant, par exemple, des « profils de clients » à d'autres enseignes sur la base, notamment, des données collectées via ladite carte de fidélité. L'information à fournir doit porter notamment, sur les différents traitements opérés, les données collectées ainsi que les destinataires de données avec leurs finalités propres.

59. Soyez également attentifs au fait que le RGPD prévoit le cas de la sous-traitance effectuée par des sous-traitants et stipule que lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection des données que celles fixées entre le responsable du traitement et son sous-traitant doivent s'appliquer et donc être imposées au second sous-traitant au moyen d'un contrat ou d'un autre acte juridique (voir en ce sens l'article 28.4 du RGPD). Le sous-traitant doit avoir l'accord préalable, général ou spécifique, du responsable du traitement pour recourir aux services d'un sous-traitant et, en cas d'accord



préalable général, le tenir informé de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections (article 28.2 du RGPD). La relation entre le sous-traitant initial et le sous-traitant ultérieur doit également faire l'objet d'un contrat.

60. Enfin, notez que vos employés ne sont pas vos sous-traitants. Aussi longtemps qu'ils agissent sous votre autorité dans le cadre d'un lien de subordination, ils sont partie intégrante de votre organisation.

### 3. Achat, location, enrichissement de données à caractère personnel

61. De plus en plus, les pratiques de marketing direct impliquent le recours à différentes organisations offrant des services de mise à disposition, par courtage, vente ou location des données à caractère personnel issues de différentes sources, ayant ou non fait l'objet de transformations via enrichissement, couplage de données, avec ou sans profilage. Ces organisations, qu'elles soient principalement occupées en tant que « data brokers » ou d'autres entreprises actives dans l'industrie publicitaire (en ce compris, les entreprises qui louent ou vendent des données relatives à leurs propres clients ou autres contacts), apparaissent parfois comme incontournables pour vous permettre d'atteindre vos objectifs.

62. Tant le nombre et le type d'acteurs opérant dans ce secteur que les sources de provenance des données et les moyens utilisés sont divers et variés. Les données peuvent ainsi être collectées directement auprès des personnes concernées ou indirectement, online ou offline. L'ensemble des opérations de traitement appliqués à ces données à caractère personnel est soumis aux règles du RGPD et donc aux sanctions prévues par l'article 83 du RGPD en cas de non-respect de ces règles.

63. Dans la pratique, il est fréquent que les personnes concernées ignorent que des données à caractère personnel les concernant sont collectées par ces organisations et, a fortiori, ce qu'elles en font. Le rapport « Out of control » publié le 14 janvier 2020 par le Forbrukerradet, membre de l'Union européenne des associations de consommateurs (le « BEUC ») fait état d'une situation répandue de collecte et usage de données à caractère personnel à l'insu des détenteurs et utilisateurs de smartphone<sup>18</sup>. La transparence est pourtant cruciale afin de traiter des données de manière loyale et licite. Il résulte de cette absence de transparence une perte totale de contrôle de leurs données par les personnes concernées et un risque évident pour leurs libertés et droits fondamentaux dès lors qu'elles ne sont même plus en mesure d'exercer leurs droits.

64. Cette obligation de transparence existe dans le chef de tous les organismes qui se transmettent les données à caractère personnel. Les responsables de traitement qui collectent les données directement auprès des

---

<sup>18</sup> Ce rapport est disponible en ligne via le lien suivant : <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/>



personnes concernées (par exemple leurs clients ou prospects) et qui entendent communiquer ces données à des organisations spécialisées dans leur traitement à des fins de marketing direct doivent en informer clairement les personnes concernées, en identifiant, si pas les destinataires spécifiques lorsque cela s'avère (réellement) impossible, à tout le moins les catégories de destinataires concernés (par exemple leur secteur d'activité), les activités poursuivies par ceux-ci (par exemple le type de services ou produits qu'ils proposent) et les traitements de données à caractère personnel qu'ils entendent faire (par exemple de l'enrichissement de ces données avec des données issues de la base de données XY ou de bases de données de type X contenant des données de type Y et la fourniture des données issues de cet enrichissement à des entreprises actives dans le secteur Z aux fins d'utilisation à des fins d'envoi de message publicitaires par e-mail avec une fréquence annuelle maximale de 4 messages par personne ciblée) et recueillir le consentement préalable de ces personnes quant au traitement de leurs données à caractère personnel (dont la liste doit leur être fournie), par ces catégories de tiers, dans le cadre des finalités qu'ils poursuivent et selon les traitements (enrichissement, déduplication, profilage, etc) de données à décrire. Il en va ainsi du respect de l'article 13 du RGPD.

65. De la même façon, une information transparente et claire doit être fournie aux personnes concernées par les organisations qui collectent directement auprès d'elles, ou indirectement auprès de différentes sources, des données à caractère personnel, pour en faire du commerce en tant qu'intermédiaires vers des clients intéressés d'accéder aux listes de données collectées, classées ou non, couplées ou non, enrichies ou non.
66. Si ces organisations spécialisées dans l'agrégation<sup>19</sup>, la revente, la location ou le courtage de données ne fournissent pas une telle information, elles sont en défaut de respecter, soit, l'article 13 du RGPD (dans l'hypothèse où elles collectent ces données directement auprès des personnes concernées, notamment au moyen de questionnaires d'habitude de consommation qu'elles adressent directement aux individus) soit, l'article 14 du RGPD (lorsqu'elles collectent ces données de manière indirecte, par exemple en rachetant des listes de données auprès d'autres organisations), lequel implique également d'identifier la source de provenance des données. Et ce, à moins qu'elles ne puissent justifier le défaut d'information sur la base d'une des hypothèses visées au paragraphe 5 de l'article 14 du RGPD qui implique de démontrer soit que, les personnes concernées ont déjà reçu toute l'information requise, soit que la fourniture de cette information se révèle impossible ou exigerait des efforts disproportionnés.
67. A charge pour les organisations dont le modèle est fondé sur la collecte massive de données à caractère personnel dans le but d'en faire commerce de démontrer qu'elles ne disposent pas des moyens techniques leur permettant, sans engager d'efforts disproportionnés, d'informer les personnes concernées. Dans le cas des modèles actuels les plus fréquemment rencontrés, ces organisations disposent en effet au moins d'une adresse postale ou électronique, permettant de contacter ces personnes de manière directe et certaine Elles

---

<sup>19</sup> Agréger des données à caractère personnel peut notamment revenir à les assembler, à les regrouper, sur la base de correspondances établies au préalable, de clés qui font des liens entre les données ou de modèles plus complexes.





restent en tout état de cause tenues de prendre les mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes des personnes concernées, y compris en rendant cette information publiquement disponible, sur leur site Internet par exemple. Une publication sur le site Internet de votre organisation ne suffit toutefois pas à rencontrer les exigences des articles 13 et 14 du RGPD si vous disposez d'autres moyens pour informer les personnes concernées.

LE SAVIEZ-  
VOUS

?

L'Autorité de protection polonaise a sanctionné une entreprise en date du 25 mars 2019 d'un montant de près de 220.000 euros (PLN 943 000) pour défaut à son obligation d'information.

La infligée concerne une société qui traite, à des fins commerciales, les données de personnes concernées provenant de sources accessibles au public, tel que le registre électronique central, et des informations sur l'activité économique de ces personnes. L'entreprise n'a pas respecté son obligation d'information vis-à-vis de plus de 6 millions de personnes.

L'Autorité a vérifié le non-respect de l'obligation d'information à l'égard des personnes physiques exerçant une activité économique - les entrepreneurs qui exercent actuellement cette activité ou l'ont suspendue, ainsi que les entrepreneurs qui ont exercé cette activité dans le passé. Le responsable du traitement s'est acquitté de l'obligation d'information en fournissant les informations requises en vertu de l'art. 14 (1) - (3) du GDPR uniquement en ce qui concerne les personnes dont il disposait des adresses électroniques.

Dans le cas des autres personnes, le responsable du traitement n'a pas respecté l'obligation d'information - comme il l'a expliqué au cours de la procédure - en raison des coûts opérationnels élevés. Par conséquent, elle n'a présenté la clause d'information que sur son site Web.

L'Autorité polonaise a estimé qu'une telle action était insuffisante dès lors que cette entreprise disposait d'adresses postales et de numéros de téléphones de certaines personnes. Elle pouvait donc se conformer à son obligation d'information à leur égard, c'est-à-dire les informer notamment sur : leurs données, la source de leurs données, le but et la durée du traitement prévu, ainsi que les droits des personnes concernées en vertu du RGDP.

L'Autorité a estimé que l'infraction commise à l'encontre du responsable du traitement était intentionnelle, car - comme il a été établi au cours de la procédure - la société était consciente de l'obligation de fournir les informations pertinentes, ainsi que de la nécessité d'informer directement les personnes.

Si vous souhaitez en savoir davantage sur cette affaire : [https://edpb.europa.eu/news/national-news/2019/first-fine-imposed-president-personal-data-protection-office\\_en](https://edpb.europa.eu/news/national-news/2019/first-fine-imposed-president-personal-data-protection-office_en)

68. Enfin, lorsque vous collaborez avec ces organisations intermédiaires pour améliorer vos campagnes de marketing en récupérant auprès d'elles des données à caractère personnel dont vous ne disposiez pas, vous êtes vous aussi tenus de fournir outre l'information requise aux personnes concernées, conformément à l'article 14 du RGPD, **au plus tard** au moment de votre première communication avec celles-ci.



69. En outre, vous devez vous assurer de la qualité des données que vous obtenez par ce biais. Votre responsabilité implique également que vous preniez soin de sélectionner les partenaires à même de vous garantir de façon effective que les données à caractère personnel ont été collectées de manière licite et loyale. **Il vous appartient de vous assurer de l'origine des données, de la manière dont elles ont été collectées, sur quelle base juridique, par qui, pour quelles finalités, pour quelle durée et quels traitements.**

LE SAVIEZ-VOUS



L'ICO (autorité de protection au Royaume-Uni) a sanctionné la société Rainbow (UK) Limited d'une amende de £20 000 en octobre 2016. Cette dernière avait fait appel aux services de The Data Supply Company Ltd, une entreprise de courtage de données, sans vérifier au préalable que les personnes concernées dont elle avait récupéré les données à caractère personnel avaient, ou non, effectivement consenti à l'utilisation de leurs données à des fins de marketing. L'ICO a enjoint dans sa décision de sanction de procéder à de telles vérifications au titre de *due diligence*.

Notez également qu'en janvier 2017, The Data Supply Company Ltd a elle aussi été sanctionnée par l'ICO d'une amende de £20 000 dans la mesure où les courtiers sont eux aussi tenus de veiller à ce qu'ils traitent les données personnelles "loyalement et licitement". L'ICO a pu préciser que cela signifie notamment qu'ils sont également chargés de s'assurer que les personnes ont été suffisamment informées de la façon dont leurs données personnelles sont traitées - par exemple, que le courtier en données les vend à des organisations particulières à des fins particulières, et qu'ils ne doivent pas prétendre vendre des listes de personnes qui ont consenti à recevoir des textes de marketing, des courriels ou des appels automatisés de la part d'organisations particulières à moins d'avoir des dossiers clairs de ces consentements.

Pour plus d'informations sur cette affaire :

[http://tpsservices.co.uk/images/news/07-02-2017/The\\_Data\\_Supply\\_Company\\_Ltd\\_Monetary\\_Penalty\\_Notice.pdf](http://tpsservices.co.uk/images/news/07-02-2017/The_Data_Supply_Company_Ltd_Monetary_Penalty_Notice.pdf)

70. Il est dès lors recommandé de poser les questions suivantes aux organisations auprès desquelles vous obtenez des données :

- ✓ Les données ont-elles été collectées directement ou indirectement auprès des personnes concernées ?
- ✓ Par qui et dans quel contexte ?
- ✓ Sur quelle base juridique ont-elles été traitées ?
- ✓ Si le consentement a été recueilli, demandez la preuve, demandez quand et comment le consentement a été recueilli ;
- ✓ Les personnes concernées ont-elles été informées ? Sur quoi (vérifiez que la transmission de leurs données à votre organisation ou des organisations de votre catégorie en vue des utilisations que vous envisagez a bien été prévue et de façon claire), comment et par qui ?



71. Renseignez-vous également pour savoir si l'organisation aux services de laquelle vous souhaitez recourir fait ou non partie d'un organisme professionnel, est ou non adhérent d'une charte ou accrédité par un organisme indépendant.
72. Toutes ces précautions préalables font partie des efforts de mise en conformité (« due diligence ») attendus d'un responsable de traitement **et** du respect de l'article 25 du RGPD qui vous impose d'intégrer la **protection des données à caractère dès la conception de vos traitements et par défaut**, tout au long de votre traitement.

#### 4. Filiales – Fusions, scissions et acquisitions

73. Notez également que les personnes concernées doivent être informées de la possibilité que leurs données soient communiquées à des tiers en ce compris aux filiales d'une organisation ou, à une entité tierce en cas de fusion, scission ou acquisition impliquant le responsable du traitement (quel que soit la forme de cette opération).
74. Lorsqu'une concentration d'entreprise (ou toute autre forme d'opération ayant un impact sur l'identité du responsable du traitement ou sur l'accès aux données dont il est responsable) vient à se produire, il appartient à l'organisation tierce qui accède ainsi aux données d'informer les personnes concernées, de son identité, de ses finalités, de ses traitements, des données traitées, de leur durée de conservation, des éventuels (nouveaux) destinataires de ces données et des droits dont disposent les personnes concernées, comme celui de s'opposer au traitement de leurs données.

## B. Déterminez vos finalités de traitement

### Article 5.1, b) du RGPD :

« Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites, et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; (...) »

#### 1. Finalité(s) initiale(s)

75. L'une des obligations primordiales d'un responsable de traitement est de déterminer la ou les finalités qu'il poursuit et qui requière(nt) que des données à caractère personnel soient traitées. En d'autres termes, les objectifs qu'il entend atteindre au moyen de l'utilisation de ces données personnelles.



76. La détermination correcte de vos finalités de traitement est essentielle à l'examen de proportionnalité des données et donc de vos traitements de données (exercice obligatoire qui vise à garantir que les données traitées et leurs traitements sont proportionnés par rapport aux finalités poursuivies) . Vous devez d'abord bien cerner et prévoir vos finalités de traitement pour pouvoir ensuite définir les traitements qui seront nécessaires à la réalisation de celles-ci.

77. Voici quelques exemples de finalités de marketing direct :

- ✓ informer vos clients quant à vos nouveaux produits ou services;
- ✓ établir le profil de vos clients ;
- ✓ permettre à des tiers d'utiliser les données de vos clients pour établir des profils d'électeurs ;
- ✓ proposer des offres personnalisées pour l'anniversaire de vos clients ;
- ✓ tenir informé vos clients de vos différentes actions
- ✓ faire la promotion de votre image de marque envers le grand public;
- ✓ inviter vos clients ou prospects à des événements (pour la promotion de votre organisation) ;
- ✓ communiquer à vos clients des offres ciblées susceptibles de rencontrer leurs intérêts ;
- ✓ démarcher de nouveaux clients, abonnés ou affiliés.

78. Il vous appartient ensuite de les indiquer de la façon la plus précise possible dans votre registre d'activités de traitements (Voir les considérants 88, 89 et 90 de cette recommandation) ainsi que dans le document que vous utiliserez pour fournir l'information requise aux personnes concernées (dès lors que la précision de vos finalités de traitement est également essentielle afin de pouvoir assurer le respect de l'obligation de transparence prévue aux articles 13 et 14 du RGPD qui prévoient expressément que les personnes concernées doivent être informées des finalités de traitement).



Dans la plupart des cas, prévoir que « *nous traitons vos données pour des finalités de marketing direct* » ne suffit pas à fournir une information précise au sens du RGPD. Le niveau de détail attendu dépend notamment du type de communications de marketing (sms, mail, téléphone, courrier etc), de leur fréquence (mensuelles, semestrielles, etc), de leur contenu (informations sur la marque, un produit, un service, newsletter, des bons de réductions) ou encore de la complexité des traitements en question (notamment sur la base d'un profilage et de la précision de celui-ci par exemple).

La transparence quant à vos finalités de traitement implique également d'être loyal. Prévoir que « *nous traitons vos données afin d'améliorer nos services* » alors que le but poursuivi par vos communications de marketing est de promouvoir vos services et d'encourager vos clients à y recourir, n'est propre à éclairer la personne concernée sur le fait que vous entendez traiter ses données pour des finalités de marketing direct.



## 2. Finalité(s) ultérieure(s)

79. A cet égard, soyez également vigilants à informer clairement sur vos finalités ultérieures de traitement qui devront également faire l'objet de l'information à fournir aux personnes concernées.

### Article 13.3 du RGPD

« Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2. »

80. En outre, si le traitement ultérieur ne repose ni sur le consentement de la personne concernée, ni sur une norme<sup>20</sup>, vous devez effectuer un **test de compatibilité** entre la finalité initiale et la finalité ultérieure conformément, entre autres, à ce que prévoit l'article 6.4 du RGPD et que résume le considérant 50 :

### Considérant 50 du RGPD :

« Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données à caractère personnel ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les exigences liées à la licéité du traitement initial, devrait tenir compte, entre autres: de tout lien entre ces finalités et les finalités du traitement ultérieur prévu; du contexte dans lequel les données à caractère personnel ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données; la nature des données à caractère personnel; les conséquences pour les personnes concernées du traitement ultérieur prévu; et l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu. »

81. L'examen de compatibilité doit être réalisé par le responsable initial du traitement tant en ce qui concerne ses traitements qu'en ce qui concerne les traitements envisagés par les tiers responsables de traitements auxquels il entend communiquer les données.



Il en va ainsi pour toutes les données que vous seriez amenés à utiliser dans le cadre de finalités ultérieures, même si ces données peuvent être considérées comme « publiques » (par exemple les données à caractère personnel publiées par les personnes concernées elles-mêmes sur leurs comptes de médias sociaux). La question n'est pas de savoir si les données sont disponibles publiquement mais de savoir si la finalité pour laquelle elles ont été traitées au départ est ou non compatible avec la ou les finalités ultérieure(s).

<sup>20</sup> L'article 13 RGPD précise plus exactement que : « (...)ni sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1. (...)»



82. Lorsqu'un même responsable de traitement entend réutiliser, à des fins de marketing direct, des données à caractère personnel qu'il a lui-même collecté initialement à d'autres fins que celles de marketing direct, l'obligation du test de compatibilité lui incombe. Si le consentement préalable (répondant aux conditions de validité imposées par le RGPD) des personnes concernées a été récolté quant à l'usage de leurs données par l'organisation souhaitant ré-utiliser ces données, le test de compatibilité n'est pas nécessaire. Par contre, si aucun consentement n'a été récolté, le test de compatibilité doit être effectué entre la finalité pour laquelle les données ont été collectées et la finalité de marketing direct. Cette ré-utilisation pourrait être illégitime en cas d'incompatibilité avec la finalité initiale en raison, notamment, de l'absence de relation entre les personnes concernées et cette organisation et en l'impossibilité qui en découle de conclure qu'un tel usage entrerait dans les attentes raisonnables de ces personnes.

### Exemple 15

La société « Tout à neuf » est spécialisée dans les travaux de bâtiment. Elle cherche à se faire connaître auprès de nouveaux clients. Elle fait appel au service de la société « In the pocket » qui dispose d'une base données alimentée régulièrement avec les nom et coordonnées de personnes physiques ayant récemment acheté un terrain dans la Région et qui auront sûrement besoin de main d'œuvre pour faire construire leurs habitations. « In the pocket » indique à « Tout à neuf » qu'elle obtient directement ces données auprès des administrations communales dans le cadre de leur gestion des demandes de permis de bâtir. Le patron de Tout à neuf interroge In the pocket quant à la légalité d'une réutilisation de ces données par son entreprise.

Cette dernière la rassure : les administrations communales ne feraient sûrement rien d'illégal et elle croit savoir que les personnes concernées ont bien été informées par les administrations communales du fait que leurs coordonnées seraient transmises à des entreprises commerciales à des fins de marketing direct. In the pocket n'informe pas elle-même les personnes concernées à ce sujet.

Tout à neuf est conquise, elle accède à la base de données de In the pocket et adresse un courrier pour proposer ses services aux personnes ayant acheté un terrain dans son périmètre d'activité. Dans son courrier elle explique aux personnes via qui et de quelle manière elle a pris connaissance de leurs données à caractère personnel, elle précise quelles données ont été collectées, les finalités pour lesquelles elle les traite et les traitements effectués. Elle indique aux personnes contactées qu'elles peuvent à tout moment s'opposer au traitement de leurs données et indique qu'en cas d'absence de réponse dans un délais de 6 mois, les données seront de toutes façon supprimées de leur base de données.

La finalité d'un tel traitement ultérieur (et donc ledit traitement) pose problème à plusieurs niveaux :

1° Les données à caractère personnel ont initialement été collectées par les administrations communales pour se conformer à une obligation légale. En communiquant leurs données à caractère personnel, les personnes concernées n'ont pas donné leur consentement à ce que celles-ci soient communiquées à un tiers à des fins d'utilisation pour des finalités commerciales. Elles ne pouvaient pas non plus raisonnablement s'attendre à un traitement ultérieur dans le cadre de cette finalité.

- ✓ Les administrations communales sont donc en infraction à leurs obligations issues des articles 5.1,b), 6.4 et 13 RGPD.



### Exemple 15 (suite)

- ✓ Le consentement préalable, libre, éclairé, univoque et spécifique des personnes concernées aurait dû être demandé au stade de la collecte initiale des données.

2° Au moment de sa collecte de données auprès des administrations communales, In the Pocket n'a pas communiqué aux personnes concernées qu'elle avait récupéré leurs données auprès des administrations communales ni de quelle manière elle allait les traiter. Les personnes concernées qui n'avaient pas été informées au départ, n'ont à nouveau pas pu consentir à de tels traitements ultérieurs lesquels ne sont pas plus compatibles avec le traitement initial.

- ✓ In the Pocket est en infraction à ses obligations issues des articles 5.1,b), 6.4 et 14 RGPD.

3° Tout à neuf quant à elle respecté ses obligations issues de l'article 14 du RGPD mais cela ne suffit pas. Les données ayant été traitées ultérieurement sans consentement des personnes concernées et pour des usages dont les finalités sont incompatibles, il y a également violation des articles 5.1, b) et 6.4 dans son chef.

83. Tant le devoir d'informer les personnes concernées que celui de vous informer vous-même lorsque vous collectez des données de manière indirecte, en tant que responsable du traitement, est important. Si vous ne disposez pas des bonnes informations quant à la licéité du traitement initial, vous ne serez ni en mesure de correctement informer les personnes concernées, ni d'effectuer le test de compatibilité vous permettant d'utiliser les données dans le cadre de vos propres finalités de traitement ultérieur. Vous risquez donc de voir vos traitements entachés d'illicéité et dès lors, d'être sujets à sanction.

84. Enfin, vous ne pouvez traiter des données à caractère personnel que pour des finalités réelles et existantes ou, si potentielles, réalistes dans un futur proche au regard de votre activité actuelle. Vous ne pouvez ainsi par exemple pas préciser que vous collectez la donnée « date de naissance » « pour envoyer un cadeau d'anniversaire » si vous n'envoyez en réalité pas de tel cadeau, ni même « au cas où nous voudrions vous envoyer un cadeau d'anniversaire » si cela n'est pas réaliste.

## C. Définissez vos opérations de traitement

### 1. Notion

#### Article 4.2 du RGPD : définition du traitement de données à caractère personnel

« toute opération ou ensemble d'opérations de traitement effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. »

85. Vos traitements de données commencent dès la collecte de ces données et se poursuivent jusqu'à la suppression de ces données, après leur enregistrement dans une base données ou encore leur



communication à des tiers. Vous traitez également des données (nom, prénom, adresse postale ou email par exemple) lorsque vous adressez vos communications de marketing direct aux personnes concernées.

86. Il ne faut pas confondre les finalités d'un traitement de données et le traitement lui-même. Dans les exemples repris au considérant 77 de la Recommandation, les traitements seraient par exemple :

- ✓ **établir un profil concernant des personnes déterminées, en croisant différentes données les concernant, obtenues au moyen des informations communiquées directement par ces personnes à votre organisation et à vos partenaires commerciaux,** afin de les informer sur vos nouveaux produits;
- ✓ faire la promotion de vos futurs services, **en utilisant le numéro de téléphone de prospects pour leur envoyer des SMS ;**
- ✓ **utiliser le service de messagerie d'un réseau social pour envoyer des messages** afin de proposer des offres personnalisées pour l'anniversaire de vos clients ;
- ✓ **utiliser l'adresse e-mail de vos clients** pour les tenir informés de vos différentes actions, leur envoyer votre newsletter ;
- ✓ inviter à des événements pour la promotion de votre organisation, **en contactant vos clients par courrier postal ;**
- ✓ démarcher de nouveaux clients, abonnés ou affiliés, **en faisant du porte à porte (cfr l'explication du considérant 35 à ce sujet).**

87. Vous devez, comme pour vos finalités de traitements, être transparents vis-à-vis des personnes concernées quant aux vos traitements que vous effectuez de vos données. Donc en pratique leur fournir une information détaillée quant à ces traitements, avant d'entamer ces traitements. Le niveau de détail attendu dépend, entre autres, du type de personnes concernées (enfants, professionnels, experts, etc), de la manière dont sont traitées leurs données à caractère personnel et du degré d'intrusion dans leur droit à la vie privée qu'impliquent ces traitements.

88. Notez que la précision des opérations de traitement que vous réalisez pour chaque finalité permet d'évaluer la proportionnalité (et donc l'admissibilité) de ces traitements par rapports à vos finalités (objectifs). Il serait par exemple difficile de justifier un traitement de données par profilage pour envoyer une newsletter identique à l'ensemble de vos clients.

89. En outre, notez qu'un même traitement de données peut parfois être réalisé pour atteindre plusieurs finalités et que, dans ce cas, des informations précises à ce sujet doivent être fournies.







Imaginons que vous traitez les données noms et adresses de vos clients pour leur envoyer tous les mois vos offres promotionnelles sur la base de leur consentement préalable. S'ils retirent leur consentement à ce que vous traitiez leurs données pour cette finalité, cela ne veut pas dire que vous deviez effacer purement et simplement leurs données de vos systèmes POUR AUTANT que vous disposiez d'une base juridique valable pour la poursuite d'une autre finalité, par exemple, l'envoi de factures mensuelles.

Vous ne pourrez toutefois plus traiter ces mêmes données pour la finalité d'envoi d'offres promotionnelles. Cela signifie que vous devrez notamment cesser toute opération de traitement de ces données qui sert uniquement liée à cette finalité.

90. N'oubliez pas non plus de tenir à jour votre registre des activités de traitement.

#### Article 30 RGPD

« Chaque responsable de traitement et, le cas échéant, le représentant du responsable du traitement, tiennent un registre des activités de traitement effectuées sous leur responsabilité. (...) »

Cette obligation s'applique aux organisations de plus de 250 personnes et aux organisations dont le(s) traitement(s) :

- ✓ Est/sont susceptible(s) de comporter un risque pour les droits et libertés des personnes concernées ;
- ✓ N'est/ne sont pas occasionnel(s) ;
- ✓ **Ou** s'il(s) porte(nt) notamment sur les catégories particulières de données visées à l'article 9.1 RGPD ou sur les données relevant de l'article 10 RGPD.

91. Ce registre doit permettre d'identifier et de disposer d'une vue d'ensemble de vos traitements de données à caractère personnel mais également d'autres informations comme les données ou catégories de données à caractère personnel que vous traitez. Ce registre doit être fait par écrit (électronique) et doit être clair et compréhensible .

92. Le registre vous aide donc également à recenser de manière minutieuse les données que vous traitez et vous sert dès lors d'outil indispensable à la connaissance de votre écosystème de traitement des données dont vous êtes responsable. Un registre correctement tenu est donc un gain de temps pour vous aider à respecter vos obligations du RGPD et permet à l'ensemble des personnes travaillant au sein de votre organisation et impliquées dans le traitement des données utiles à votre organisation d'être consultées si vous en avez besoin et/ou informées des traitements de l'organisation, ce qui permet également d'augmenter la prise de conscience relative à la protection des données à tous les niveaux. Cela vous aidera également à établir, en cas de besoin, une analyse d'impact relative à la protection des données ainsi que de collaborer avec l'APD en cas de demandes de sa part quant à certains de vos traitements.



## 2. Profilage

93. Au même titre que d'autres traitements auxquels il est régulièrement recouru dans le cadre des finalités de marketing direct, le profilage est un traitement de données au sujet duquel vous devez clairement informer les personnes concernées . Le profilage n'est pas une finalité mais bien un traitement effectué dans le but d'atteindre certaines finalités telle que, par exemple, la vente de données ou apprendre à mieux cibler votre clientèle.

### Exemple 16

En commandant sur l'e-shop de la boutique « Chic et Chok», les clients peuvent lire que leurs données à caractère personnel sont nécessaires afin de « *permettre à Chic et Chock d'établir un profil d'acheteur pour mieux connaître ses clients* ».

- ✓ Chic et Chock entend profiler ses clients. Présenté de la sorte, elle laisse entendre erronément que le profilage serait une finalité de traitement alors que le profilage est un traitement et non pas une finalité en soi.

94. L'article 4.4 du RGPD définit le profilage comme « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* ».

95. Le profilage fait l'objet d'une attention particulière dans la mesure où son processus est souvent invisible pour les personnes concernées. Il donne lieu à la création de nouvelles données à caractère personnel déduites ou dérivées de données fournies au préalable directement par ces personnes, de données transactionnelles<sup>21</sup> ou d'informations et traces laissées par celles-ci au cours de leur navigation sur des pages de site Internet.

96. En outre, le profilage peut entraîner des conséquences négatives pour les personnes concernées car il peut être déloyal en limitant ou ciblant par exemple le type d'information communiqué à certaines catégories de personnes concernées (comme le ciblage politique sur un média social) et/ou donner lieu à de la discrimination, par exemple s'il donne lieu à un refus d'accès à un service ou en à un ciblage avec des produits plus coûteux voire risqués financièrement.

97. C'est en raison des particularités de ce traitement que le profilage est abordé de manière spécifique par le RGPD, qui l'examine dans ses **trois facettes**. Il peut en effet s'agir d'un profilage général, d'une prise de décision fondée sur le profilage avec l'intervention d'une personne physique ou d'un profilage pouvant

<sup>21</sup> Lignes directrices WP251 rev.01, endossée par l'EDPB relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, version révisée le 6 février 2018, p.10.



aboutir à une prise de décision exclusivement automatisée, sans intervention humaine. Les deux premières facettes sont soumises à l'entière respect du RGPD en tant que traitement de données à caractère personnel. La troisième facette, quant à elle, connaît, outre les règles du RGPD, applicables de façon générale, des règles plus strictes issues de l'article 22 du RGPD.

98. Le RGPD est en effet particulièrement strict lorsque le profilage facilite la **prise de décision automatisée** à l'égard d'une personne concernée sans intervention d'une personne physique. L'article 22 du RGPD prévoit en effet que toute personne concernée a le droit de s'opposer au fait de *faire l'objet d'une décision exclusivement fondée sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.*



Si vous entendez produire une décision exclusivement fondée sur la base d'un traitement automatisé, veillez à recueillir un **consentement explicite** de la personne concernée. Vous êtes également tenus de permettre à la personne d'exprimer son point de vue et, le cas échéant, contester la décision ainsi prise. Soyez également attentifs au fait que vous devez également recueillir un consentement explicite de la personne concernée si vous entendez prendre une décision automatisée sur la base de données visées à l'article 9 du RGPD (à moins que le traitement ne soit nécessaire pour des motifs d'intérêt public important). Vous devez enfin mettre en place les mesures appropriées pour garantir la sauvegarde des libertés et droits fondamentaux ainsi que des intérêts des personnes concernées.

Notez que le consentement explicite requiert, outre les conditions de validité de l'article 7 du RGPD, un écrit clair et précis de la personne concernée qui donne son consentement.

99. Le marketing direct peut, dans certaines situations, impliquer des décisions exclusivement fondées sur un traitement automatisé « produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ». L'EDPB indique que cela peut être le cas, selon les caractéristiques particulières de la situation, y compris en ce qui concerne :

- ✓ Le caractère intrusif du processus de profilage, y compris le suivi des personnes sur différents sites web, appareils et services ;
- ✓ Les attentes et les souhaits des personnes concernées ;
- ✓ La façon dont l'annonce est diffusée ; ou
- ✓ Le recours aux vulnérabilités connues des personnes concernées visées<sup>22</sup>.

100. L'EDPB rappelle également qu' « *un traitement qui pourrait avoir peu d'incidences sur les personnes en général peut en effet avoir un effet significatif à l'égard de certains groupes de la société, tels que les groupes minoritaires ou les adultes vulnérables* » et que « *des prix différentiels fondés sur des données à caractère personnel ou des caractéristiques personnelles pourraient également avoir un effet significatif si*

<sup>22</sup> Pour une information complète relative au profilage, veuillez consulter la version révisée de 2018 des Lignes directrices EDPB WP251 rev.01 relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, disponible via le lien suivant : [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612053](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053)



*par exemple, des prix prohibitifs empêchent effectivement une personne d'accéder à certains biens ou services.»<sup>23</sup>*

### Exemple 17

La société « Omniscient ou presque » revend à la société « Toutassurix », une compagnie d'assurance, des profils de personnes sans le consentement de celles-ci ou sans connaître les données sous-jacentes. Les profils classent les consommateurs en catégories avec des qualificatifs tels que « profil ethnique de deuxième génération : part souvent en voyage », « jeune ménage : motorisé », « famille nombreuse : difficile de joindre les deux bouts », ou une note qui met l'accent sur la situation familiale et/ou la vulnérabilité financière des personnes concernées.

Toutassurix dispose de différents produits d'assurance mais souhaite effectuer un tri préalable et réserver certains produits et/ou conditions à certaines catégories de clients. Elle adresse donc des informations sur ses produits d'assurance, par mails à ses clients existants, à des conditions différentes, sur la base de ces profils établis par Omniscient ou presque. Les différences existant entre les différents produits et conditions de Toutassurix sont significatives et peuvent impliquer des conséquences financières importantes allant jusqu'à l'impossibilité d'y recourir au risque de s'endetter alors que d'autres solutions existent.

L'ensemble des décisions « prises » par Toutassurix concernant le contenu de la communication aux personnes concernées sont exclusivement fondées sur la base d'un traitement automatisé, aucun de ses collaborateurs n'ayant revu et/ou adapté ni les profils, ni les dossiers des clients avant d'envoyer les courriels.

- ✓ Toutassurix doit demander le consentement explicite préalable de ses clients pour un tel traitement de données ;
- ✓ Les clients de Toutassurix doivent pouvoir comprendre pourquoi de tels produits leurs sont proposés et demander à ce qu'on réévalue les propositions en tenant compte d'autres éléments, voire de corriger ceux sur la base desquels les profils ont été façonnés. Ils doivent également pouvoir refuser de telles décisions.

#### 101. **Profilage et décision purement automatisée ne sont pour autant pas nécessairement liés.**

Une décision automatisée peut en effet être prise sans profilage et un profilage peut être réalisé sans aboutir à une décision automatisée. De manière générale, le traitement de données par profilage requiert de votre part une attention particulière eu égard au nombre et aux types de données utilisées, au processus lui-même ou encore aux sources desquelles proviennent les données. Dès lors, même si le profilage que vous appliquez aux données à caractère personnel n'aboutit pas ou n'a pas pour but d'aboutir à la prise d'une décision automatisée, ledit traitement de données par profilage est intégralement soumis aux règles du RGPD. Vous devez être notamment attentifs à préciser aux personnes concernées de quelle manière elles vont être profilées et pourquoi (article 13 et 14 RGPD).

102. Enfin, rappelez-vous que si vous n'êtes pas en mesure de vous assurer de la provenance des profils que vous récupérez ni de l'information qui a été fournie à ce sujet aux personnes concernées, mieux vaut ne pas traiter ces données à caractère personnel afin d'éviter tout risque.

<sup>23</sup> Lignes directrices WP251rev.01, pp.24-25.



## D. Identifier les données nécessaires à la poursuite de vos finalités

### 1. Notion de « donnée à caractère personnel »<sup>24</sup>

#### Article 4.1, RGPD

« Toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une personne physique « identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de géolocalisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »

103. Les termes « identifiés » et « identifiables » sont au cœur de la compréhension de ce qu'est une donnée à caractère personnel. Si les données permettant directement d'identifier une personne sont souvent évidentes (par exemple la combinaison des nom, prénoms et de l'adresse ou de la date de naissance ou encore un numéro d'identification unique, comme un numéro de client), il est parfois plus difficile de savoir ce qu'il y a lieu de comprendre comme « données permettant d'identifier indirectement une personne » (par exemple une donnée pseudonymisée).
104. Toute information qui est liée à une personne, aussi minime puisse-t-elle vous paraître lorsque vous la considérez isolément (par exemple un âge, une commune de résidence, la couleur des yeux ou le genre, voire un numéro de matricule), est une donnée à caractère personnel dès lors que combinée avec une ou plusieurs autres, elle permet d'identifier, d'individualiser une personne physique. C'est ainsi que le RGPD est applicable aux données à caractère personnel ayant fait l'objet d'une pseudonymisation. Une donnée pseudonymisée ne peut en principe plus être attribuée à une personne concernée précise sans avoir recours à des informations supplémentaires et pour autant que ces informations soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données ne soient pas attribuées à une personne identifiée ou identifiable. Les données pseudonymisées sont dès lors couvertes par la définition de données à caractère personnel et donc, par le RGPD, dans la mesure où elles peuvent permettre d'identifier une personne.
105. A contrario, les données dites « anonymisées » ne sont pas considérées comme des données à caractère personnel en ce qu'elles ne devraient pas permettre d'identifier une personne, même en utilisant des informations complémentaires. Si le RGPD exclut encore à ce jour de son champ d'application les données dites « anonymes » pour cette raison, la frontière les séparant tend à s'amenuiser considérablement.

---

<sup>24</sup> Pour plus d'informations à ce sujet, veuillez consulter l'opinion WP136 relative au concept de données à caractère personnel adoptée le 20 juin 2007 par le Groupe 29, disponible via le lien suivant : [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136\\_fr.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_fr.pdf)



Une recherche menée par une équipe de chercheurs de l'Université catholique de Louvain et de l'Imperial College de Londres, démontre qu'il est possible d'identifier des personnes physiques sur la base de 4 données « anonymisées » issues de leurs transactions bancaires, avec un taux de certitude de 90%, en leur appliquant un certain algorithme.

Sur la base de probabilités et de corrélations statistiques appliquées à des métadonnées issues de transactions bancaires, il est ainsi possible, avec une quasi-certitude, d'identifier une personne qui s'est rendue dans un magasin de bricolage, puis dans sa salle de sport, avant de se rendre dans un restaurant, et qui termine sa journée en allant au cinéma.

Pour davantage d'information au sujet de cette étude :

- ✓ <https://www.nature.com/articles/s41467-019-10933-3>
- ✓ <https://uclouvain.be/en/discover/press/news/anonymising-personal-data-not-enough-to-protect-privacy-shows-new-study.html>
- ✓ <https://www.imperial.ac.uk/news/192112/anonymising-personal-data-enough-protect-privacy/>

106. Ce qui est vrai pour des données considérées comme « anonymes » l'est *a fortiori* pour des données à caractère personnel. Les mises en corrélations de certaines données à caractère personnel (comme par exemple l'âge, la commune de résidence, le sexe et la couleur des yeux) permettent une identification des personnes qui sont en relation avec vous en tant que clients, prospects, abonnés ou électeur par exemple.
107. Enfin, rappelons que seules les données des personnes physiques vivantes sont des données à caractère personnel.

## 2. Principe de minimisation des données

### Article 5.1, c) RGPD

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

108. L'une des premières tâches à accomplir en tant que responsable de traitement est de passer en revue les données et/ou catégories de données à caractère personnel dont vous disposez. Le respect du principe de minimisation est fondamental pour que vos activités de traitement soient conformes au RGPD.
109. Cet exercice doit être intégré dans votre activité en permanence et fait, par cela, partie de ce que l'on appelle la « privacy by design », principe fondateur du nouveau cadre de règles et essentiel au principe, lui aussi transversal, d'« accountability ».



110. Il implique que vous procédiez à un examen des données que vous entendez collecter ou dont vous disposez déjà en tenant compte de de l'adéquation, de la pertinence et de la limitation à ce qui est nécessaire aux finalités que vous poursuivez et des traitements que vous entendez effectuer de ces données. Il n'est possible d'effectuer cet examen qu'après avoir déterminé au préalable toutes les données que vous traitez et les finalités que vous souhaitez poursuivre de par l'utilisation de ces données.

111. Les possibilités commerciales engendrées par la collecte massive de données mais également par leur profilage ou encore par les coûts moins élevés de stockage peuvent vous encourager, à tort, à collecter plus de données à caractère personnel que vous n'en avez réellement besoin, au cas où cela s'avèrerait utile pour l'avenir<sup>25</sup>.



Il ne s'agit pas de collecter, générer ou conserver un maximum de données parce que cela est « possible » techniquement. Il s'agit de collecter, générer ou conserver uniquement les données dont vous avez réellement besoin pour mener à bien vos finalités existantes ou futures, pour autant que celles-ci soient réalistes à court terme.

112. Ce principe de minimisation imposé par le RGPD peut également être un outil de perfectionnement de vos propres besoins de marketing direct. En ayant recours aux données pertinentes, vous améliorez la qualité de votre activité. Vous améliorez aussi la qualité de vos interactions avec vos clients, abonnés ou autre, et donc votre image.

113. Le principe de minimisation exige, notamment, de garantir que la durée de conservation des données soient limitée au strict minimum.

#### Article 5.1, e) du RGPD

Cet article précise le principe de limitation de conservation des données en stipulant que les données peuvent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

114. Enfin, connaître vos données c'est aussi identifier celles relevant de catégories particulières encadrées par l'article 9 du RGPD ou par l'article 10 du RGPD ou encore attachées à des personnes vulnérables comme les données relatives à des personnes mineurs ou ne disposant pas de la capacité nécessaire pour exercer certaines actions.

---

<sup>25</sup> Lignes directrices EDPB relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, version révisée le 6 février 2018, p.12.



### L'Article 9.1 RGPD pose l'interdiction de principe du traitement des données relevant des catégories suivantes

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

En matière de marketing direct, seul le **consentement explicite** permet le traitement de telles données, comme le prévoit l'article 9.2 du RGPD.

115. Si vous disposez du consentement des personnes concernées pour traiter certaines catégories particulières de données, cela n'est pas sans conséquence sur l'organisation de votre activité. Vous devrez en effet probablement désigner un délégué à la protection des données<sup>26</sup> et réaliser une analyse d'impact relative à la protection des données<sup>27</sup>.

116. Attention, si de prime abord certaines données peuvent vous sembler être de « simples » données à caractère personnel ne relevant pas directement de la catégorie des données de l'article 9 du RGPD, comme les données relatives aux habitudes de vie, les données relatives à des prestations sportives ou à des préférences alimentaires, celles-ci peuvent souvent se révéler être des données sensibles au regard de leur potentiel à révéler de nombreuses informations au sujet de la personne concernée. Des habitudes alimentaires peuvent en effet révéler des soucis de santé ou des orientations philosophiques ou religieuses. Des données sportives peuvent également devenir sensibles si elles sont traitées en tant que données relatives à la santé. Mieux vaut, en cas de doute, être vigilant et considérer ce type de données comme relevant de l'article 9 du RGPD.

117. L'une des manières d'éviter de traiter des données sensibles dont vous n'auriez ni besoin ni l'autorisation est, outre d'éviter de les demander explicitement, de limiter les possibilités de saisines de textes dans les champs libres et de procéder à une veille de vos espaces de stockage tels que vos bases de données afin d'encadrer au mieux ces données sensibles, et de les supprimer rapidement le cas échéant.

### 3. Maîtrisez votre gestion des données

118. L'article 25 du RGPD pose les principes fondamentaux de la protection des données « dès la conception » (privacy by design) et « par défaut » (privacy by default).

<sup>26</sup> Pour davantage d'informations à ce sujet, veuillez consulter notre dossier thématique « DPO » <https://www.autoriteprotectiondonnees.be/dossier-thematique-delegue-a-la-protection-des-donnees>

<sup>27</sup> Pour davantage d'informations à ce sujet, veuillez consulter notre dossier thématique « AIPD » <https://www.autoriteprotectiondonnees.be/analyse-dimpact-relative-a-la-protection-des-donnees>





119. Compte tenu des technologies et possibilité existantes, des moyens financiers et humains dont vous disposez, vous devez assurer la protection des données dès la conception de vos traitements et de vos moyens de traitement, par des mesures techniques (par exemple la pseudonymisation des données à caractère personnel) et organisationnelles appropriées pour permettre d'endiguer les éventuels risques que peuvent présenter vos traitements au regard de leurs caractéristiques propres (en tenant compte du nombre et du type de données à caractère personnel, de vos traitements eux-mêmes, de la durée de conservation, des personnes pouvant accéder aux données etc).
120. La protection dès la conception implique que vous intégrez, avant même le lancement de vos traitements, les principes de protection des données (que l'on retrouve à l'article 5 du RGPD), ainsi que les libertés et droits fondamentaux des personnes concernées, dont les droits dont elles disposent conformément aux articles 12 à 22 du RGPD.
121. Il est important à cet égard que vous ayez une vue claire sur vos différents outils et modalités de stockage de données, comme par exemple vos bases de données, afin de gérer consciencieusement les données à caractère personnel dont vous disposez. Celles-ci se retrouvent souvent copiées de manière éparse au sein de différents systèmes, au sein de votre organisation ou auprès de vos sous-traitants. Si les back-up sont à encourager, afin d'éviter les pertes de données, la multiplication de copies de ces données dans différents systèmes, bases de données et applications multiplie les risques inutiles et vous empêche de disposer d'une vue d'ensemble de ces données et donc des personnes auxquelles elles se rattachent.

#### Article 25.2 du RGPD (Privacy by default)

« Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique de traitement sont traitées. Cela s'applique à la **quantité de données** à caractère personnel collectées, à **l'étendue de leur traitement**, à leur **durée de conservation** et à leur **accessibilité**. En particulier ces mesures garantissent que, par défaut, les données ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée. »

122. Vous devez faire en sorte de ne pas collecter plus de données que nécessaire et garantir la **qualité des données** dont vous disposez. Grâce à des données **exactes et mises à jour**, vous pouvez ainsi mieux maîtriser les opérations de traitement que vous appliquez à ces données et les rendre plus efficaces mais également conformes au RGPD.

#### Article 5.1, d) du RGPD

Les données à caractère personnel doivent être « exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder. »



123. A cet égard, notez que l'article 5ter de la loi du 8 août 1983 *organisant un registre national des personnes physiques* permet, dans certaines conditions strictes, aux personnes majeures qui entretiennent avec des organismes une relation contractuelle dont l'exécution nécessite des prestations successives, d'autoriser ces organismes à recevoir communication par les services du registre national des modifications apportées à certaines de leurs données<sup>28</sup>. Veuillez examiner attentivement cette disposition et ses conditions d'application afin d'en faire usage le cas échéant.

124. Vous êtes notamment tenus par la **limitation de la conservation des données**, celles-ci ne pouvant être traitées pour une durée excédant celle nécessaire au regard des finalités. En gérant correctement vos bases de données vous pourrez ainsi rapidement identifier les données devenues obsolètes ou ne pouvant plus être traitées, par exemple lorsqu'une personne s'y est opposée ou a retiré son consentement.

LE SAVIEZ-VOUS



L'Agence danoise de protection des données a sanctionné la société IDdesign au paiement d'une amende de 1,5 million de couronnes danoises (plus de 200.000 euros) pour n'avoir pas effacé des données concernant environ 385 000 clients.

L'une des questions abordées lors de la visite de l'Autorité en leurs locaux était de savoir si l'entreprise avait fixé des délais pour l'effacement des données des clients et si ces délais avaient été respectés. Au cours de l'inspection, il s'est avéré que certains magasins de meubles de la société utilisaient un système plus ancien, qui avait été remplacé par un système plus récent dans les autres magasins. Dans l'ancien système, des informations sur les noms, adresses, numéros de téléphone, adresses e-mail et l'historique des achats de quelque 385.000 clients étaient collectées. Au cours de l'inspection, IDdesign a également déclaré que les données à caractère personnel de l'ancien système n'avaient jamais été supprimées.

IDdesign n'indiquait pas à quel moment les données à caractère personnel contenues dans l'ancien système n'étaient plus nécessaires aux fins du traitement et ne précisait donc pas les délais applicables à l'effacement des données à caractère personnel traitées dans le système.

L'Agence de protection des données considère donc que IDdesign n'a pas respecté les exigences en matière de protection des données du RGPD en ayant traité les données à caractère personnel pendant une période plus longue que nécessaire.

Si vous souhaitez en savoir davantage : [https://edpb.europa.eu/news/national-news/2019/danish-dpa-set-fine-furniture-company\\_en](https://edpb.europa.eu/news/national-news/2019/danish-dpa-set-fine-furniture-company_en)

<sup>28</sup> Loi du 8 août 1983 :

[https://www.ejustice.just.fgov.be/cqi\\_loi/change\\_lq.pl?language=fr&la=F&cn=1983080836&table\\_name=loi](https://www.ejustice.just.fgov.be/cqi_loi/change_lq.pl?language=fr&la=F&cn=1983080836&table_name=loi)



125. Maîtriser vos espaces de stockage c'est aussi vous permettre de **séparer les données « sensibles » des autres** afin de prévoir des **mesures de sécurité adéquates**. Cela vous permet également de vérifier et de déterminer spécifiquement pour des données sensibles, la **base juridique issue de l'article 9.2 du RGPD** sur laquelle vous vous basez pour les traiter.

126. Cela vous permet également de dissocier, au besoin, les bases de données clients/affiliés/abonnés et autres des « prospects », mais aussi de **gérer efficacement l'exercice des droits** des personnes concernées, comme par exemple le retrait du consentement ou le droit d'opposition au traitement de leurs données pour vos finalités de marketing direct (voir infra aux considérants 127, 131, 161 à 166, 215 et 238).

LE SAVIEZ-VOUS

?

L'Autorité de protection des données hellénique a imposé une amende à un opérateur télécom pour non-respect du droit d'opposition et du principe de la protection des données par la conception (privacy by design) en matière de conservation des données personnelles de ses abonnés.

Il est en effet apparu après investigations menées suite à de nombreuses plaintes de destinataires de communications de marketing direct de cet opérateur, que leur opposition au traitement de leurs données à de telles fins n'avait jamais été prise en compte en raison d'une erreur technique.

L'opérateur télécom ne disposait pas de mesures organisationnelles appropriées, c'est-à-dire d'une procédure spécifique lui permettant de détecter que le droit d'opposition de la personne concernée ne pouvait être effectivement exercé.

Par la suite, l'opérateur a retiré environ 8 000 personnes des destinataires de ses messages, qui avaient tenté sans succès de faire usage de leur droit d'opposition depuis 2013. L'Autorité a constaté une violation du droit d'opposition au traitement à des fins de prospection directe (article 21, paragraphe 3, du RGPD) ainsi que de l'article 25 (protection des données « by design ») du RGPD et a infligé une amende administrative de 200 000 euros sur la base des critères de l'article 83, paragraphe 2, dudit règlement.

Source : [https://edpb.europa.eu/news/national-news/2019/administrative-fines-imposed-telephone-service-provider\\_en](https://edpb.europa.eu/news/national-news/2019/administrative-fines-imposed-telephone-service-provider_en)

127. Veillez également à intégrer dans vos bases de données et mettre à jour régulièrement, voire automatiquement si cela est possible techniquement, les listes telles que la liste « Ne m'appellez plus » : <https://www.dncm.be/fr/suis-je-deja-dans-la-liste/> établie spécifiquement pour permettre aux personnes de ne pas être contactées par téléphone à des fins de marketing direct.



128. Si vous souhaitez en savoir davantage sur les mesures applicables dans le cadre de la protection des données « by design » et « by default », veuillez consulter les lignes directrices adoptées par l'EDPB sur le sujet<sup>29</sup>.

## **E. Vérifiez que vous disposez d'une base juridique**

### **1. Pourquoi une base juridique ?**

129. Un traitement de données à caractère personnel n'est autorisé que s'il trouve un fondement dans l'une des six bases juridiques prévues par l'article 6 du RGPD<sup>30</sup>. Vous ne pouvez traiter de données sans base juridique, vous devez donc vous assurer d'en disposer d'une avant le lancement de votre traitement.

130. Il est également essentiel de vous interroger sur votre base juridique dès lors que les conditions de chacune des bases prévues par l'article 6 du RGPD sont différentes.

131. La base juridique a des implications sur les droits des personnes concernées dont vous devez maîtriser les spécificités afin, non seulement d'en informer correctement les personnes mais également d'assurer l'exercice effectif de leurs droits.

132. Enfin, soyez attentif au fait que certaines législations spécifiques vous imposent de recourir à l'une ou l'autre base juridique pour encadrer un certain type de traitement. A cet égard, en matière de prospection commerciale par voie électronique, la e-Privacy Directive impose, en règle générale, de recourir au consentement des personnes concernées, tout en permettant, à titre d'exception et sous réserve de certaines conditions, de recourir à ce que l'on connaît sous le terme « soft opt-in », qui est une application allégée de la base juridique des intérêts légitimes.

133. Mise à part des cas très précis prévus par ces éventuelles lois, aucune base juridique n'est automatique. Il vous faut tenir compte du contexte du traitement que vous souhaitez mettre en place.

### **2. Est-il possible de changer de base juridique ?**

134. La base juridique ne peut pas être modifiée en cours de traitement. Cela signifie que si vous indiquez disposer d'une base juridique non appropriée ou que celle-ci « tombe » parce que ses conditions ne sont pas ou plus remplies, le traitement ne peut plus être poursuivi.

---

<sup>29</sup> [https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_guidelines\\_201904\\_dataprotection\\_by\\_design\\_and\\_by\\_default.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf)

<sup>30</sup> Conformément à l'article 8.2 de la Charte des droits fondamentaux précise que « ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. »



135. Par exemple, en cas de traitement fondé sur le consentement, dès lors que la personne retire son consentement, vous devez cesser tous traitements de données fondés sur cette base, à moins de continuer à traiter les mêmes données dans le cadre d'une autre finalité pour laquelle vous disposez d'une autre base juridique valable.
136. Il n'est pas non plus possible de disposer de deux bases juridiques pour une même finalité de traitement, ni d'alterner de l'une à l'autre. Vous devez faire un choix et vous y tenir.

#### Exception : le consentement obtenu en vertu de la directive 95/46/CE

Lorsque le RGPD est entré en vigueur, de nombreux responsables du traitement actifs en marketing direct qui fondaient leurs traitements de données sur la base du consentement ont été confrontés à une situation particulière. Le RGPD ayant renforcé les conditions de validité du consentement, il n'était plus possible de traiter les données à caractère personnel pour des finalités de marketing direct sur la base du consentement préalablement obtenu sauf dans l'hypothèse où ce consentement précédemment obtenu l'ait été conformément aux exigences RGDP.

Dans la négative, les Lignes directrices WP259 sur le consentement au sens du règlement 2016/679, adoptées par le G29 le 28 novembre 2017, telles que révisées le 10 avril 2018 et confirmées par l'EDPB lors de sa première séance plénière, ont ouvert la possibilité pour les responsables de traitement de changer, le cas échéant, de base juridique en cours de traitement. (Voir en ce sens la page 36 des lignes directrices mentionnées ci-avant)

Les responsables de traitement pouvaient donc soit renouveler le consentement précédemment obtenu en requérant un nouveau consentement conforme aux exigences RGPD, soit fonder ces traitements sur une autre base juridique tout en s'assurant que les traitements ainsi poursuivis respectent les principes de loyauté et de responsabilité.

La majorité des responsables de traitement actifs en marketing direct ont choisi de demander à nouveau leur consentement aux personnes concernées afin que le nouveau consentement soit conforme aux exigences de l'article 7 du RGPD. D'autres ont opté pour la poursuite de leurs activités de traitement sur la base des intérêts légitimes et ont par conséquent notamment fourni à leurs clients toute l'information requise sur le traitement de leurs données ainsi qu'une possibilité de s'opposer instantanément à ces traitements.

A cet égard, certains ont alors eu recours à l'exception du « soft opt-in », issue de la ePrivacy Directive. Cette exception n'est valable que pour les communication envers les clients et dans le seul cadre des communications électroniques pour la promotion de produits ou de services similaires à ceux déjà acquis par ces clients.

Nous verrons ci-après de quelle manière il convient d'aborder ces bases juridiques.



### 3. Quelle base juridique pour les traitements de marketing direct ?

137. Comme indiqué ci-avant au considérant 132, certaines lois spécifiques précisent la base juridique sur laquelle les responsables du traitement doivent obligatoirement se fonder afin d'être autorisés à traiter des données. Il vous appartient donc de vérifier que vous n'êtes pas tenus, par une loi spécifique, d'utiliser une base juridique spécifique. En outre, lorsque vous traitez des données à caractère personnel relevant de l'article 9 du RGPD, vous devez pouvoir démontrer que votre traitement de données s'appuie sur l'une des bases juridiques prévues par cette même disposition. Soyez également attentif au fait que les données relevant de l'article 10 du RGPD ne peuvent être traitées que moyennant le respect des conditions prévues par cet article.
138. Par ailleurs et en tout état de cause, n'oubliez pas d'informer les personnes concernées, conformément aux exigences de l'article 13 ou de l'article 14 du RGPD, quant à la base juridique de vos traitements. Quelle que soit la base juridique sur laquelle vous vous appuyez, elle doit être communiquée aux personnes concernées.
139. Aucune hiérarchie n'existe entre les bases juridiques prévues par le RGPD. Il vous appartient par contre d'être en mesure de démontrer que votre traitement s'appuie valablement sur une base des bases juridiques édictées par l'article 6 du RGPD (et 9.2 du RGPD, le cas échéant). Notez toutefois que certaines bases juridiques sont plus adaptées que d'autres à la réalité des traitements de données à caractère personnel réalisés dans le cadre de finalités de marketing direct. D'autres peuvent quant à elles être difficiles à appliquer valablement au regard des conditions qui leurs sont liées. Tel est notamment le cas de la base juridique « du contrat » prévue à l'article 6.1, b) du RGPD. Pour être applicable, cette base juridique implique que le traitement de données soit ***nécessaire à l'exécution d'un contrat*** conclu avec la personne concernée ***ou à l'exécution de mesures précontractuelles*** prises à la demande de celle-ci.
140. La notion fondamentale à prendre en considération dans l'examen d'un possible recours à cette base juridique est celle de la « nécessité ». Pour pouvoir reposer sur un contrat, le traitement de données doit être strictement nécessaire à la réalisation de ce contrat, ou de mesures précontractuelles demandées par la personne concernée. Recourir à la base juridique du contrat implique de définir spécifiquement l'objet de ce contrat, sa substance et son objectif fondamental. Cela implique également que tout traitement de données qui n'est pas directement nécessaire à la réalisation de cet objet ne pourra pas s'appuyer sur cette base juridique.
141. Comme le rappelle l'EDPB dans son avis sur la base juridique du contrat, un contrat ne peut étendre artificiellement les catégories de données ou types d'opérations de traitement nécessaires à la réalisation



du contrat auquel la personne concernée est partie<sup>31</sup>, et ce que recouvre un contrat ne dépend pas uniquement de la perspective du responsable du traitement mais également des attentes raisonnables de cette personne<sup>32</sup>. Au regard de l'extrême précision de cette base juridique, son application est donc des plus limitées.

#### Exemple 18

Madame Latige commande sur le site Internet de « La main verte » 2 sacs de terreau et 6 pots de géraniums. Elle souhaite se faire livrer à domicile et payer ses achats au moyen de sa carte de crédit. Pour pouvoir exécuter le contrat de livraison à domicile, il vous est nécessaire d'obtenir ses données « nom, prénom, adresse, et coordonnées bancaires ».

- ✓ Ces données sont nécessaires à l'exécution du contrat.

Si La main verte demande également les données relatives à sa date de naissance et à sa préférence en terme de couleurs et de fleurs, ces données ne sont pas nécessaires à la réalisation du contrat.

142. Il faut avoir particulièrement égard à la spécificité de l'objet et du contexte du contrat qui se noue entre le responsable du traitement et la personne concernée. C'est cette spécificité inhérente aux relations contractuelles qui limite la possibilité de recourir à la base juridique de l'article 6.1, b) pour des finalités de marketing direct, hormis dans les cas éventuels où l'objet du contrat conclu entre la personne concernée et une organisation serait précisément et uniquement de recevoir des communications de marketing direct et que les données à caractère personnel communiquées seraient ainsi uniquement traitées pour cette finalité.

143. Lorsqu'une prestation peut être réalisée en dehors du traitement de données nécessaire à l'exécution du contrat, cette autre prestation doit reposer sur une autre base juridique.

#### Exemple 18bis

Madame Latige en demandant à se faire livrer sa commande de terreau et de pots de fleurs à domicile communique ses coordonnées pour pouvoir recevoir sa commande. La semaine suivante, elle retrouve dans sa boîte aux lettres le catalogue automne-hiver de La main verte ainsi qu'un courrier de type « newsletter » de l'une de ses sociétés sœurs, active dans l'entretien des jardins.

- ✓ Le traitement des données de Madame Latige pour lui envoyer le catalogue ou les communiquer à des partenaires commerciaux n'était pas nécessaire à l'exécution du contrat de livraison de sa commande.
- ✓ Pour bien faire, il aurait fallu anticiper et :
  - Soit demander le consentement de Madame Latige, conformément aux exigences de l'article 7 du RGPD;
  - Soit lui indiquer que ses données pourraient être traitées pour lui envoyer des informations sur des produits similaires offerts par La main verte en lui offrant la possibilité de s'y opposer.

<sup>31</sup> Point 31 des Lignes Directrices 2/2019 de l'EDPB relative au traitement de données à caractère personnel fondé sur l'article 6(1)(b) du RGPD dans le contexte de la fourniture de services online aux personnes concernées. La version anglaise est disponible via ce lien : [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines-art\\_6-1-b-adopted\\_after\\_public\\_consultation\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf)

<sup>32</sup> Point 32 de ces lignes directrices.



#### Exemple 18 bis (suite)

- ✓ Dans le cas contraire, le traitement des données de Madame Latige pour ces finalités ultérieures devra passer le test de compatibilité de l'article 6.4 du RGPD.
- ✓ Dans un cas comme dans l'autre, il aurait fallu fournir à Madame Latige une information de qualité indiquant que La main verte traite ses données à caractère personnel afin de lui adresser son catalogue de produits et qu'elle communique ses données à tels et tels partenaires commerciaux de La main verte pour qu'eux aussi puissent lui adresser des communications promotionnelles, telles que des newsletters.

## 4. Les intérêts légitimes



Avant d'examiner la manière dont fonctionne la base juridique des intérêts légitimes, vous devez examiner si vous tombez ou non sous le coup de l'application de l'une ou l'autre loi spéciale qui vous empêcherait d'y recourir. Pour rappel, lorsque vous adressez des **communications non sollicitées de marketing direct par voie électronique**, en ce compris via des systèmes automatisés d'appel et de communication sans intervention humaine (automates d'appel), de télécopieurs ou de courrier électronique, **à des fins commerciales**, vous devez disposer du **consentement préalable** des abonnés ou des utilisateurs pour ce faire (article 13.1 de la Directive e-Privacy).

Toutefois, l'article 13.2 de cette Directive prévoit une **exception dite de « soft opt-in » pour les courriers électroniques** (défini comme : *tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère*) de marketing direct, adressés aux **clients ou abonnés existants** dont une **organisation aurait obtenu les coordonnées électroniques dans le cadre de la vente d'un produit ou d'un service de son propre fait**. Dans ce contexte, cette organisation est autorisée à adresser un courrier électronique à ces catégories de personnes à des fins de prospection directe **pour des produits ou services analogues qu'elle-même fournit** pour autant que lesdits clients se voient donner clairement et expressément la **faculté de s'opposer**, sans frais et de manière simple, à une telle exploitation des coordonnées électroniques **au moment où elles sont recueillies et lors de chaque message**, au cas où ils n'auraient pas refusé d'emblée une telle exploitation.

- ✓ **Ces règles s'appliquent uniquement dans ce contexte précis et uniquement dans celui-ci. Si vous souhaitez faire usage de cette exception, vous devez vous conformer à toutes ses conditions d'application.**
- ✓ **Les principes qui y sont retenus sont par ailleurs utiles à l'examen de la base juridique des intérêts légitimes pour les responsables du traitement qui souhaitent y recourir sans entrer dans les situations de traitement de données couvertes par le champ d'application de la e-Privacy Directive.**

#### L'article 6.1, f) du RGPD

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





144. Cette base juridique doit être examinée dans les trois aspects qu'elle recouvre :

Premièrement, il est essentiel que les intérêts que vous poursuivez en tant que responsable du traitement ou ceux poursuivis par les tiers auxquels vous souhaitez communiquer les données, soient reconnus comme **légitimes (a.1)**.

Deuxièmement, les traitements envisagés doivent être **nécessaires** à la réalisation de ces intérêts (**a.2**).

Troisièmement, il faut que la **mise en balance** de ces intérêts, face aux intérêts, libertés et droits fondamentaux des personnes concernées, penche en faveur des intérêts du responsable du traitement (**a.3**).

#### *[a.1. Identification de la légitimité de vos intérêts](#)*

145. Le **considérant 47 du RGPD** apporte une réponse lorsqu'il précise que « *le traitement de données à caractère personnel à des fins de prospection peut être considéré comme étant réalisé pour répondre à un intérêt légitime.* »

146. Sans le dire de manière péremptoire, cette assertion permet à tout le moins de considérer le marketing direct comme une finalité **pouvant être** considérée comme légitime au sens de l'article 6.1, f) du RGPD. Cette disposition n'implique cependant pas que tout traitement de données personnelles à des fins de prospection puisse être considéré comme légitime. **Cela n'est juste pas exclu par principe et reste possible.**

#### *[a.2. Vos traitements sont-ils nécessaires à la réalisation des finalités poursuivies dans le cadre de vos intérêts légitimes?](#)*

147. Demandez-vous si d'autres moyens qui sont à votre disposition permettraient d'aboutir au même résultat pour votre activité sans traitement de données à caractère personnel ou, sans traitement inutilement intrusif pour les personnes concernées. Si la réponse est non, vous pouvez passer à la dernière étape : la mise en balance.

#### **Exemple 19**

L'agence de voyage « Tornado » souhaite envoyer à ses clients récents son nouveau catalogue de destinations. Elle envoie le catalogue par voie postale mais voudrait s'assurer de ce que ses destinataires ouvriront bien leur boîte aux lettres. Elle envoie donc, en parallèle, un SMS et un courriel pour leur signaler qu'elle leur a envoyé le catalogue et qu'il serait vraiment dommage de ne pas le consulter.

- ✓ La finalité poursuivie est « envoyer le catalogue par la poste à mes clients récents » ;
- ✓ Le traitement des données « numéro de téléphone » et « adresse mail » de ces clients n'est pas nécessaire à la réalisation de cette finalité.



### a.3. Mise en balance

148. Vous devez évaluer si vos intérêts (attirer du monde à l'ouverture de votre nouveau magasin, faire connaître votre nouvelle gamme de produits ou maintenir votre marque dans l'esprit des gens après l'arrivée d'un gros concurrent par exemple) peut prévaloir sur les intérêts, libertés et droits fondamentaux des personnes dont vous entendez traiter les données à caractère personnel.
149. Pour réaliser cette mise en balance, le considérant 47 du RGPD fournit un paramètre important puisqu'il précise qu'il doit être tenu compte des **attentes raisonnables** des personnes concernées **fondées sur leur relation avec le responsable du traitement**. Ces « attentes raisonnables » sont celles que peut avoir la personne concernée quant aux traitements qui seront ou pourraient être faits de ses données, quant aux données à son sujet qui pourraient faire l'objet de ces traitements, quant à la/aux raison(s) (finalité(s)) pour lesquelles elles seront ou pourraient être traitées et par qui.

! Vous devez à ce titre particulièrement **avoir égard au public cible** dont vous traitez les données et vers lesquelles vous dirigez vos communications de marketing direct. Si celles-ci concernent ou peuvent concerner des mineurs, vous devez être extrêmement prudents avant de considérer que vos intérêts peuvent prévaloir leurs libertés et droits fondamentaux ainsi que sur leurs propres intérêts. Une autorité amenée à en juger fera preuve d'une plus grande sévérité en présence de mineurs.

150. Notez qu'en aucun cas vous ne pouvez invoquer un intérêt quelconque des personnes que vous visez à recevoir la communication que vous leur adressez (ou plus généralement à traiter leurs données à des fins de marketing direct). Les intérêts à mettre dans la balance face aux intérêts, libertés et droits fondamentaux des personnes concernées sont uniquement les vôtres, à savoir, en règle générale, faire la promotion de vos produits, services ou image de marque. L'intérêt que les consommateurs, clients, membres ou d'autres personnes, que vous convoitez, pourraient avoir à recevoir des communications de marketing direct ne rentre pas en ligne de compte.
151. Si vous entendez prendre des intérêts de tiers en compte dans la mise en balance, n'oubliez pas que ceux-ci ne priment pas nécessairement ceux des personnes concernées et que les attentes raisonnables de ces dernières sont primordiales dans votre mise en balance. Par exemple, si vous disposez des nouvelles adresses de résidence de vos clients en cas de déménagement de ceux-ci et que certains tiers souhaitent disposer de ces nouvelles coordonnées pour mettre à jour leurs propres fichiers clients/prospects, pour autant que ces intérêts soient légitimes (premier point qu'il vous appartient de vérifier) vous ne pouvez pas tenir compte de seuls intérêts mais devez également prendre en considération les attentes raisonnables des personnes concernées. A cet égard, il est important que vous précisiez cette possibilité dans



l'information que vous fournissez au préalable à vos clients/membres afin de leur permettre notamment, le cas échéant, de s'opposer à une telle communication de données aux tiers.



Vous devez également tenir compte des catégories de données à caractère personnel que vous entendez traiter. Si parmi ces données se retrouvent ou peuvent se retrouver des données relevant de la catégorie des données « sensibles », vous ne pouvez pas fonder votre traitement sur la base juridique des intérêts légitimes, conformément à l'article 9 du RGPD, à moins d'être dans les conditions de l'article 9.1, d).

#### Article 9.1, d)

« le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres dudit organisme ou aux personnes entretenant avec lui des contacts réguliers en liaison avec ces finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées.

LE SAVIEZ-VOUS



La CJUE, dans son arrêt C-708/18 du 11 décembre 2019 « *TK c. Asociația de Proprietari bloc M5A-ScaraA* », a rappelé, sur la base des dispositions de la Directive 95/46 CE, les principes suivants en matière d'intérêts légitimes et de l'exercice de mise en balance qu'il implique :

« **Le critère tenant à la gravité de l'atteinte aux droits et aux libertés** de la personne concernée constitue un **élément essentiel de l'exercice de pondération ou de mise en balance** au cas par cas, exigé par l'article 7, sous f), de la directive 95/46. » (considérant 56 de l'arrêt)

« À ce titre, **il doit notamment être tenu compte de la nature des données** à caractère personnel en cause, en particulier de la nature éventuellement **sensible** de ces données, ainsi que de la nature **et des modalités concrètes du traitement des données** en cause, en particulier **du nombre de personnes qui ont accès à ces données et des modalités d'accès à ces dernières**. » (considérant 57 de l'arrêt)

« Sont également pertinentes aux fins de cette pondération **les attentes raisonnables** de la personne concernée à ce que ses données à caractère personnel ne seront pas traitées lorsque, dans les circonstances de l'espèce, cette personne ne peut raisonnablement s'attendre à un traitement ultérieur de celles-ci. » (considérant 58 de l'arrêt)

152. Il en va de même pour les données à caractère personnel relevant de l'article 10 du RGPD qui ne peuvent être traitées que sous le contrôle de l'autorité publique ou sur la base d'une loi.

153. Le second élément qui doit être pris en compte dans cette mise en balance est l'obligation de prévoir des **garanties supplémentaires** qui pourraient limiter toute incidence injustifiée sur la personne concernée. Par ces garanties, on entend notamment : la minimisation des données traitées, l'utilisation de



technologies renforçant la protection de la vie privée; une transparence absolue et la mise en évidence d'un **droit général et inconditionnel de s'opposer au traitement**<sup>33</sup>.

154. **La possibilité de s'opposer** au traitement de données constitue en effet un **élément incontournable** dans l'examen **des garanties à fournir** lorsque vous entendez recourir à la base juridique des intérêts légitimes pour fonder vos traitements de données à des fins de marketing direct. Sans l'offre d'un droit d'opposition réel et efficace, aucun équilibre ne peut être trouvé entre les intérêts légitimes que vous poursuivez et les libertés et droits fondamentaux des personnes concernées.

### *b. Le droit d'opposition*

155. Veuillez noter tout d'abord que le droit d'opposition n'existe pas uniquement dans le cadre des traitements réalisés dans le cadre des finalités de marketing d'une part, ni ne se limite aux traitements fondés sur les intérêts légitimes d'autre part, puisqu'il peut également être exercé dans le cadre des traitements réalisés pour l'exercice d'une mission d'intérêt public.

156. Cela étant, en plus d'être l'une des conditions nécessaires au constat de garanties suffisantes lorsque le traitement de donnée s'appuie sur les intérêts légitimes, le RGPD prévoit spécifiquement un droit inconditionnel à s'opposer au traitement de ses données pour des finalités de marketing direct :

#### **Article 21.2 du RGPD**

« lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le **droit de s'opposer à tout moment au traitement** des données à caractère personnel la concernant à de telles **fins de prospection, y compris le profilage dans la mesure où il est lié à une telle prospection.** »

157. Cette spécificité du droit d'opposition aux traitements de données réalisés à des fins de marketing direct préexistait au RGPD puisque la Directive 95/46/CE le prévoyait déjà en son article 14 b).

158. L'inconditionnalité du droit à s'opposer est spécifique aux traitements réalisées à des fins de marketing direct en ce sens que lorsqu'une personne concernée fait usage de son droit d'opposition conformément à l'article 21.1 du RGPD, en dehors de toute finalité de marketing direct, une seconde mise en balance intervient opposant « la situation particulière » de la personne concernée et les motifs légitimes et impérieux que peut alors invoquer le responsable du traitement, qui pourraient justifier que le traitement soit, malgré l'opposition, maintenu.

<sup>33</sup> 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, adoptée le 9 avril 2014 par le Groupe 29, disponible via le lien suivant : [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_fr.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf)



159. Or, lorsqu'il est fait usage du droit d'opposition en matière de marketing direct, cette opposition donne lieu directement et sans examen supplémentaire, à **l'arrêt pur et simple de tout traitement de données** de la personne concernée pour des finalités de marketing direct, conformément à l'article 21.3 du RGPD.



**L'efficacité du mécanisme d'opposition tient particulièrement compte de la facilité qu'ont les personnes concernées à l'exercer d'une part, et de l'effectivité de son exercice d'autre part.**

### *b.1. Facilité de l'exercice du droit d'opposition*

#### **Considérant 70 du RGPD**

« Lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée devrait avoir le droit, **à tout moment et sans frais**, de s'opposer à ce traitement, y compris le profilage, dans la mesure où il est lié à une telle prospection, qu'il s'agisse du traitement initial ou ultérieur. Ce droit devrait **être porté à la connaissance de la personne concernée et présenté clairement et séparément de toute autre**

160. Cette facilité implique, entre autres, de **mettre le droit à s'opposer clairement en évidence, dans un langage simple et sans ambiguïté, et de le placer dans l'ensemble de vos communications de marketing** direct, dès la première de ces communications<sup>34</sup>, et bien entendu de le proposer **gratuitement**.

161. Il ne vous suffit pas d'indiquer la possibilité d'exercer ce droit dans votre « politique vie privée » (ou équivalent), il faut que cette possibilité soit présentée de façon certaine aux personnes concernées, sur un support approprié dont vous pouvez démontrer avec certitude qu'il a été mis sous les yeux de ces personnes, de manière à ce qu'ils ne puissent pas ne pas la voir.

162. Il faut également que la personne concernée puisse **l'exercer directement** (dès la fourniture de l'information obligatoire quant aux traitements de données que vous devez communiquer conformément aux exigences de l'article 13 du RGPD en cas de collecte directe, ou de celles de l'article 14 du RGPD en cas de collecte indirecte), **facilement** (si l'information obligatoire est fournie de manière digitale ou que vous contactez la personne via des canaux digitaux, un seul clic doit suffire), **sans aucune démarche supplémentaire** (une fois qu'elle s'est opposée, elle ne peut pas être requise de réitérer ni confirmer sa demande) **et sans frais** (direct ou indirect).


163. L'information fournie quant à ce droit d'opposition doit être claire et transparente. Les termes employés doivent être précis et non ambigus afin que la personne concernée comprenne bien à quoi elle peut

<sup>34</sup> Article 21.4 du RGPD « Au plus tard au moment de la première communication avec la personne concernée, le droit visé aux paragraphes 1 et 2 est explicitement porté à l'attention de la personne concernée et est présenté clairement et séparément de toute autre information.



s'opposer, comment et les conséquences (limitées à l'absence de futur traitement de ses données à des fins de marketing direct) d'une telle opposition.

#### Exemple 20

La firme Crystalclear spécialisée dans la vente d'objets en verre envoie à ses clients ayant commandé récemment des verres à vin un e-mail contenant une offre spéciale sur les verres à eau assortis. En ouvrant cet e-mail, les clients peuvent lire, dans l'ordre, le nom de la société, le titre de l'offre, un encart réservé à leur droit d'opposition et le contenu de l'offre. Cet encart précise « Vous recevez cette communication parce que vous avez récemment acheté nos produits. Si vous ne souhaitez plus recevoir de telles communications et que nous cessions de traiter vos données à caractère personnel pour nos finalités de marketing direct, cliquez ici  ».

- ✓ La place qu'occupe cette possibilité d'opposition ainsi que l'explication fournie qui s'y rattache facilitent et garantissent la possibilité pour la personne concernée de s'opposer au traitement de ses données pour des finalités de marketing direct.

#### Exemple 21

La société Ecran de fumée spécialisée dans la vente de cigarettes électroniques envoie à ses clients ayant récemment acheté des recharges sur son site une communication marketing par e-mail pour leur soumettre une offre d'une recharge gratuite à l'achat de deux. En ouvrant cet e-mail, les clients peuvent lire en grand le nom de la société et le contenu de l'offre affichée dans un coloris attractif. Tout en bas de la communication, en plus petits caractères et sans marquage distinctif, est indiqué « Je souhaite me désinscrire » avec un lien renvoyant à la politique de vie privée du site de la société Ecran de fumée dans laquelle, sous le titre « pourquoi nous traitons vos données ? » les clients de la société peuvent soumettre leur droit d'opposition par formulaire automatisé.



Dans ce contre-exemple, **plusieurs problèmes sont à relever** qui, chacun pris isolément, font que l'entreprise ne respecte pas les exigences requises en termes de facilité du droit d'opposition :

- ✓ **La place** qu'occupe la notification du droit d'opposition n'est pas conforme. Les personnes peuvent facilement la manquer.
- ✓ **La typologie** utilisée n'attire pas l'attention des personnes concernées sur leur droit d'opposition.
- ✓ **La terminologie** employée prête à confusion. **Le fait de se « désinscrire », « se désabonner » ou de « souhaiter ne plus recevoir » n'implique pas que les traitements de données à caractère personnel pour des finalités de marketing cessent.**
- ✓ Le fait que la personne **ne peut pas s'opposer au traitement de ses données** aussi facilement par le canal par lequel elle reçoit ces communications de marketing n'est pas acceptable.

164. Enfin, notez que rien ne vous empêche de permettre aux personnes concernées de sélectionner les traitements auxquels elles souhaitent s'opposer dans le cadre de vos finalités de marketing direct. Ainsi, si vos procédures le permettent, vous pouvez permettre aux personnes concernées de décider de s'opposer à ce que leurs données soient traitées dans le cadre d'un profilage et/ou pour l'envoi de courriels de newsletter et/ou de SMS promotionnels. Ceci pour autant que votre gestion interne de bases de données



permette effectivement avec certitude de respecter les droits des personnes concernées et de cesser les traitements de données auxquels les personnes concernées se sont opposées.

### *b.2. Effectivité de l'exercice du droit d'opposition*

#### **Article 21.3 du RGPD**

« lorsque la personne concernée s'oppose au traitement à des fins de prospection, les données à caractère personnel ne sont plus traitées à ces fins. »

165. Cela signifie non seulement que vous ne pouvez plus envoyer d'autres communications de marketing direct (ni même une communication visant à inciter la personne concernée à renoncer à sa décision) mais également **que vous ne pouvez plus du tout traiter les données à caractère personnel de cette personne dans le cadre de cette finalité de marketing direct, en ce compris à des fins de profilage par exemple**, dans la mesure où vous y recouriez pour réaliser vos communications de marketing direct. Tous les traitements de données liés aux finalités de marketing doivent cesser, sauf si ces mêmes traitements vous sont nécessaires pour la réalisation d'autres finalités pour lesquelles vous disposez d'une base juridique valable.

LE SAVIEZ-VOUS ?

?

L'Autorité de protection des données berlinoise a prononcé une sanction de 195.407 euros à l'encontre de la société Delivery Hero Germany GmbH, qui a été vendue au groupe néerlandais Takeaway en 2018. Cette société offrait également les services de livraison Foodora, Lieferheld et Pizza.de.

L'amende a été infligée pour diverses violations du RGPD, et notamment pour non-respect du droit d'opposition exercé par certains utilisateurs et anciens clients. Par exemple, huit anciens clients de Delivery Hero s'étaient " plaints de courriels publicitaires non sollicités de la part de l'entreprise ". En outre, une personne avait reçu 15 courriels promotionnels, même si elle s'était expressément opposée à l'envoi de tels messages.

En outre, plusieurs personnes n'avaient pas reçu d'information sur les renseignements que Delivery Hero avait stockés à leur sujet.

Pour plus d'information sur cette affaire : <https://www.gruenderszene.de/food/dsgvo-bussgeld-takeaway>



En outre, lorsque l'article 21.3 précise que « les données ne sont plus traitées à ces fins », il convient d'admettre que cela implique non seulement vos traitements de données à finalité de marketing mais également ceux des tiers auxquels vous avez communiqué ces données pour de telles finalités, charge pour vous de les en avertir. Si un traitement devient caduc, par conséquent ceux qui en découlent le deviennent également.



166. De la même manière, si vous aviez collecté certaines données uniquement pour vos finalités de marketing, vous ne pouvez en principe plus conserver celles-ci<sup>35</sup>, sauf cas de conservation pour l'exercice de contestations, et défense des droits en justice pour la personne concernée, pour la protection et la défense des droits d'une autre personne ou encore pour des motifs importants d'intérêt public de l'Union européenne ou d'un Etat membre. Vous devez toutefois, dans ce cas, limiter le traitement des données à cette seule finalité, conformément à l'article 18.1, c) et 18.2 du RGPD.

*c. L'article 6.1, f) : une base juridique évidente pour les traitements à des fins de marketing direct ?*

167. En plus des réserves émises ci-avant, se pose également la question du recours à cette base juridique pour l'ensemble de ce que l'on a pu définir comme constituant des « traitements de données personnelles pour des finalités de marketing direct ».

168. Tout d'abord, il y a lieu de distinguer les communications adressées à un client existant de celles adressées à un prospect. Les attentes raisonnables d'un client existant ne sont en effet pas les mêmes que celles d'un prospect, notamment au vu de l'absence de relation existante entre vous et ces prospects. Lorsque vous n'avez jamais eu de relation avec une personne concernée ou si cette relation remonte à très longtemps sans qu'elle n'ait été suivie depuis lors, la base juridique des intérêts légitimes ne peut pas être invoquée, faute d'attente raisonnable de leur part quant à la réception d'une communication de votre part.

169. Il peut aussi exister des situations plus nuancées, comme celles des personnes ayant marqué leur intérêt pour vos services, produits ou actions. Posez-vous toujours la question de leurs attentes raisonnables.

**Exemple 22**

Monsieur Curiosa se rend sur le site Internet de Blanches comme Neige qui vend des solutions de blanchiment dentaire. Il souhaite en apprendre davantage **sur l'un des produits proposés** et envoie une demande dans l'onglet de contact réservé à cet effet. Il introduit pour cela son adresse e-mail.

- ✓ En introduisant son adresse e-mail pour recevoir les informations sollicitées, Monsieur Curiosa ne s'attend pas raisonnablement à recevoir des newsletters et autres communications promotionnelles de Blanches comme Neige. Par contre, la société peut demander à Monsieur Curiosa, lors de sa réponse à sa question, s'il consent à recevoir des communications promotionnelles de Blanches comme Neige par la suite.
- ✓ Si Monsieur Curiosa, en contactant Blanches comme Neige avait précisé « je suis super fan de vos produits j'aimerais tout connaître, pourriez-vous me tenir informé de vos produits et vos promotions ? », ses attentes raisonnables seront manifestement de recevoir les communications de marketing direct de cette société. Il n'en reste pas moins que Blanches comme Neige devra, à la première communication, informer Monsieur Curiosa notamment sur son droit d'opposition.

<sup>35</sup> Article 5.1, e) du RGPD : « les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. (...) ».





170. Cet exemple ne signifie pas, *a contrario*, que le fait d'envoyer des communications de marketing direct à un client sur la base juridique de l'intérêt légitime uniquement parce qu'il est « client » se justifie en tout état de cause. Il vous appartient de mesurer, au préalable, si les conditions de licéité d'utilisation de cette base juridique sont rencontrées en tout point.
171. L'article 13.2 de la e-Privacy Directive apporte un élément de réponse important à prendre en considération sur ce point. Celui-ci prévoit qu'une personne peut exploiter les données à caractère personnel de ses clients existants pour lui adresser des courriers électroniques « **pour des produits ou services analogues qu'elle-même fournit** ».
172. Lorsque vous vous interrogez sur le recours à la base des intérêts légitimes pour vos traitements en matière de marketing direct, prenez en considération la nature similaire ou analogue de ce dont vous faites la promotion dans votre communication, en plus des liens qui existent entre votre organisation et les destinataires de votre communication. Par exemple, si vous avez vendu un ordinateur à une personne en 2019 et que vous lui adressez une communication de marketing relative à du chocolat que votre enseigne vend également, vous pouvez difficilement vous appuyer sur le critère des produits similaires et analogues. Si par contre votre communication porte sur des logiciels antivirus, il s'agit de produits similaires et analogues. Cela signifie que même si votre organisation, enseigne, propose une large gamme de produits ou services différents les uns des autres, il ne suffit pas d'analyser la relation de client ou non client des personnes auxquelles vous entendez adresser des communications de marketing direct. Il vous faut aussi tenir compte de l'ensemble des critères des attentes raisonnables de ces personnes, exigence fondamentale du RGPD dans le cadre de votre mise en balance.

#### Exemple 23

Monsieur Curiosa commande un kit de blanchiment dentaire sur le site de Blanches comme Neige. Il devient ainsi client de cette société. Plusieurs mois après cette commande, Blanches comme Neige développe un nouveau pôle d'activités et se lance sur le marché des détachants textiles. Elle souhaite le communiquer à tous ses clients existants.

- ✓ Le critère des produits similaires ou analogues n'est pas rencontré.
- ✓ Il est préférable de recourir à la base juridique du consentement pour éviter de se voir sanctionner pour traitement de données sans base juridique valable.

173. L'illustration faite sur la base de l'article 13 de la e-Privacy Directive ne doit pas être lue comme excluant les communications non électroniques de la possibilité d'être fondées, le cas échéant, sur la base juridique des intérêts légitimes, de la même manière qu'elle ne doit pas induire en erreur sur le fait que cette base ne pourrait être utilisée par des organisations ne faisant pas la promotion de produits ou de services. Si vous êtes une organisation caritative et souhaitez envoyer des courriers postaux ou électroniques par exemple, pour faire la promotion de vos activités et œuvres, vous êtes en mesure d'examiner valablement



si la base juridique des intérêts légitimes peut s'appliquer à vos traitements de données à caractère personnel.

174. Au regard de l'analyse qui précède, gardez à l'esprit que si la base juridique des intérêts légitimes n'est pas à exclure automatiquement pour fonder des traitements de données à caractère personnel dans le cadre du marketing direct, elle n'est pas nécessairement aisée à appliquer à ceux-ci, ni parfois même valable, selon les caractéristiques propres à vos traitements.

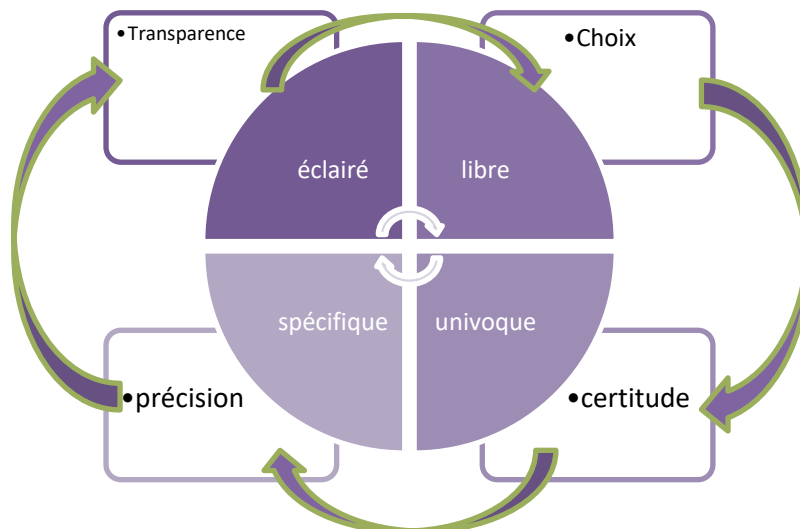
## 5. Le consentement

### a. Notion

#### Article 4.11 du RGPD

« 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. »

175. Schématiquement, un consentement valide se présente comme suit :



176. Les critères de validité du consentement au sens du RGPD forment un tout indissociable. Il ne peut y avoir de consentement qui ne soit que spécifique libre et univoque s'il n'est pas éclairé et inversement.



Si vous effectuez des traitements de données de à des fins de marketing direct sur la base du consentement des personnes concernées, vous devez vous assurer de la réunion des 4 conditions précitées, sans quoi, vous ne disposez pas d'une base juridique valable pour vos traitements de données, ce qui les rend illicites et donc, sujets à sanction.



La CNIL, Autorité de protection des données française, a prononcé le 21 janvier 2019 en formation restreinte, une sanction de 50 millions d'euros à l'encontre de la société GOOGLE LLC en application du RGPD pour manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité.

Elle a ainsi constaté que les informations fournies par GOOGLE ne sont pas aisément accessibles, claires et compréhensibles pour les utilisateurs et qu'elles ne permettent pas de comprendre clairement que la base juridique sur laquelle repose les traitements de données à des fins de personnalisation de la publicité est le consentement.

La formation restreinte a estimé que le consentement n'est pas valablement recueilli pour deux raisons.

Tout d'abord, le consentement des utilisateurs n'est pas suffisamment éclairé. L'information sur ces traitements, diluée dans plusieurs documents ne permet pas à l'utilisateur de prendre conscience de leur ampleur. Par exemple, dans la rubrique dédiée à la « Personnalisation des annonces », il n'est pas possible de prendre connaissance de la pluralité des services, sites, applications impliqués dans ces traitements (Google search, You tube, Google home, Google maps, Playstore, Google photo...) et donc du volume de données traitées et combinées.

Ensuite, la formation restreinte constate que le consentement recueilli n'est ni « spécifique » ni « univoque ». Bien que GOOGLE permette de paramétrer les options d'utilisation de ses services lors de la création d'un compte, le RGPD n'est pas pour autant respecté dès lors que l'utilisateur doit faire la démarche de cliquer sur « plus d'options » pour accéder au paramétrage, où, qui plus est, l'affichage d'annonces personnalisées est pré-coché par défaut.

Or le consentement n'est « univoque », comme l'exige le RGPD, qu'à la condition que l'utilisateur effectue un acte positif (cocher une case non précochée par exemple). Enfin, avant de créer son compte, l'utilisateur est invité à cocher les cases « j'accepte les conditions d'utilisation de Google » et « j'accepte que mes informations soient utilisées telles que décrit ci-dessus et détaillées dans les règles de confidentialité » pour pouvoir créer son compte. Un tel procédé conduit l'utilisateur à consentir en bloc, pour toutes les finalités poursuivies par GOOGLE sur la base de cet accord (personnalisation de la publicité, reconnaissance vocale, etc.). Or le consentement n'est « spécifique », comme l'exige le RGPD, qu'à la condition qu'il soit donné de manière distincte pour chaque finalité.

Pour davantage d'information sur cette affaire : [www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la](http://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la)

## ***b. Examen des conditions de validité du consentement***

### ***b.1. Un consentement éclairé***

177. La personne qui donne son consentement doit parfaitement comprendre pourquoi et à quoi elle consent. Cette condition est inextricablement liée à l'information qui doit être fournie par le responsable du traitement à la personne concernée, au moment de la collecte de ses données si elles sont obtenues



directement auprès de la personne concernée ou dans un délai raisonnable si elles ne sont pas obtenues auprès de cette personne. Cette information doit être certaine (et donc pas simplement « accessible » mais présentée d’emblée à la personne de sorte qu’elle ne puisse pas ne pas la voir), claire, formulée dans un langage compréhensible et complète (et porter aussi par exemple sur toute opération de profilage qui serait effectuée en plus des autres traitements de données qui sont parfois plus visibles pour la personne concernée).

178. En outre, la demande de consentement doit être présentée séparément de toute autre demande (en ce compris d’acceptation de conditions générales, de politiques relatives à la vie privée ou de poursuite de la navigation).

**Article 7.2 du RGPD :**

« Si le consentement (...) est donné dans le cadre d’une déclaration écrite qui concerne d’autres questions, la demande de consentement est présentée dans une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulées en des termes clairs et simples (...). »

179. L’exigence de transparence constitue l’un des piliers fondamentaux du régime mis en place par le RGPD. Allant de pair avec les principes de loyauté et de licéité du traitement, fournir une information de qualité aux personnes concernées est indispensable pour leur permettre de prendre une décision en toute connaissance de cause.

180. Pour que le consentement soit éclairé, votre document d’information doit être conforme aux articles 13 et/ou 14 du RGPD et dès lors, au minimum, contenir les aspects suivants<sup>36</sup> :

- ✓ L’identité du responsable du traitement et des destinataires des données, à tout le moins, les catégories de destinataires et les finalités qu’ils poursuivent,
- ✓ La finalité de chacune des opérations de traitement pour lesquelles le consentement est sollicité,
- ✓ Les opérations de traitements, en particulier les plus intrusives (par exemple profilage et/ou la prise de décision automatisée conformément à l’article 22, §2, c) du RGPD, le cas échéant,)),
- ✓ Les données ou catégories de données collectées et utilisées,
- ✓ Le droit de retirer son consentement à tout moment,
- ✓ En cas de transfert des données vers certains pays n’appartenant pas à l’EEA, 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 46 du RGPD

<sup>36</sup> EDPB, avis WP259 rév. 01, « *Lignes directrices sur le consentement au sens du règlement 2016/679* », p.15, point 3.3.1.



## b.2. Un consentement libre

**Les considérants 42 et 43 du RGPD peuvent se résumer comme suit :**

Le consentement comme base juridique ne sera pas valable si:

- La personne est **contrainte** de le donner pour éviter un **préjudice** ;
- La personne **ne peut retirer** son consentement **à tout moment** ; ou si
- Le consentement est présenté comme une **partie non négociable** des conditions générales.

181. L'individu auquel on demande de consentir au traitement de ses données doit avoir une réelle possibilité d'accepter ou de refuser, sans pour autant se voir priver de l'accès à un service ou à tout autre avantage, en cas de refus (comme par exemple, l'accès aux articles de presse mis en ligne gratuitement, ne peut être conditionné au traitement de données à caractère personnel pour des finalités de marketing direct).



Ne conditionnez pas la fourniture de vos produits ou services (même gratuits) à l'acceptation du traitement de données à caractère personnel non-nécessaires à la prestation du service ou à la fourniture du produit. N'essayez pas de forcer ou d'inciter, de quelque manière que ce soit, les personnes concernées, à vous fournir leur consentement à ces traitements.

182. Afin de déterminer si le consentement est donné librement, l'article 7.4 RGPD précise qu'« *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.* »

183. L'usage des termes « entre autres » signifie qu'une série d'autres situations peuvent tomber sous le coup de cette disposition et que toute pression ou influence inappropriée exercée sur la personne concernée en l'empêchant d'exercer sa volonté rendra le consentement non valable avec les conséquences que cela implique<sup>37</sup>.

### Exemple 24

Une application mobile de coaching sportif demande à ses futurs utilisateurs de pouvoir traiter leur données à caractère personnel « pour pouvoir fonctionner et leur envoyer de la publicité comportementale ». La publicité comportementale n'est en rien nécessaire au fonctionnement correct de l'application mobile. Cependant, l'application ne laisse pas le choix à ses futurs utilisateurs : ils acceptent tout ou ils n'ont droit à rien. Dès lors que les personnes ne peuvent utiliser l'application mobile sans consentir au traitement de leurs données à des fins publicitaires, leur consentement ne peut être considéré comme étant donné librement et ce, même si certaines personnes consentent réellement au traitement de leurs données pour de telles finalités.

<sup>37</sup> WP259 rév. 01, p.6.



## LE SAVIEZ-VOUS ?



Notre Autorité infligé une sanction de 10.000 euros à un commerçant qui utilisait la carte d'identité électronique afin de créer une carte de fidélité pour ses clients, sans proposer d'autre alternative comme moyen d'identification.

Le plaignant ne voulant pas présenter sa carte d'identité, la carte de fidélité lui a été refusée alors qu'il a proposé de transmettre par écrit au commerçant les données le concernant pour pouvoir bénéficier d'une carte de fidélité. Du fait de l'absence d'alternative(s), si les clients refusent que leur carte d'identité électronique soit utilisée pour la création d'une carte de fidélité, ils en sont pénalisés et ne peuvent pas bénéficier des mêmes avantages et réductions que les autres.

La Chambre Contentieuse de l'APD a jugé cette pratique non conforme au RGPD notamment au regard du fait que le consentement donné dans le cas d'espèce ne peut être considéré comme un consentement donné librement car aucune alternative n'est proposée aux clients.

Pour plus d'information : [www.autoriteprotectiondonnees.be/news/APD-sanctionne-un-commercant-pour-lutilisation-de-l-eid-pour-une-carte-de-fidelite](http://www.autoriteprotectiondonnees.be/news/APD-sanctionne-un-commercant-pour-lutilisation-de-l-eid-pour-une-carte-de-fidelite)

### *b.3. Un consentement spécifique*

184. Le consentement donné doit l'être pour « une ou plusieurs finalités spécifiques ». En outre, en cas de pluralité de finalités, la personne concernée doit pouvoir choisir parmi ces finalités, si elle souhaite ne pas consentir à certaines d'entre elles.

185. Cette exigence procède de la volonté d'accorder un certain degré de contrôle aux personnes concernées quant aux usages de leurs données à caractère personnel. Il en va également de l'obligation de transparence à l'égard de celles-ci et de leur liberté à consentir à certaines traitements et pas à d'autres, notamment en matière de placement de cookies pour lesquels vous devez, entre autres, distinguer clairement entre les cookies fonctionnels de ceux qui ne le sont pas, tels que les cookies analytiques.



## LE SAVIEZ-VOUS ?



Le 17 décembre 2019, notre Autorité a infligé une sanction de 15.000 euros à l'encontre d'une société en raison de la contrariété aux règles du RGPD de sa technique de récolte de consentement au placement de cookies.

L'APD a ainsi notamment pu constater un manque de vigilance répété de cette société à l'égard de son obligation de transparence prévues par les articles 12 et 13 du RGPD et pour ne pas avoir obtenu de consentement valable (opt-in) pour le placement de cookies.

L'intégralité de cette décision est disponible via le lien suivant :

[www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/BETG\\_12-2019\\_FR.pdf](http://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/BETG_12-2019_FR.pdf)

### Exemple 25

#### Placement de cookies sur votre site Internet

- ✓ Vous devez informer les visiteurs de votre site Internet des cookies que vous envisagez d'utiliser, ainsi que de leur(s) finalité(s) et des données qu'ils collectent. Cette information doit être visible, claire et accessible dès que la personne concernée commence sa navigation sur votre site Internet. Le plus pratique est de recourir à un bandeau d'information à cet égard.
- ✓ Dans ce bandeau d'information (par exemple), vous devez indiquer la possibilité et la manière de paramétrer les cookies, afin de garantir aux personnes concernées la possibilité de consentir ou non à la collecte de certaines de leurs données par le placement de certains types de cookies. Pour permettre ce choix, vous devez être extrêmement clair quant aux finalités poursuivies par collecte de données via des cookies, par exemple :
  - Acceptez-vous le dépôt et la lecture de cookies afin que **nous** [nom de l'organisation] puissions analyser vos centres d'intérêts pour vous proposer des publicités personnalisées ?
  - Acceptez-vous le dépôt et la lecture de cookies afin que **nos partenaires** [listing des partenaires concernés] puissent analyser vos centres d'intérêts pour vous proposer des publicités personnalisées ?
  - Acceptez-vous le dépôt et la lecture de cookies afin d'analyser votre navigation et nous permettre de mesurer l'audience de notre site Internet ?

186. Les cookies intrusifs et non fonctionnels doivent être paramétrés par défaut comme inopérants. Vous ne pouvez, en tout état de cause, exiger des personnes concernées qu'elles doivent à chaque fois retourner dans leurs propres paramètres de navigation pour empêcher le placement de cookies non fonctionnels.

187. Comme toutes les exigences liées au consentement, le caractère spécifique du consentement est inextricablement lié à l'information complète qui doit être fournie par le responsable du traitement. Vous devez donc énumérer clairement et spécifiquement chacune des finalités poursuivies sans quoi, le consentement donné n'est pas valable car pas spécifique.



### Exemple 26

La société « HouseKeyper » propose plusieurs services à ses clients, lesquels peuvent être client de tous les services proposés ou de certains d'entre eux. HouseKeyper collecte les données à caractère personnel dans le cadre de la prestation de chacun de ses services, conformément au contrat qui la lie à ses clients. Afin d'améliorer son marketing en adressant des communications plus ciblées à ses clients, cette société aimerait enrichir ou coupler les données qu'elle collecte dans le cadre de son service de livraisons à domicile avec les données qu'elle collecte dans le cadre de son service de livret d'épargne. Elle aimerait également fournir ce résultat à des tiers intéressés par ces données couplées.

- ✓ Pour pouvoir effectuer ce couplage/enrichissement de données, HouseKeyper est obligée de demander le consentement distinct, éclairé, spécifique, libre et univoque de ses clients quant à cette opération de couplage/enrichissement.

188. La précision des finalités permet d'éviter un détournement d'usage des données à caractère personnel. La personne a consenti à la finalité A mais pas à la finalité B. Si elle ne savait pas que ses données seraient traitées dans le cadre des finalités A et B, le consentement fourni pour l'une ne peut servir pour l'autre. Cela vaut autant pour des finalités poursuivies par le même responsable de traitement que pour des finalités (ultérieures ou pas) poursuivies par des tiers.

### Exemple 26 bis

Pour bien faire, en plus d'une information complète, claire, transparente et accessible concernant les finalités et les traitements concernés, HouseKeyper devrait demander le consentement de ses clients de la manière suivante :

« Je consens à ce que les données à caractère personnel à mon sujet récoltées via « ce formulaire » dans le cadre du service de livraison auquel j'ai souscrit, soient enrichies ou couplées avec les données à caractère personnel à mon sujet récoltées par HouseKeyper dans le cadre de la conclusion de mon contrat d'ouverture de livret d'épargne :

- ✓ afin de produire un résultat, tel qu'un profile-type de consommateur, utile à nos campagnes de marketing pour vous proposer des produits mieux ciblés : OUI/NON
- ✓ à ce que le résultat de cet exercice et l'assimilation de ce résultat à un profile-type ainsi que vos coordonnées e-mail soient communiquées à et utilisées par [nom de l'organisation en question], active dans le secteur de la vente de [décrire la catégorie d'activités] à des fins d'envoi de publicités ciblées par e-mail [décrire] : OUI/NON.

189. Si vous souhaitez traiter des données pour une finalité différente que celle pour laquelle vous les avez originellement collectées et que ce premier traitement se fonde sur le consentement comme base juridique, vous devez solliciter le consentement pour cette nouvelle finalité de manière complémentaire.

### Exemple 27

Un opérateur télécom dispose des données de ses clients pour la fourniture d'un accès à des chaînes de télévision et de sa gestion administrative. Il souhaite leur transmettre des publicités commerciales ciblées sur base des préférences et habitudes de consommation, donc en pratique, sur base d'une analyse des programmes qu'ils visionnent. Cette finalité d'analyse comportementale aux fins de transmission de publicité ciblée n'était pas prévue au moment de la collecte initiale des données à caractère personnel de ses clients. Leur consentement doit dès lors leur être demandé de manière spécifique pour cette nouvelle finalité.





190. Si vous poursuivez différentes finalités de marketing direct et/ou que celles-ci impliquent différentes sortes d'opérations de traitement, soyez précis. Permettez à la personne de consentir à chacune d'elles séparément. N'utilisez pas un bouton unique d'acceptation (consentement « en bloc » types boutons « Tout accepter ») ou une formulation trop générale. Lister clairement les différentes finalités (et opérations de traitements qui y correspondent) pour lesquelles vous demandez le consentement afin que les personnes concernées puissent faire valoir leur consentement de manière sélective, le cas échéant.

#### *b.4. Un consentement univoque*

191. Le RGPD prévoit que le consentement nécessite un acte positif clair, qui doit être donné au moyen d'une déclaration, écrite ou orale. Cette condition a avant tout pour but **d'éviter la moindre ambiguïté quant à la volonté de la personne concernée** de fournir son consentement.

192. Cette exigence met un terme à la méthode des cases pré-cochées, des cases à cocher pour manifester son refus de consentement (**opt-out**), ou encore à la technique consistant à annoncer que la poursuite de la navigation sur un site web équivaut à un consentement (à la collecte de données via des cookies par exemple).

**NEW**

Lorsque la base juridique retenue pour vos traitements de données est le consentement, le critère de l'acte positif clair retenu par le RGPD ne vous permet plus de considérer le silence ou l'inactivité de la personne concernée comme une indication de son choix, pas plus que le simple fait qu'elle continue à utiliser un service ou qu'elle ne décoche pas une case pré-cochée.

**LE SAVIEZ-VOUS**

?

Dans son arrêt C-673/17 du 1<sup>er</sup> octobre 2019 nommé « Planet49 », la CJUE a estimé que le consentement fourni par le moyen d'un opt-out et/ou d'une case pré-cochée était insuffisant pour valider le consentement des internautes au placement de cookies.

Les internautes qui souhaitaient participer à un jeu concours organisé par Planet49 étaient redirigés vers une page web sur laquelle ils devaient inscrire leurs nom et adresse. Sous les cases à remplir pour l'adresse se trouvaient deux mentions, accompagnées de deux cases à cocher dont la seconde fait l'objet de la question préjudicielle soumise à la CJUE.

[...]



Cette case était cochée par défaut et se lisait comme suit :

*« J'accepte que le service d'analyse du web Remintrex soit mis en œuvre chez moi. En conséquence, l'organisateur du jeu promotionnel, [Planet49], installera des cookies après avoir été agréé pour le jeu promotionnel, ce qui lui permettra d'exploiter par Remintrex mes navigations sur le web et mes visites sur les sites web des partenaires publicitaires et d'adresser de la publicité centrée sur mes intérêts. Je peux supprimer les cookies à tout moment. Lire les détails ici. »*

En activant le lien électronique figurant dans la mention accompagnant la seconde case à cocher, sous le mot « ici », apparaissaient les informations relatives au placement de cookies sur le disque dur des internautes.

La Cour a estimé que le consentement de la personne concernée peut rendre un tel traitement licite pour autant que ce consentement soit « indubitablement » donné par la personne concernée. Or, dit-elle, « seul un comportement actif de la part de cette personne en vue de manifester son consentement est de nature à remplir cette exigence ». Elle ajoute qu'« à cet égard, il apparaît pratiquement impossible de déterminer de manière objective si l'utilisateur d'un site Internet a effectivement donné son consentement au traitement de ses données personnelles en ne décochant pas une case cochée par défaut ainsi que, en tout état de cause, si ce consentement a été donné de manière informée. En effet, il ne peut être exclu que ledit utilisateur n'ait pas lu l'information accompagnant la case cochée par défaut, voire qu'il n'ait pas aperçu cette case, avant de poursuivre son activité sur le site Internet qu'il visite. »

Voir : <http://curia.europa.eu/juris/document/document.jsf?docid=218462&doclang=FR>

193. Dans le contexte numérique, (achat de produits en ligne, inscriptions diverses etc), les personnes concernées font l'objet de nombreuses demandes de consentement, desquelles il peut résulter à la fois une perte de contrôle des personnes concernées et une certaine lassitude les poussant à répondre « oui » ou « non » à tout par automatisme.

194. Afin d'éviter ce risque, vous pouvez varier les manières de recueillir le consentement. Les cases à cocher ne sont pas la seule technique envisageable.

### Exemple 28

En naviguant sur un site Internet, une bannière s'affiche indiquant « en faisant glisser la barre vers la gauche, vous consentez à l'utilisation de l'information X à une fin Y. Veuillez répéter le mouvement pour confirmer ».

Pour autant que les consignes soient claires pour que la personne comprenne exactement ce à quoi elle consent, qu'elle est en train d'y consentir en effectuant le mouvement et qu'elle peut poursuivre sa navigation sans effectuer ce mouvement, le consentement recueilli de la sorte est valable au regard du RGPD. De la même manière, agiter la main devant une caméra intelligente, faire tourner son smartphone dans le sens indiqué ou, enregistrer un consentement verbal, sont autant de manières de recueillir valablement le consentement de la personne.





Ne perdez pas de vue que le recours au mécanisme dit de **l'opt-out** ne donne **pas** lieu à la récolte d'un **consentement valable** !

#### Exemple 29

La société « Pas vu Pas pris » souhaite utiliser sa base de données clients pour leur adresser des informations sur les nouveaux services qu'elle propose pour fournir des alibis. L'entreprise n'avait pas demandé préalablement à ses clients s'ils souhaitaient, ou non, recevoir de telles communications commerciales. L'entreprise songe dès lors à leur adresser un courrier ou un email par lequel il leur sera spécifié qu'ils sont libres de refuser de recevoir de telles communications. Le courrier indique une adresse email à laquelle les clients peuvent envoyer un message s'ils ne veulent pas recevoir ces communications. L'email prévoit une case à cocher pour ce faire. Les deux communications précisent qu'en l'absence de réponse contraire de leur part ou de « cochage » de la case, elle considèrera qu'ils consentent à recevoir des publicités promotionnelles.

- ✓ L'absence de réaction des clients de Pas vu Pas pris ne constitue pas un consentement valable au regard du RGPD.

195. Le fait qu'une personne ne clique pas une case d'opt-out ne permet pas au responsable du traitement de déduire de façon certaine que cette personne a consenti de manière univoque au traitement de ses données à caractère personnel. En outre, comme nous le verrons ci-après, le RGPD ajoute une obligation d'être en mesure de prouver le consentement pour le responsable du traitement qui entend en faire usage comme base juridique à son traitement de données. Sans cette preuve, le traitement est illicite et donc susceptible d'engendrer des sanctions pour celui-ci. Mieux vaut donc toujours recourir à un mécanisme tel que l'opt-in.



L'exigence d'obtenir un acte positif de consentement ne peut pas être lue de manière dissociée des autres exigences applicables au consentement. Pour rappel, le consentement doit être donné de manière informée. Cela implique notamment que la personne doit comprendre non seulement ce à quoi elle consent mais également qu'elle est en train de consentir.

196. Les personnes concernées doivent pouvoir comprendre clairement les choix dont elles disposent et, si plusieurs choix existent, celui de consentir au traitement de leurs données à caractère personnel pour des finalités de marketing direct spécifiques doit apparaître clairement et de façon similaire à tout autre choix. De la même manière, si le responsable du traitement envisage d'utiliser ces données dans le cadre de plusieurs finalités de marketing direct, la personne concernée doit être en mesure d'en accepter certaines et en refuser d'autres, le cas échéant. Un bouton unique permettant à la personne de cocher l'ensemble des cases par lesquelles on lui demande un consentement n'est donc pas valable.



### Exemple 30

Une personne passe commande sur le site de prêt-à-porter « Cache misère ». Pour pouvoir finaliser sa commande, il lui est demandé de fournir ses données de contact. Une fois ces informations remplies, une fenêtre « pop up » apparaît à l'écran indiquant, de manière visible, « Vos données sont utilisées pour vous envoyer la commande. Nous autorisez-vous à utiliser ces données pour la facturation ? ». En bas à droite de ce cadre, un bouton à cliquer d'une taille apparente et d'une couleur différenciée indique « tout accepter ». Or, en haut à gauche, en petit caractère et fondu dans la fenêtre, une flèche d'agrandissement de la fenêtre permet de découvrir l'ensemble du message, lequel précise également que « vous nous autorisez à utiliser vos données pour vous envoyer nos offres promotionnelles. Vous nous autorisez à communiquer vos données à nos partenaires commerciaux. »

- ✓ Bien que la personne ait eu la possibilité de prendre connaissance de ces informations complémentaires et d'accepter ou non ces différents traitements de données, cette possibilité n'était pas claire. De ce fait, elle n'a pas pu consentir valablement à l'ensemble des traitements de ses données.

197. Ne demandez pas le consentement de manière ambiguë ou superficielle . Si le consentement de la personne doit être non équivoque, il vous appartient avant tout de ne pas l'être.

198. En outre, le fait d'avoir consenti à recevoir des communications promotionnelles ou informatives par courriel n'implique pas que l'on consente à recevoir des appels téléphoniques. Il est donc **nécessaire de veiller à recueillir un consentement** non équivoque tant **sur le contenu** des communications que **sur les moyens utilisés** pour cela. Il y a lieu dès lors de dissocier les demandes si plusieurs outils de communications peuvent être utilisés, plutôt que de formuler une demande unique.

199. Enfin, si vous recueillez le consentement par la voie verbale, veillez à soit l'enregistrer (moyennant information préalable), soit le faire confirmer par écrit. Cela procède également de votre obligation d'« accountability » qui vous impose de documenter vos traitements de données à caractère personnel.

### Exemple 31

L'ONG « Hope for climate » organise un repas de récolte de fonds avec vente aux enchères. De nombreuses entreprises achètent des places et y envoient certains de leurs employés. Le réceptionniste leur indique qu'un carton de remerciements leur sera adressé suite au dîner. Il leur demande ensuite s'ils acceptent d'être photographiés durant l'évènement et s'ils acceptent que l'ONG leur envoie ultérieurement sa newsletter ainsi que toute information sur les actions menées par elle.

Les personnes qui consentent à ces traitements de données le font verbalement, auprès du réceptionniste. Ce dernier marque « OK1 » à côté du nom des personnes ayant accepté d'être prises en photo, « OK2 » en cas d'acceptation pour la newsletter et les autres communications de marketing direct. Les noms de ceux qui acceptent les deux sont marqués d'un « OK3 ».

- ✓ Ces inscriptions ne sont pas de nature à garantir une preuve du consentement recueilli.
- ✓ Afin de se réserver la preuve de ce consentement, une solution peut être d'adresser aux participants du dîner une demande de confirmation de leur consentement à recevoir des communications de marketing direct en même temps que le carton de remerciement. En l'absence de confirmation de leur part, l'ONG Hope for climate devra s'abstenir de traiter leurs données à des fins de marketing direct.



200. Quelle que soit la manière dont vous recueillez le consentement, que ce soit par formulaire électronique ou papier par exemple, veillez à ce que la demande de consentement soit claire, concise et évidente. Si vous recueillez le consentement par voie verbale, assurez-vous que l'information communiquée à ce sujet a été clairement fournie et comprise par la personne concernée. Veillez à soit enregistrer soit faire confirmer la demande de consentement suivie de la manifestation de ce consentement. De manière à être en mesure de prouver que vous avez correctement fourni l'information et que le consentement vous a été donné.

### *b.5 Le consentement explicite*

201. Dans le cas où vos traitements de données à caractère personnel relatifs à vos finalités de marketing direct impliquent le traitement de données relevant de l'article 9 du RGPD, vous devez tenir compte de la condition supplémentaire de validité du consentement pour le traitement de ces données : il doit être « explicite ».

202. Vous devrez ainsi mettre en place un système permettant à la personne concernée de formuler expressément son consentement, par exemple au moyen d'une déclaration écrite de la personne, avec, le cas échéant, une signature de cette dernière. Vous pouvez également demander à la personne concernée de confirmer expressément son consentement par l'envoi d'un e-mail à cet effet ou en lui faisant remplir un formulaire en ligne. Ou encore, vous pourriez demander à la personne concernée de confirmer verbalement son consentement en l'enregistrant, pour autant qu'elle ait pu disposer d'informations suffisamment claires et complètes à ce sujet<sup>38</sup>.

### *c. Peut-on demander son consentement à un mineur ?*

203. Lorsque vos activités sont ou peuvent être destinées à un public composé, entre autres, d'enfants, vous devez être particulièrement attentifs à ce que ceux-ci puissent valablement consentir au traitement de leurs données pour des finalités de marketing direct. L'exigence du consentement, « éclairé » peu en effet faire défaut lorsqu'il s'agit de mineurs ne disposant pas de la pleine capacité de discernement.

204. Il vous appartient donc de vous assurer que les mineurs sont en mesure de comprendre ce à quoi ils s'engagent, notamment en expliquant dans un langage extrêmement simple mais complet quelles données vous souhaitez utiliser, pour quelles finalités et comment vous allez les traiter, tout en insistant sur le fait qu'ils peuvent à tout moment retirer leur accord.

---

<sup>38</sup> Pour plus d'information à ce sujet, veuillez consulter la WP259, p.21 à 23.



Dans le cadre des services de la société de l'information offerts directement à des enfants, des règles spécifiques s'appliquent. L'article 8 du RGPD établit un niveau de protection supplémentaire par rapport à la Directive 95/46/CE lorsque les données à caractère personnel de mineurs sont traitées dans le cadre de ce type de services.

Le considérant 38 du RGPD précise que cette protection spécifique s'applique notamment à l'utilisation des données à des fins de marketing ou de création de profils de personnalité ou d'utilisateur.

205. Lorsque vous êtes actifs dans le secteur des services de la société de l'information, et que votre public peut inclure des mineurs, vous devez observer les règles de l'article 8 du RGPD. Pour savoir si des services ne sont pas destinés à des enfants, il est tenu compte de leur éventuelle restriction, par le site, à des personnes âgées de 18 ans et plus, pour autant que cette affirmation ne soit pas contredite par d'autres éléments tels que le contenu du site Internet ou ses plans de commercialisation<sup>39</sup>.
206. Dans ce cadre de la fourniture de tels services, vous ne pouvez, **en Belgique**, traiter des données à caractère personnel de mineurs sur la base de leur consentement que pour autant que ceux-ci aient atteint l'âge de **13 ans**<sup>40</sup>. Le critère de l'âge du « consentement numérique » a été laissé à l'appréciation des législateurs nationaux par l'article 8.1 du RGPD. Certains Etats-membres ont retenu un âge plus élevé, comme la France qui a retenu l'âge de 16 ans. Soyez donc extrêmement attentifs à cette différence cruciale lorsque vous collectez des données d'utilisateurs mineurs dans le cadre d'activités transfrontières. Dans ce cas, la meilleure pratique est d'appliquer, par vous-même, l'âge le plus élevé pour l'obtention d'un consentement valide.
207. Lorsque les personnes concernées dont vous traitez des données n'ont pas atteint l'âge vous permettant de les considérer comme des adultes (parce qu'ils sont en mesure de faire preuve de discernement), vous êtes tenus de faire valider le consentement du mineur par l'adulte titulaire de la responsabilité parentale ou d'obtenir le consentement de ce dernier pour le traitement des données à caractère personnel de l'enfant concerné. Dans ce cas, vous devez raisonnablement vous efforcer de vérifier que le consentement validé ou donné est bien celui du titulaire de la responsabilité parentale, par tous les moyens technologiques disponibles.
208. L'EDPB précise que « si les utilisateurs indiquent qu'ils ont bien l'âge minimum du 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'é

<sup>39</sup> WP259 rév. 01, , point 7.1.2., p.29.

<sup>40</sup> Voir en ce sens l'article 7 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, M.B. 5 septembre 2018.



soit pas explicitement prévue par le RGPD, elle est sous-entendue de façon implicite, dès lors que si un enfant donne son consentement valable en son nom propre, le traitement des données sera illicite. »<sup>41</sup>.

209. Enfin, notez que la vérification de l'âge ne doit pas entraîner de traitements de données supplémentaires excessifs. Le mécanisme que vous utilisez pour vérifier l'âge dépend des risques liés au traitement. Si le ou les traitement(s) envisagé(s) comporte(nt) un faible risque, une méthode, non pas infaillible mais satisfaisante, peut consister à demander à la personne son année de naissance ou de remplir un formulaire stipulant qu'il a l'âge du consentement numérique<sup>42</sup>. Si vous êtes en situation de devoir recueillir le consentement du titulaire de la responsabilité parentale, la méthode à laquelle vous devez recourir dépend également des risques liés au traitement ainsi que des technologies disponibles.

#### *d. Quelle est la durée de validité du consentement ?*

210. Rien n'est prévu par le RGPD quant à la durée pendant laquelle un consentement obtenu reste valable. Tout dépend du contexte, notamment de la portée du consentement initial, de la nature de votre activité et des attentes légitimes et raisonnables de la personne ayant donné son consentement. Il s'agit avant tout d'une question de bon sens.

211. Il vous appartient dès lors de prévoir une durée de conservation de ces données, au regard du principe général de proportionnalité.

212. L'EDBP recommande également que « le consentement soit renouvelé à des intervalles appropriées, 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 droits. »<sup>43</sup> Cela est d'autant plus vivement conseillé si vous envisagez de communiquer avec d'anciens clients, ou avec des clients ayant recouru à un service unique (par exemple la location de béquilles) ou effectué un achat unique auprès de vous.

213. Faites du renouvellement du consentement un outil de communication privilégié. Lancez des campagnes de prévention en matière de protection des données par exemple, en expliquant de quelle manière votre organisation gère les données et remerciez, à cette occasion, vos clients, abonnés ou affiliés d'avoir consenti au traitement de leurs données pour vos finalités de marketing. Expliquez-leur en quoi cela est intéressant et rappelez-leur qu'ils peuvent à tout moment retirer leur consentement, en prévoyant à l'appui, une méthode simple de retrait.

---

<sup>41</sup> WP259 rév. 01, point 7.1.2., p.29.

<sup>42</sup> WP259 rév. 01, point 7.1.3., p.30.

<sup>43</sup> WP259 rév. 01, point 5.1, p.24.



## e. Conditions supplémentaires de validité du consentement

NEW

Le RGPD apporte des clarifications et des précisions complémentaires sur les conditions d'obtention et de démonstration d'un consentement car vous êtes tenu, en tant que responsable du traitement, d'avoir la preuve de l'obtention de celui-ci. Les personnes concernées ont en outre la possibilité de retirer ce consentement à tout moment.

### Article 7 du RGPD

1. Dans le cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de **démontrer que la personne concernée a donné son consentement** au traitement de données à caractère personnel.
2. (...)
3. La personne a le droit de **retirer son consentement à tout moment**. (...) La personne en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.
4. (...).

### e.1. Preuve du consentement

214. Le RGPD introduit l'obligation explicite pour le responsable du traitement d'être en mesure de démontrer que la personne concernée a donné son consentement<sup>44</sup>. Cela procède également de l'obligation plus générale d'accountability, imposée par le RGPD aux responsables du traitement.
215. Vous êtes libres de recourir à la méthode qui vous semble la plus appropriée pour vous conformer à cette exigence. Cette obligation n'a pas pour but d'entraîner pour vous une charge de travail excessive. Elle est avant tout faite pour vous permettre de facilement démontrer votre conformité en cas de plainte d'une personne concernée ou de contrôle de l'APD.
216. En outre, il ne vous est pas nécessaire de collecter davantage de données à caractère personnel que celles dont vous disposez déjà pour prouver ce consentement.
217. Vous pouvez 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 recueilli et des informations fournies par la personne concernée pour ce faire.
218. L'obligation d'être en mesure d'apporter la preuve du consentement demeure tant que l'activité de traitement de données a lieu. Une fois terminée, la preuve de ce consentement ne devrait pas être

---

<sup>44</sup> Article 7.1 et considérant 42 du RGPD.





conservée plus longtemps que nécessaire pour le respect de cette obligation légale ou pour la contestation, l'exercice ou la défense de droits en justice comme le prévoit l'article 17.3, b) et e) du RGPD.

### e.2. Retrait du consentement

219. Le RGPD permet aux personnes ayant donné leur consentement au traitement de leurs données de le retirer à tout moment.
220. Cela implique également que ce retrait puisse se faire gratuitement et sans préjudice, comme une diminution du niveau du service fourni jusqu'alors.

#### Exemple 32

Un festival de musique vend des tickets par le biais d'une plateforme en ligne. Pour chaque ticket vendu, il demande le consentement de l'acheteur pour utiliser ses coordonnées à des fins commerciales. Afin de confirmer – ou non- leur consentement quant à l'usage de leurs données 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. En procédant de la sorte, le responsable du traitement ne respecte pas l'article 7.3 du RGPD. Bien que gratuit, il est ici plus difficile de retirer son consentement que de le donner.

221. Bien que le RGPD accorde une place fondamentale au retrait du consentement, il ne prévoit pas la forme que celui-ci doit ou peut prendre. L'EDPB indique à cet égard que lorsque « le consentement a été donné 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. »<sup>45</sup> Obliger les personnes concernées à suivre un chemin compliqué balisé de liens vers des documents électroniques subséquents ou les obligeant à communiquer un mot de passe ne répond pas à cette exigence de simplicité équivalente. En cas de placement de cookies « tiers », renvoyer l'internaute vers les pages informatives du tiers en question et l'obliger à y chercher, pour chacun de ces tiers, le moyen d'y manifester son retrait/refus de consentement ne satisfait pas non plus à cette exigence.
222. Lorsqu'une personne retire son consentement, toutes les opérations de traitement de ses données basées sur le consentement de cette personne doivent être cessées. Cela n'entache pour autant pas d'illicéité les opérations effectuées sur la base du consentement, valablement donné, avant le retrait.
223. En outre, en cas de retrait du consentement, vous devez évaluer si la conservation des données qui servaient à la réalisation de vos finalités de marketing direct se justifie ou non, même en l'absence d'une

---

<sup>45</sup> WP259, p.25.



demande d'effacement de la personne concernée et ce, conformément à l'article 5.1, e) du RGPD qui vous impose de limiter la conservation des données à caractère personnel à la finalité poursuivie.

224. Si ces données sont nécessaires à la réalisation d'un traitement à d'autres fins, pour lesquelles vous disposez d'une base juridique valable, peut-être pourrez-vous les conserver ces données (voir en ce sens les considérants 166, 217 et 218 de la Recommandation). A contrario, si aucune autre base juridique ne justifie le traitement de ces données, celles-ci doivent être supprimées.

## F. Soyez transparents

### Article 12.1 du RGPD

« Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour une information destinée spécifiquement à un enfant.

Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique.

Lorsque la personne fait la demande, les informations peuvent être fournies oralement à condition que l'identité de la personne concernée soit démontrée par d'autres moyens. »

225. Afin de respecter les règles en matière de traitement de données pour des finalités de marketing direct, il est crucial que vous veilliez scrupuleusement au respect de votre obligation de transparence, telle qu'encadrée par l'article 12 du RGPD, qui porte tant sur les informations devant être fournies aux personnes concernées que sur l'exercice des droits conférés aux personnes concernées par les articles 15 à 22.

226. En ce qui concerne les articles 13 et 14 du RGPD mentionnés à plusieurs reprises dans la Recommandation (voir en ce sens les considérants 64, 66, 67, 78, 101, 134, 158 et 176), soyez très attentifs au fait que le premier s'adresse aux responsables du traitement qui collectent directement les données auprès des personnes concernées et le second, aux responsables du traitement qui collectent des données à caractère personnel de manière indirecte. Selon que vous soyez dans l'une ou l'autre de ces situations, reprenez qu'au plus vous fournissez d'informations, claires et compréhensibles, au mieux cela rencontre l'exigence de transparence de l'article 12 du RGPD.

227. Soyez attentifs aux critères de temporalité qui diffèrent de l'un à l'autre de ces articles. Lorsque vous collectez les données directement auprès de la personne concernée, vous devez lui fournir, notamment, les éléments d'information repris à l'article 13 du RGPD **au moment où les données en question sont obtenues**. Lorsque les données ne sont pas collectées directement auprès de la personnes concernée, l'article 14 vous impose de fournir les informations qu'il stipule **dans un délai raisonnable de maximum**



**un mois à compter de la réception des données à caractère personnel et à la première communication avec la personne concernée si les données sont traitées aux fins de communiquer avec elle.**

228. Utilisez toujours des termes clairs et simples, accessibles à vos interlocuteurs.

#### **Considérant 58 du RGPD**

« Le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre et formulée dans des termes clairs et simples et, en outre, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels. »

229. Les politiques de protection des données, connues du public sous différentes appellations, se révèlent être souvent longues et fastidieuses à décrypter, placées sous une rubrique en fin de page, rédigées de manière linéaire et peu intelligible.

230. L'accessibilité de l'information ne se limite pas aux termes utilisés mais s'étend également à la manière dont vous la communiquez et à l'endroit où l'information est proposée. Si aucune forme de communication ne vous est imposée, vous êtes tenus d'opter pour celle qui sera la plus efficace, voire de recourir à plusieurs formes de communication pour diffuser l'information : un texte, un message audio, une vidéo d'accompagnement.

231. Par exemple, si vous disposez d'un site Internet, votre politique de vie privée devrait, pour être la plus accessible possible, apparaître immédiatement à l'écran, en invitant les visiteurs de votre site à en prendre connaissance. Les politiques de vie privée placées en bas de page, en petits caractères, sans que l'attention ne soit attirée dessus ne répondent pas aux exigences de l'article 12 du RGPD. Veillez aussi à fournir les informations primordiales à la compréhension du/des traitements et des données collectées en premier lieu, en séparant clairement ceux qui sont de votre chef et ceux qui sont de celui de destinataires éventuels des données.

232. N'oubliez pas non plus que vous ne pouvez pas communiquer les informations requises aux articles 13 et 14 du RGPD en les intégrant dans un document qui a un autre objet, comme vos conditions générales par exemple. A l'instar des politiques en matière d'utilisation des cookies, vous devez présenter ces documents séparément.

233. Aucune forme ne vous est imposée en ce qui concerne le contenu de l'information. L'article 12.7 du RGPD précise notamment que les informations à communiquer peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu.



234. Les informations à fournir conformément aux articles 13 et 14 du RGPD doivent notamment porter sur les droits des personnes concernées. Il est de votre responsabilité de garantir et faciliter leur exercice (voir l'article 12.2 du RGPD) en expliquant aux personnes concernées de manière visible et compréhensible les droits dont elles disposent. Il faut éviter qu'elles doivent multiplier les démarches pour pouvoir exercer leurs droits.



Outre le droit d'opposition (article 21 du RGPD) ou le droit de retirer son consentement (article 7.3 du RGPD) lorsque ceux-ci sont applicables, ainsi que celui de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (article 22 du RGPD), n'oubliez pas de renseigner et de garantir aux personnes concernées leur **droit d'accès** (conformément aux conditions de l'article 15 du RGPD), leur **droit de rectification** (conformément à l'article 16 du RGPD), lorsqu'il s'applique, leur **droit à l'effacement** (conformément aux conditions de l'article 17 du RGPD), leur **droit à la limitation** des traitements (conformément à l'article 18 du RGPD), de **notifier la rectification ou l'effacement** des données aux destinataires de données (voir l'article 19 du RGPD) et leur **droit à la portabilité** des données (voir l'article 20 du RGPD), le cas échéant.

235. En ce qui concerne le droit à l'effacement, une personne peut en faire usage lorsque, par exemple, elle retire le consentement qu'elle avait donné. Soyez attentifs au fait que, en dehors des cas de figure où vous seriez tenus légalement de conserver ces données, lorsqu'une personne retire son consentement, il va de soi que vous ne disposez plus d'une base juridique pour traiter ses données. Il vous appartient donc, avant même que cette personne n'ait fait usage de son droit à l'effacement, de procéder vous-même à la suppression de ses données à caractère personnel. Vous pouvez donc prévoir une notification automatique informant les personnes procédant au retrait de leur consentement que leurs données seront supprimées de vos bases de données. Il en va de même dans le cas où les personnes s'opposent au traitement de leurs données fondé sur vos intérêts légitimes. L'article 17.1, d) du RGPD prévoyant en effet qu'une personne concernée peut demander l'effacement lorsqu'un traitement est illicite. Or, en cas d'opposition au traitement de leurs données pour des finalités de marketing et hors du cas où vous seriez tenus de conserver ces données pour garantir une autre finalité (avec une base juridique valable), leur traitement en devient illicite.



Même si vous estimez ne pas devoir faire suite à l'un des droits exercés par une personne concernée, vous devez toujours la tenir informée des mesures prises à la suite de sa demande, au plus tard dans un délai d'un mois à compter de la réception de sa demande, prolongeable de deux mois si la demande est complexe ou si vous avez à traiter de trop nombreuses demandes pour la capacité de votre organisation. Tenir informée la personne des mesures prises implique également de la tenir informée si le délai de traitement de sa demande se voit prolongé.



## IV. Conclusion

236. Au regard du nombre et de la variété des acteurs concernés, du nombre et des catégories de données traitées, ainsi des types de traitements opérés, parfois très intrusifs, dans le cadre des finalités de marketing direct, les responsables du traitement actifs dans ce domaine font l'objet d'une des priorités des autorités de contrôle, tant du point de vue de leur accompagnement que de celui de leur contrôle. C'est au regard du nombre d'acteurs, de personnes concernées et de données traitées dans ce secteur que le marketing direct constitue l'une des priorités d'action du plan stratégique 2020-2025 de l'Autorité de protection des données.
237. Le RGPD apporte de nombreuses clarifications pour les opérateurs recourant au marketing direct. Ce Règlement introduit également un nouveau paradigme en imposant que la protection des données à caractère personnel soit prise en compte par les responsables de traitement dès la conception de leurs traitements de données à caractère personnel et à tous les stades de ceux-ci. Il impose notamment à cet égard aux responsables du traitement d'assurer aux personnes concernées de pouvoir contrôler leurs données. Les personnes sont concernées par et associées, comme acteur clé et incontournable, à la gestion de leurs données à caractère personnel.
238. Vous devrez ainsi déterminer précisément vos finalités de traitement, vous assurer de disposer d'une base juridique valable pour la poursuite de celles-ci, être en mesure de vous conformer à et de répondre à vos obligations de transparence en étant parfaitement clairs et honnêtes envers les personnes concernées quant à ce que vous faites avec leurs données à caractère personnel et en assurant et respectant l'exercice de leurs droits. Vous devez également mettre en place les mesures de sécurité adéquates eu égard aux risques que peuvent présenter vos traitements pour les données à caractère personnel dont vous êtes en charge. Vous devez également pouvoir à tout moment démontrer ce que vous avez mis en place pour être en conformité avec le RGPD, conformément au principe d'accountability.
239. Votre conformité au RGPD ne doit pas être dictée par le seul risque de sanction mais, avant tout, par le souci de nouer par le respect des règles de protection des données une véritable relation de confiance avec les personnes concernées qui vous sont essentielles pour la poursuite de votre activité. Le RGPD doit devenir un langage commun à tous les acteurs auxquels il s'adresse, et dont il s'agit de maîtriser les codes et le vocabulaire afin que les différentes parties impliquées parviennent à se comprendre et à assurer le respect de ce qu'il vise à préserver : la protection des données à caractère personnel et des personnes auxquelles elles sont attachées.
240. Enfin, agir conformément au RGPD n'est pas uniquement une obligation au regard des données à caractère personnel que vous traitez. Il s'agit également d'une éthique de comportement sur le marché,



tant envers les personnes concernées qu'entre partenaires. Afin d'assurer l'uniformité et la cohérence des pratiques de marketing direct entre responsables de traitement actifs en ce domaine et communiquer celles-ci de façon claire et transparente aux personnes concernées, l'Autorité de protection des données recommande la mise en place de Codes de conduites des secteurs concernés en la matière, tel que prévus par l'article 41 du RGPD.

