#FOCUSGDPR - 6/2/2020

6e colloque du think tank www.cap-numerique.org

#FocusGDPR – 6/2/2020
Séance plénière

- Oratrices:
  - Alexandra JASPAR : Directrice du centre de connaissances
    - *Alexandra Jaspar est diplomée de l'ULB et de Northwestern University (Chicago). Elle est experte en protection des données à caractère personnel depuis 19 ans. Elle était avocate au cabinet d'avocats Linklaters et ensuite directrice du département Compliance (anti-blanchiment d'argent et vie privée) chez Bpost . Elle est également "Lecturer" à la Solvay Business School (Programme in EU data protection).*
  - Pavlina PENEVA : *Responsable Communication PME à l'Autorité de la protection des données.*
    - *Madame PENEVA est diplômée de l'ULB avec un Master spécialisé en droit européen. Au sein de l'APD elle occupe actuellement le poste de responsable communication pour les PME. Avant Mme PENEVA a travaillé au sein de la Commission européenne, à la direction générale de la recherche et de l'innovation, pendant 6 ans en tant qu'experte juriste en protection des données.*
  - Juline DESCHUYTENEER : *Conseillère juridique à l'Autorité de protection des données*
    - *Après avoir entamé son stage d'avocate au barreau de Bruxelles, Juline Deschuyteneer a rejoint l'Autorité de protection des données où elle exerce en tant que conseiller juridique en protection des données à caractère personnel depuis 6 ans. Elle a obtenu son diplôme en Droit public à l'Université Libre de Bruxelles et a complété sa formation au sein de cette Université en Droit international des Affaires.*
- Contenu :
  1. Compétences, priorités et bilan de l'APD (des 20 premiers mois du RGPD) –
  2. Quels sont les problèmes les plus fréquemment rencontrés dans les PME ? Quelques exemples concrets.
  3. Rappel des acteurs principaux et des obligations majeures (respect des principes de licéité, de transparence et de proportionnalité; registre des activités de traitement) ;
  4. Présentation de la nouvelle recommandation de l'APD relative au marketing direct;
  5. Les actions de l'APD spécifiquement pour les PME.

http://www.cap-numerique.org

#FocusGDPR – 6/2/2020 Ateliers

Atelier « responsable de traitement de données personnelles »

- **Orateurs :**
  - Damien JACOB :
    - *Chargé de cours et de formation en Belgique (EPHEC, HEPL, HEPHC, HEC-LIEGE), au Grand-Duché et en France. Il est également conseiller indépendant (stratégies sur le web, e-Business, e-Commerce).*
    - *Co-animateur pour l'ASBL CAP NUMERIQUE*
  - JULINE DESCHUYTENEER
    - *Conseillère juridique à l'Autorité de protection des données*
  - Pavlina PENEVA
    - *Responsable Communication PME à l'Autorité de la protection des données*

- **Contenu:**
  - **Rappel des obligations incombant au responsable de traitement selon les RGPD.**
    - **Des recommandations seront apportées pour la rédaction de la charte vie privée, ainsi pour la mise en conformité des traitements de données à des fins de marketing (newsletters, tracking publicitaire,…).**
    - **Echange questions / réponses.**
  - **La nouvelle recommandation de l'APD relative au marketing direct**

Atelier « sous-traitant web »

- **Oratrice :**
  - Alexandra JASPAR :
    - Directrice du centre de connaissances

- **Rappel des obligations incombant au sous-traitant selon le RGPD.**
- **Des recommandations seront également apportées pour bien clarifier la relation contractuelle avec le donneur d'ordre (le responsable du traitement) pour la conception des sites (cookies, opt-in,…) et pour correctement assurer le rôle du sous-traitant.**
- **Echange questions / réponses.**

Responsables du traitement et RGPD

Direct Marketing et RGPD

GBA Gegevensbeschermingsautoriteit

APD Autorité de protection des données

DSB Datenschutzbehörde

DPA Data Protection Authority

Juline Deschuyteneer

06 février 2020

Marketing Direct :de quoi parlons-nous ?

- **Cette notion n'est pas définie par le RGPD**
- **Il n'existe pas, à ce jour, de définition ou de position harmonisée au niveau légal européen**
- **Défini par l'APD dans sa Recommandation de 2020 comme :**

> 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.

Marketing direct : de quoi parlons-nous ? Notions clés

- **Tout type de communication sollicitée et non sollicitée, sous quelque forme que ce soit**
- **Adressée directement à une ou plusieurs personnes dans un cadre privé ou professionnel**
- **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**
- **Emanant d'une organisation ou d'une personne**
- **Dans un cadre commercial ou non**

Tout type de communication sollicitée et non sollicitée, sous quelque forme que ce soit

Le marketing direct regroupe l'ensemble des actions de communication personnalisées ou individualisées ayant pour vocation de susciter une réponse plus ou moins immédiate de la part du destinataire (commande, demande de devis, appel sur n° vert, prise de RDV, etc.).

- **Les communications peuvent être électroniques ou non, photo, vidéos, textes, audio,...**
- **Originellement, les communications de marketing direct se faisaient par téléphone, fax, courrier postal**
- **Développement de nouvelles technologies, d'Internet, du commerce en ligne et des réseaux sociaux: SMS, MMS, e-mail, pop-up, bannières, chatbox**
- **Recours aux méthodes de targeting, profiling**

Désormais, RTL adapte sa pub à... vous !

Sud Presse - 03 Feb. 2020
Page 19

* Sud Presse : La Meuse - Basse Meuse, La Nouvelle Gazette - Centre, La Nouvelle Gazette - Charleroi, La Meuse - Huy Waremme, La Meuse - Liège, La Meuse - Luxembourg, La Province, La Meuse - Namur, La Nouvelle Gazette - Entre Sambre et Meuse, La Meuse - Verviers, La Capitale, Nord Eclair - Mouscron, Nord Eclair - Tournai

Ça s'appelle l'« addressable TV » et c'est, pour le petit écran, l'équivalent de ce que les internautes connaissent depuis un petit temps avec la pub ciblée. En d'autres termes, de la publicité adaptée à vos centres d'intérêt et à votre mode de vie. Des algorithmes rendent le procédé possible sur les réseaux sociaux et autres sites internet.

Désormais, dès le mois de février, sans opérer aucune manipulation, installé dans votre canapé, vous aurez également droit à des « réclames » personnalisées si vous êtes branché sur l'une des chaînes de RTL (TVI, Plug et Club) et à condition d'avoir Proximus TV comme opérateur.

correspondre à la demande

Car ce sont les boxes Proximus qui détiennent les données pouvant dresser le profil de chaque téléspectateur. Selon le groupe RTL et sa régie publicitaire IP, « cette nouvelle manière de faire de la publicité correspond à la demande des consommateurs : une étude a prouvé que 66 % de ceux-ci souhaitent que les publicités correspondent mieux à leurs intérêts et à leur mode de vie. ».

Concrètement, si vous êtes, par exemple, de jeunes parents, attendez-vous à voir, dans un futur proche, les écrans publicitaires de RTL remplis de réclames pour des couches-culottes et autres petits pots pour bébés. Alors que votre voisine de 80 ans, vivant seule avec son chien, sera, elle, davantage abreuvée de spots de firmes pharmaceutiques voire de croquettes pour animaux de compagnie.

Le profilage d'audience s'attaque aux banques

L'Echo - 04 Feb. 2020

Hello Bank! est la banque qui attire le plublic le plus jeune. ©AFP

"Dites-moi ce que vous 'likez', je vous dirai quelle est votre banque." Telle est la promesse d'une start-up hennuyère qui a passé des centaines de milliers de profils au peigne fin.

La quantité faramineuse de données disponibles sur les réseaux sociaux constitue un trésor pour qui sait les analyser. Des start-ups se sont ainsi développées ces dernières années en travaillant sur le profilage d'audience. C'est le cas de SOPRISM, une entreprise belge basée à La Louvière.

Avec toutes les informations brassées, nous permettons aux dirigeants de prendre des décisions fondées sur les données et non sur l'intuition.

Tout type de communication sollicitée et non sollicitée, sous quelque forme que ce soit

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 ».

- ✓ 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.

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

➢ ~~Études de marché, sondages, enquêtes de satisfaction~~

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.

➢ ~~Activités purement domestiques~~

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.

Par qui ? Vers Qui ?

Organisations commerciales, ONG, politiques, personnes physiques

Personne(s) physique(s)
Dans le cadre de sa vie privée ou professionnelle

Qui implique un traitement de données à caractère personnel

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.

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.

https://www.youtube.com/watch?v=PrwQ-guwvfs

Conformité au RGPD dans le cadre du marketing direct : une réalité

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.

Conformité au RGPD dans le cadre du marketing direct : une obligation

- **Comme pour tout traitement de données, les traitements de données réalisés dans le cadre des communications de marketing direct doivent être conformes aux règles du RGPD**

- **Les responsables du traitements sont tenus de s'y conformer sous peine de sanctions mais aussi et avant tout afin de respecter les droits des personnes concernées par ces traitements**

Conformité au RGPD dans le cadre du marketing direct : une opportunité

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, abonnées 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.

Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente Article 5.1, a) du RGPD

Vérifiez que vous disposez d'une base juridique

. 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[30]. Vous ne pouvez traiter de données sans base juridique, vous devez donc vos assurez d'en disposer d'une avant le lancement de votre traitement.

. 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.

. 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.

Attention !
Certaines lois sont d'application dans des contextes spécifiques et prévoient des bases juridiques précises pour certains types de traitements de données à caractère personnel (voir e-Privacy)

Base juridique du traitement

- **Hormis les lois spécifiques, aucune base juridique n'est d'application automatique.**
- **Il n'existe pas de hiérarchie entre les bases juridiques prévues à l'article 6 du RGPD mais vous devez en avoir une pour pouvoir traiter des données à caractère personnel => Pas de base juridique, pas de traitement et elle doit exister avant le traitement**
- **On ne peut pas en changer en cours de traitement (sauf lors du passage vers le RGPD pour les traitements fondés sur le consentement)**
- **Si une base juridique est mal déterminée ou que ses conditions ne sont pas ou plus remplies ou qu'elle cesse d'exister (par exemple : retrait du consentement) le traitement doit cesser**

Base juridique : consentement et intérêt légitime

- **Rappel : aucune hiérarchie entre les bases de l'article 6 du RGPD**
- **Certaines se prêtent plus facilement aux réalités des traitements de données à caractère personnel réalisés dans le cadre du marketing direct**
- **La recommandation APD examine particulièrement le consentement (articles 6.1, a) et 7 du RGPD) et les intérêts légitimes (article 6.1, f) du RGPD)**

Intérêt légitime

Considérant 47 du RGPD

- Ne signifie pas que la base juridique des intérêts légitimes soit la seule opérante en matière de marketing direct
- Ne signifie pas que tous les traitements réalisés dans le cadre du marketing direct soient légitimes au regard du RGPD

Évaluez votre intérêt

- Considérant 47 = **possibilité**, pas automatique
- Les **traitements sont-ils nécessaires** à la réalisation des finalités poursuivies ? = d'autres traitements moins intrusifs ne permettent pas d'aboutir au même résultat ?
- Mise en balance = **attentes raisonnable** de votre public cible + catégories de données (! Données sensibles)

Droit d'opposition

- Article 21.2 du RGPD :spécifiquement dédié aux traitements réalisés en cas de marketing direct et/ou profilage et diffère de l'article 21.1 du RGPD =>**automatique**
- **À tout moment et sans frais**
- Mis en avant de manière **évidente et claire**
- **Exercice facilité** (aucune démarche supplémentaire)
- **Effectivité** : lorsqu'exercé les données ne sont plus traitées au fins de marketing direct

Intérêt légitime

LE SAVIEZ-VOUS ?

La CJUE, dans son arrêt C-708/18 du 11 décembre 2019 « *TK c. Asociaţia 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)

Pour l'arrêt intégral :
http://curia.europa.eu/juris/document/document.jsf?text=&docid=221465&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=7256287

Intérêt légitime

Considérant 47 du RGPD

- Ne signifie pas que la base juridique des intérêts légitimes soit la seule opérante en matière de marketing direct
- Ne signifie pas que tous les traitements réalisés dans le cadre du marketing direct soient légitimes au regard du RGPD

Évaluez votre intérêt

- Considérant 47 = **possibilité**, pas automatique
- Les **traitements sont-ils nécessaires** à la réalisation des finalités poursuivies ? = d'autres traitements moins intrusifs ne permettent pas d'aboutir au même résultat ?
- Mise en balance = **attentes raisonnable** de votre public cible + catégories de données (! Données sensibles)

Droit d'opposition

- Article 21.2 du RGPD :spécifiquement dédié aux traitements réalisés en cas de marketing direct et/ou profilage et diffère de l'article 21.1 du RGPD =>**automatique**
- **À tout moment et sans frais**
- Mis en avant de manière **évidente et claire**
- **Exercice facilité** (aucune démarche supplémentaire)
- **Effectivité** : lorsqu'exercé les données ne sont plus traitées au fins de marketing direct

Droit d'opposition

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.

Intérêt légitime

Considérant 47 du RGPD

- Ne signifie pas que la base juridique des intérêts légitimes soit la seule opérante en matière de marketing direct
- Ne signifie pas que tous les traitements réalisés dans le cadre du marketing direct soient légitimes au regard du RGPD

Évaluez votre intérêt

- Considérant 47 = **possibilité**, pas automatique
- Les **traitements sont-ils nécessaires** à la réalisation des finalités poursuivies ? = d'autres traitements moins intrusifs ne permettent pas d'aboutir au même résultat ?
- Mise en balance = **attentes raisonnable** de votre public cible + catégories de données (! Données sensibles)

Droit d'opposition

- Article 21.2 du RGPD :spécifiquement dédié aux traitements réalisés en cas de marketing direct et/ou profilage et diffère de l'article 21.1 du RGPD =>**automatique**
- **À tout moment et sans frais**
- Mis en avant de manière **évidente et claire**
- **Exercice facilité** (aucune démarche supplémentaire)
- **Effectivité** : lorsqu'exercé les données ne sont plus traitées au fins de marketing direct

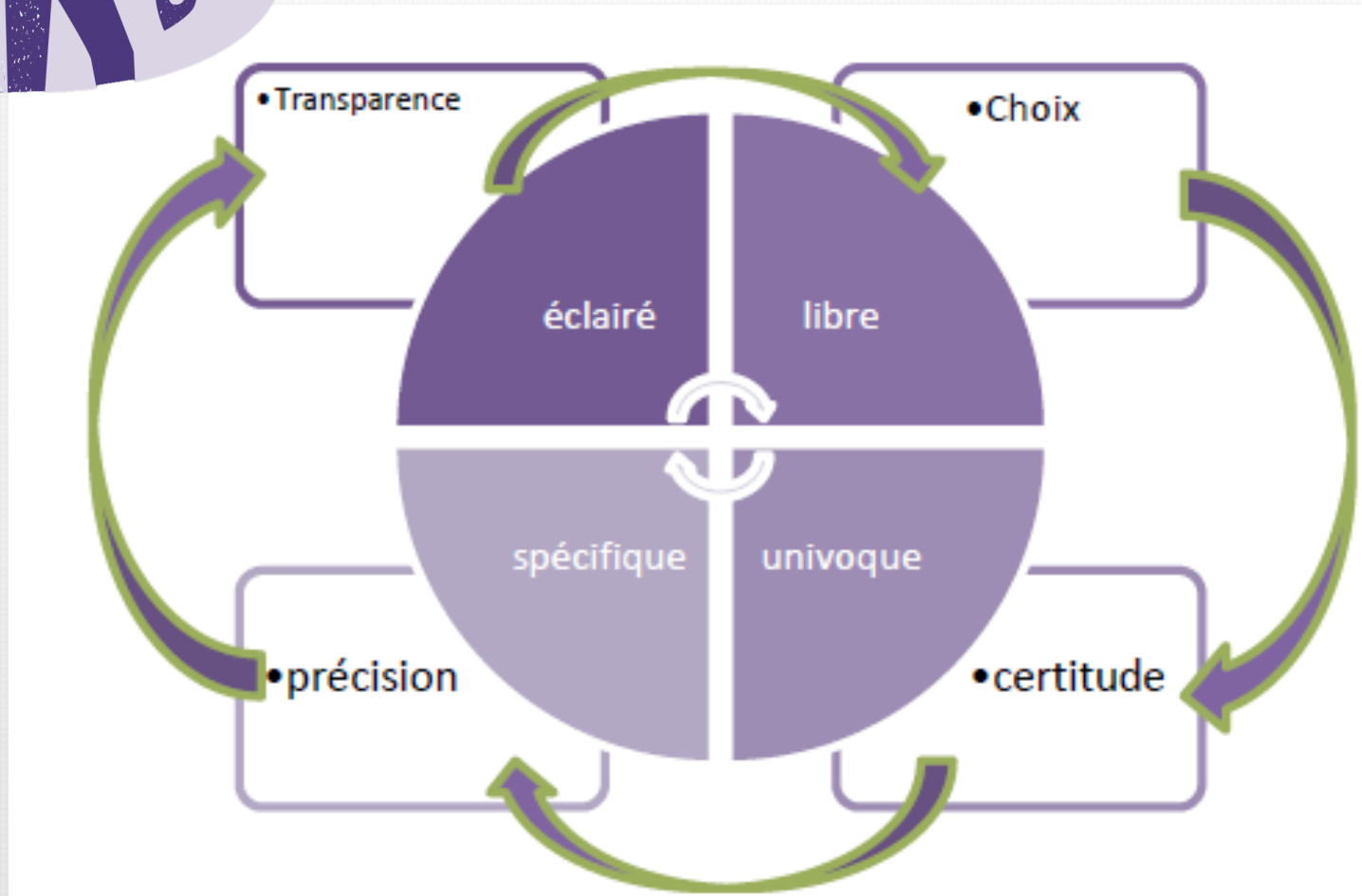
Effectivité du droit d'opposition

Article 21.3 du RGPD

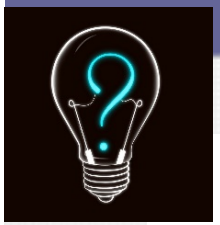
« lorsque la personne concernée s'oppose au traitement à des fins de prospection, les données à caractère personnel ne sont plus traitées à ces fins. »

. 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 consentement



Le consentement éclairé



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 concerne).

. 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[36] :

- ✓ 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

Le consentement libre

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.

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.gegevensbeschermingsautoriteit.be/nieuws/GBA-sanctioneert-een-handelaar-voor-het-gebruik-van-de-eid-om-klantenkaart-aan-te-maken

Le consentement spécifique

. 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.

. 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.

Éviter les détournements de finalités

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.

Le consentement univoque

OPT-OUT = OUT

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 1er 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.

[...]

Le consentement univoque : position CJUE

[...]

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

Consentement

- Dans les cas où le traitement porte sur des données à caractère personnel relevant de l'article 9 (données sensibles), le consentement donné doit être explicite
- Dans le cadre de services de la société d'information, un mineur ne peut pas consentir valablement au traitement de ses données s'il n'a pas atteint l'âge de 13 ans (si pas, il faut le consentement du/des titulaire(s) de la responsabilité parentale
- Durée du consentement : Pensez à renouveler le consentement obtenu
- Gardez la preuve du consentement

Retrait du consentement

- **Le consentement doit pouvoir être retiré par la personne concernée à tout moment et sans frais ou démarche supplémentaire**

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.

- **Aucune forme n'est précisée par le RGPD**
- **En principe les données à caractère personnel ne sont plus traitées (conservation à d'autres fins ?)**

Maîtrisez vos traitements conformément au RGPD : finalités du traitement

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.

Essentiel à l'examen de proportionnalité des données traitées

Exemples :

- ✓ 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 évènements (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.

Finalités du traitement

- **Une donnée traitée pour une finalité initiale ne peut en principe pas être traitée ultérieurement, sauf si la personne a donné son consentement pour cette nouvelle finalité ou si cette finalité ultérieure est compatible à la finalité initiale**
- **Le responsable du traitement doit examiner si l'une ou l'autre de ces conditions est remplie, qu'il réutilise des données qu'il a collecté lui-même initialement ou qu'il réutilise des données collectées par des tiers (autres organisations commerciales, data broker, administrations publiques, réseau sociaux,…)**

Finalité initiale et finalité ultérieure

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).

N'oubliez pas d'**informer les personnes concernées** ou de veiller à ce qu'elles aient été informées. **Vous devez vous renseigner** auprès des responsables de traitement initiaux si vous collecter les données indirectement

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.

Maîtrisez vos traitements conformément au RGPD : opérations de traitement

Opérations de traitements à distinguer des finalités du traitement

Profilage et/ou décision purement automatisée

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[21] ou d'informations et traces laissées par celles-ci au cours de leur navigation sur des pages de site Internet.

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.

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 aboutir à une prise de décision exclusivement automatisée, sans intervention humaine. Les deux premières facettes sont soumises à l'entièreté du 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.

Maîtrisez vos traitements conformément au RGPD : gestion des données

Minimisation des données

Mises à jour des données et gestion des droits

~~Multiplication des copies~~ de données

Données sensibles, personnes vulnérables

Durée de conservation

Privacy by design et by default

Maîtrisez vos traitements conformément au RGPD : gestion des données

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. A 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.

Maîtrisez vos traitements conformément au RGPD : gestion des données

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 donnée 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-

En Conclusion

. 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.

. 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.

. 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.

Cap Numérique

- Inciter la société et les entreprises wallonnes à tirer **profit de tous les avantages offerts par les outils numériques** de la manière la plus adéquate possible ;
- Veiller au **développement** et à la **propagation** des enseignements dans le domaine du numérique ;
- Elargir et **entretenir les liens entre les entreprises et les diplômés** des sections socio-économiques de l'enseignement supérieur abordant le domaine du numérique.

Prochains colloques :

www.cap-numerique.org

Cap Numérique

CENTRE IFAPME Namur / Brabant wallon

feweb

APD
Autorité de protection des données

#FOCUSGDPR

6e colloque du think tank www.cap-numerique.org