La Data Management Platform (DMP) & le respect de la vie privée

qualifio

Table des matières

Introduction

Qu'est-ce qu'une **Data Management Platform (DMP)** ? Pourquoi les entreprises utilisent-elles cet outil ? Est-il compatible avec les exigences du nouveau **Règlement Général sur la Protection des Données à caractère personnel (RGPD)** et avec celles de la **Proposition de Règlement *e-Privacy*** ? Tentative d'éclairage…

Data Management Platform

Une *Data Management Platform* (DMP) est un outil qui permet à une entreprise de collecter, centraliser, organiser et utiliser une masse importante de données concernant ses clients et prospects.

L'objectif premier d'une DMP est de **créer des segments d'audience** (ex. hommes sportifs entre 25 et 40 ans habitant la région de Lille) sur base d'informations provenant de différentes sources (navigation sur le site, achats, participation à un concours ou un sondage...). Ces différentes sources permettent d'enrichir les données qui sont déjà en possession de l'entreprise. La DMP facilite donc, d'une part, la réalisation de campagnes marketing ciblées et, d'autre part, la prise de décisions stratégiques quant à l'achat d'espaces publicitaires sur les canaux de distribution, mais aussi l'affichage de contenus personnalisés.

Les données collectées par la DMP proviennent de sources différentes, comme le montre le schéma ci-contre.

LES DONNÉES « FIRST PARTY »

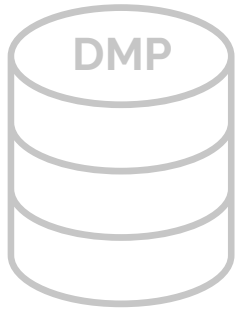
sont des données appartenant à l'entreprise. Ces données sont des données que l'entreprise a collectées elle-même (via son CRM - *CRM onboarding* ou ses cookies).

LES DONNÉES « SECOND PARTY »

sont des données fournies par les partenaires de l'entreprise.

LES DONNÉES « THIRD PARTY »

sont des données collectées via des sources tierces (sociétés qui possèdent des données provenant la plupart du temps de cookies ou autres technologies de traçage et qui affinent les segmentations en place).



Les DMP et les données personnelles

De manière générale, une DMP n'a pas pour vocation de traiter des données à caractère personnel. En effet, la plupart du temps, les données intégrées dans celle-ci et provenant des différentes sources sont, soit anonymisées, soit pseudonymisées. Elles ne permettent donc « *pas de rendre une personne directement identifiable* ».

Ces données ainsi « masquées » sont ensuite synchronisées entre les différentes sources pour que l'ensemble des informations (*first-party, second-party* et *third-party*) soient mises en commun dans la DMP, en utilisant un **identifiant unique** ne permettant plus d'identifier la personne à qui appartient ces informations (« *identity resolution* »).

Cette synchronisation des différentes sources dans la DMP est rendue possible via l'usage de cookies et/ou autres traceurs d'information (des pixels, par exemple).

Quelques DMP de références sur le marché

salesforce DMP

ORACLE bluekai

CXENSE

Adobe Audience Manager

PERMUTIVE

LOTAME™

mediarithmics

weborama

Les DMP face aux réglementations RGPD et e-Privacy [1]

Le RGPD s'applique-t-il donc aux DMP ?

C'est notamment le caractère personnel ou non des données (et donc la possibilité ou non d'identifier la personne directement ou indirectement) qui déterminera si le RGPD s'applique. Dans le cas des DMP, la question mérite d'être posée dès lors que sont mises en place différentes techniques permettant de ne plus rendre identifiables les personnes physiques et que c'est via l'utilisation de cookies que sont « assemblées » les données provenant des différentes sources.

La seule évocation des cookies dans le RGPD se trouve au considérant 30 qui expose que « *les personnes physiques peuvent se voir associer, par les appareils, applications, outils et protocoles qu'elles utilisent, des identifiants en ligne tels que des adresses IP et des témoins de connexion (« cookies ») ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence* ».

> **« Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes. »**

La réponse n'est donc pas si simple… En pratique, elle dépendra des mesures de protection du caractère privé des données, des mesures de sécurité mises en place et *in fine* des rattachements possibles qui pourront être effectués entre ces données et une personne physique.

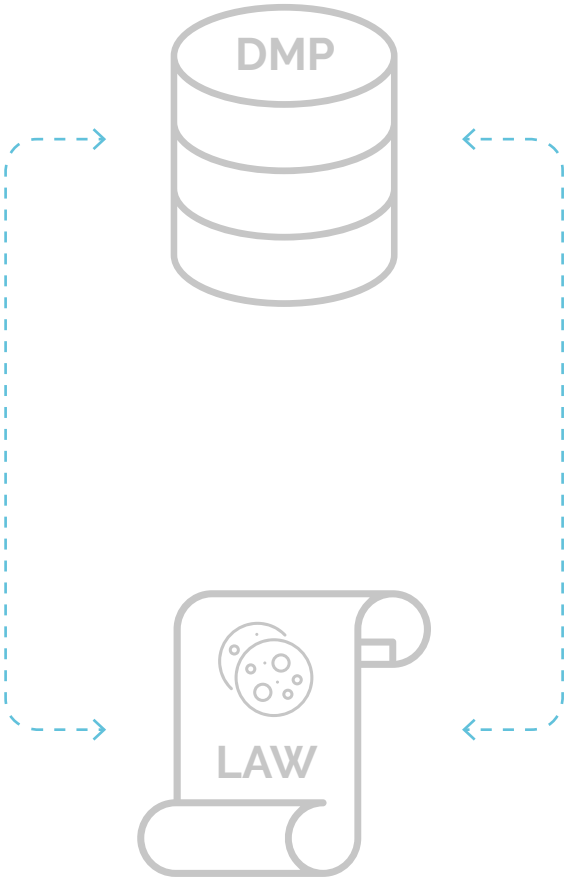
Si un rattachement, via une combinaison d'informations, est possible — rappelons que les adresses IP sont considérées comme des données à caractère personnel[2] — et qu'une personne physique peut être identifiable sur base des informations reprises dans la DMP, la réponse à cette question se devra d'être positive.

Et le projet de Règlement e-Privacy ?

L'enrichissement de la DMP se faisant également par des informations provenant de cookies ou d'autres technologies de traçage provenant notamment des partenaires tiers, il convient d'appliquer la loi du 13 juin 2005 relative aux communications électroniques. Cette loi transpose la Directive *e-Privacy* qui fera bientôt l'objet d'une révision via l'adoption d'un Règlement.

Dès lors qu'il est établi que le RGPD — à tout le moins pour une partie des DMP — et la Directive *e-Privacy* s'appliquent à ces outils, il convient de se pencher sur la question des bases légales de traitement qui pourront justifier le traitement de ces données à caractère personnel.

Sur base du RGPD, pour qu'un traitement de données à caractère personnel soit licite, il faut que le traitement soit fondé sur une des six bases légales reprises à l'article 6.



Fondement du traitement licite

Puisque chaque type de données intégré dans une DMP provient de sources différentes, il convient de distinguer la base légale qui, selon nous, pourrait permettre le traitement de ces données personnelles.

Concernant les données « first party »

Ces données sont collectées directement via l'entreprise dans le cadre de son activité.

Une entreprise pourra donc fonder, principalement, au regard du RGPD, le traitement de ces données personnelles sur une des trois bases légales de traitement[3] : le consentement de la personne concernée, la nécessité au regard des intérêts légitimes poursuivis par l'entreprise ou bien encore la nécessité en vue de l'exécution d'un contrat. Une de ces trois bases légales pourrait servir de fondement licite au traitement de données à caractère personnel visant l'incorporation de celles-ci dans une DMP.

Concernant le projet de Réglementation *e-Privacy*, deux fondements pourraient justifier le traitement par l'entreprise des données récoltées, notamment, via les cookies de l'entreprise : le consentement de l'utilisateur final ou, sur base de l'article 8 du projet de Règlement, si cela est « *nécessaire pour fournir un service* [...] *demandé par l'utilisateur final* ».

La justification relative à la base légale invoquée pour fonder le traitement de ces données *first party* incombera évidemment au responsable du traitement qui se devra de pouvoir démontrer soit le consentement, soit la nécessité par rapport à l'exécution d'un contrat ou à la fourniture d'un service, soit enfin, la proportionnalité entre ses intérêts légitimes et le respect de la vie privée des personnes concernées.

LA PRATIQUE DU CRM ONBOARDING

Le ***CRM Onboarding*** consiste à créer un lien entre les informations détenues par une entreprise dans son CRM et des informations contenues dans une DMP. Cette liaison est possible via l'association d'informations contenues dans le CRM à un identifiant en utilisant un cookie. Ce cookie permettant de faire le lien avec les informations détenues dans le CRM et de « hacher » ou « masquer » les données personnelles du CRM avant qu'elles n'entrent dans la DMP.

Concernant les données « second party »

Les données « *second party* » sont celles qui sont reçues par des partenaires de l'entreprise et qui sont intégrées dans la DMP. Dans cette chaîne de transmission, chacun des protagonistes se doit de bien vérifier qu'il respecte ses obligations afin que le traitement final (l'intégration dans la DMP) soit valide et licite.

DONNÉES RÉCOLTÉES AUPRÈS DE PERSONNES PHYSIQUES

↓

Les partenaires commerciaux récoltent les données et les transmettent à une autre entreprise

↓

Réception des données "second party" par l'entreprise

↓

INTÉGRATION DANS LA DMP

LES BASES LÉGALES DE TRAITEMENT POUR LA SOCIÉTÉ QUI RÉCOLTE LES DONNÉES

Au regard de la finalité d'un transfert vers une entreprise tierce, il ne sera possible, selon nous, de fonder ces transferts que sur les bases légales du consentement ou de l'exécution d'un contrat (par ex. contrat de vente de données).

En effet, on le sait, le RGPD impose une information claire, transparente, aisément accessible et compréhensive pour la personne concernée quant aux données récoltées et aux finalités.

Exception faite du cas du contrat de vente des données via lequel la personne concernée sera informée du transfert, nous pensons que la base légale permettant d'assurer la meilleure transparence possible et d'atteindre les objectifs du RGPD — ainsi que du projet de Règlement *e-Privacy* —, en la matière, est la base légale du consentement.

Rappelons également que le projet de Règlement *e-Privacy* prévoit que les conditions du consentement donné dans ce cadre seront identiques à celles de celui donné dans le cadre du RGPD[4].

L'INFORMATION QUANT À CES TRAITEMENTS SI LA DMP EST SOUMISE AU RGPD

L'entreprise qui reçoit ces données ne les a, *de facto*, pas récoltées elle-même. Dès lors, il convient d'informer les personnes concernées de leur traitement en vertu de l'article 14 du RGPD.

Cette information devrait pouvoir se trouver dans un document spécifique[5] qui concerne la protection de la vie privée : la politique vie privée.

L'information, respectant les prescrits de l'article 14 du RGPD, doit donc être transmise aux personnes concernées relativement au fait que l'entreprise reçoit et traite des données de ses partenaires tiers.

En effet, eu égard au devoir d'information et de transparence lors de traitements ultérieurs, le Groupe 29[6] écrit que :

> **« l'obligation d'information doit permettre à ce que la personne concernée puisse raisonnablement s'attendre, au moment et dans le contexte de la collecte de ses données, à un traitement particulier. En d'autres mots, la personne concernée ne devrait pas être prise par surprise quant à la finalité du traitement de ses données personnelles.[7] »**

Il convient également que cette entreprise s'assure de la validité de la base légale utilisée par son partenaire qui lui transmet les données personnelles car la licéité du traitement qu'elle compte effectuer sera dépendante de la validité de la base légale choisie par son partenaire pour opérer ce traitement.

Concernant l'intégration dans la DMP des données « second party » et relations avec les tiers

L'intégration dans la DMP, outil pouvant appartenir à une autre entité juridique, nécessite, puisqu'il s'agira de sous-traitance ou de responsabilité conjointe[8], que l'on rappelle que ce traitement se devra d'être encadré par « *un contrat ou un acte juridique au titre du droit de l'Union ou d'un État membre.* » [9]

En pratique ces contrats ou actes juridiques prendront la forme de DPA (« *Data Processing Agreement* ») ou de JCA (« *Joint Controllers Agreement* ») signés entre les différentes organisations impliquées[1].

Concernant les données « third party »

Ces données sont acquises via des plateformes « data tierces ».

Il convient de rappeler, que comme dans le cas des *first-* et *second-party*, seules les données *third party* permettant d'identifier ou de rendre identifiables une personne tomberont sous l'application du RGPD.

En outre, ces données étant majoritairement acquises via des cookies, il conviendra de vérifier que celles-ci aient été obtenues licitement dans le respect du Règlement *e-Privacy*.

De manière générale, ce sont les entreprises commercialisant la DMP qui intégreront ces données *third party* afin d'enrichir les données de *first* et *second party* et de permettre un ciblage plus précis des personnes concernées.

À l'instar des données *second party*, l'entreprise qui utilise la DMP devra s'assurer de la licéité du traitement des données personnelles.

[1]Cette notion de coresponsabilité pourrait prendre une tournure encore plus importante si la CJUE venait à suivre l'avis de son Avocat général dans l'**affaire Fashion ID**.

En pratique

1

FIRST PARTY

Yolanda achète des vêtements dans un magasin de la société MAS qui est active dans la vente de vêtements en tout genre et de crème solaire. Auparavant, Yolanda avait déjà utilisé le site de la société MAS pour acheter de la crème solaire (indices entre 30 et 50). Lors de son achat dans la boutique physique, elle s'inscrit à la newsletter de la société MAS en laissant juste son adresse email (yola@gmail.com) et en acceptant le traitement de ses données personnelles.

2

SECOND PARTY

Une société partenaire de la société MAS (la société Birthdaytop) est active dans l'évènementiel et a organisé une soirée dans un club de célibataires pour fêter l'anniversaire des 35 ans d'une femme qui a confirmé l'évènement en utilisant la même adresse email que celle donnée à MAS quelques jours plus tôt via son application disponible sur Android.

3

THIRD PARTY

Yolanda fait des recherches sur internet à partir de son laptop pour une croisière pour les célibataires dans les Caraïbes sur le site de la société www.caraibestropcool.com. À nouveau une série de cookies et de pixels est déposée sur son ordinateur.

En pratique

4

La société MAS procède à l'*onboarding* de son CRM, demande à la société Birthdaytop de lui transmettre les données qu'elle a sur les femmes célibataires (ou susceptibles de l'être) et achète des données au site www.caraibestropcool.com pour avoir des informations relatives aux nouvelles tendances des départs aux Caraïbes afin d'améliorer son offre de maillots.

5

La société MAS intègre et anonymise les données qu'elle possède, a reçues et a achetées auprès de www.caraibestropcool.com et les synchronise dans une DMP.

6

Lors de cette synchronisation, un identifiant unique AABR0976 est créé. Il correspond à une femme âgée de 25 à 35 ans, célibataire et intéressée par les voyages dans les pays nécessitant une protection UV importante. Sur base de cet identifiant la société MAS va pouvoir cibler les propositions commerciales faites à Yolanda.

En pratique

Le consentement relatif au traitement des données de Yolanda porte probablement sur les informations que celle-ci a données lors de son achat en magasin. Elles ont directement été obtenues auprès de Yolanda par la société MAS. En outre, comme Yolanda avait déjà acheté de la crème solaire via le site internet de la société MAS, en utilisant la technique du *CRM onboarding*, cette société peut intégrer tant les informations provenant de sa boutique physique que de son site internet.

Les informations relatives à l'âge et à la date d'anniversaire de Yolanda ne figuraient pas dans les informations « *first party* ». La société MAS devrait donc, avant de les traiter, vérifier que Yolanda a – dans la mesure où la base légale justifiant le traitement des données à caractère personnel est le consentement – donné valablement son consentement pour le traitement de ses données.

Concernant les données relatives au voyage, elles ont été obtenues via des cookies. Il convient donc de vérifier que ces informations ont été obtenues légalement au regard de la loi du 13 juin 2005.

La Société MAS, en tant que responsable de traitement, devra donc démontrer que le traitement du profil qu'elle établit, et qui contient énormément de données personnelles (d'identification, financières, d'identification électronique…), est basé sur un consentement répondant aux exigences du RGPD et du Règlement *e-Privacy* dès son application.

Conclusion

Par l'utilisation massive de données, dont parfois des données personnelles, la **DMP n'échappe donc pas aux exigences du RGPD**. Elle n'échappera pas non plus aux obligations de la Directive *e-Privacy*.

Le vrai défi de l'usage de la DMP sera le suivi du consentement car, à l'heure actuelle, il semble difficile de vérifier que le consentement a été obtenu valablement auprès de la personne concernée par tous les acteurs de la chaîne !

Et pourtant, aussi bien le responsable de traitement que les sous-traitants devront s'assurer de la légalité du consentement s'ils veulent éviter de lourdes sanctions…

À propos des auteurs

Frédéric Dechamps est avocat au Barreau de Bruxelles depuis 1997 et membre de la commission des nouvelles technologies du Barreau de Bruxelles.

Avocat au sein du cabinet **Lex4u**, il intervient régulièrement dans des colloques et des conférences pour ses matières de prédilection :

- le droit commercial (pratiques de commerce, droit des sociétés, etc.) ;
- la propriété intellectuelle (droit d'auteur, droit des marques, etc.);
- les nouvelles technologies.

Frédéric est également en charge de la gestion des contrats sur le site web **Lawbox**.

Nathan Vanhelleputte est inscrit au Barreau de Bruxelles depuis février 2018.

Après deux années passées à travailler pour la société d'assurances AIG, il quitte l'entreprise américaine pour participer à la fondation d'un cabinet de consultance spécialisé dans les matières de la Compliance et du Regulatory.

C'est après cette expérience qu'il décide de rejoindre **Lex4u** pour y travailler notamment sur les matières de droit commercial, droit des contrats, droit de la protection des données à caractère personnel ainsi que le droit des nouvelles technologies.

Nathan est DPO certifié par la Solvay Brussels School.

LAWBOX
smart law for smart people

lex4u
Avocats-Advocaten-Lawyers

qualifio

À propos de Qualifio

Qualifio est la plateforme de référence en Europe dans le marketing interactif et la collecte de données. Elle permet de créer et de publier facilement des contenus interactifs viraux (quiz, jeux-concours, enquêtes et plus de 50 autres formats innovants) sur tous les canaux digitaux.

Comment ça marche ?

CRÉEZ

Choisissez votre campagne interactive et customisez-la sans aucune intervention technique

PUBLIEZ

En quelques clics, publiez votre campagne sur vos sites, apps, réseaux sociaux ou sur un mini-site dédié

COLLECTEZ DES DONNÉES

Menez des campagnes 100% conformes au RGPD grâce à un ensemble de fonctionnalités dédiées

OBTENEZ DES RÉSULTATS

Consultez et exportez les données collectées et statistiques de vos campagnes en temps réel

SEGMENTEZ ET MONÉTISEZ

Connectez Qualifio à vos outils marketing et data (CRM, DMP, e-mail, automatisation, SSO, Analytics, etc.)

Ce contenu vous a plu ?

INSCRIVEZ-VOUS À NOTRE NEWSLETTER

Plus d'infos sur Qualifio ?

PARLEZ À UN EXPERT

www.qualifio.com

Références

[1] La Directive *e-Privacy* est déjà d'application depuis longtemps en Belgique via sa transposition dans la loi du 13 juin 2005 relative aux communications électroniques. Afin d'harmoniser la matière, un Règlement européen est en cours d'adoption et était prévu pour le 25 mai 2018 (Proposition de Règlement du parlement européen et du conseil 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 (« Proposition de règlement *e-Privacy* »)).

[2] C.J.U.E (2è ch.), *19 octobre 2016, P. Breyer c. Bundesrepublik Deutschland* , ***C-582/14***.

[3] Même s'il existe six bases de traitement pouvant licitement justifier le traitement de données à caractère personnel, nous n'étayerons pas celles relatives au respect d'une obligation légale, à la nécessité en vue de la sauvegarde d'intérêts vitaux ainsi que celle relative à la poursuite d'une mission de services publics en ce que ces trois bases légales seront les moins utilisées pour justifier des traitements via une DMP dans le cadre d'entreprises privées.

[4] Art. 9 de la Proposition de règlement *e-Privacy*.

[5] Dans ce sens, Avis WP260 du groupe 29, *Guidelines on Transparency under Regulation 2016/679* p. 18 point 33.

[6] Devenu le ***European Data Protection Board***.

[7] Avis WP260 du groupe 29, *Guidelines on Transparency under Regulation 2016/679* p. 23 point 45.

[8] Voyez sur les critères d'appréciation de la qualité de sous-traitant ou responsable conjoint le très récent **arrêt de la CJUE du 10 juillet 2018** concernant les Témoins de Jéhovah (C-25/17).

[9] Article 28, point 3 du RGPD.