Data Management Platforms (DMPs) & data privacy

qualifio

Table of contents

Introduction

What is a **Data Management Platform (DMP)**? Why do companies use them? Are they compatible with the requirements of the new **General Regulations on the Protection of Personal Data (GDPR)** and the **proposal for an ePrivacy Regulation**? Big questions occupying much of the energy and time of brands, agencies and publishers...

Data Management Platform

A Data Management Platform (DMP) is a platform that allows a company to collect, centralise, organise large amounts of data about customers and prospects.

The primary objective of a DMP is to **create audience segments** (e.g. sportsmen between 25 and 40 years old living in the Lille region) via the classification of data collected from different sources. These could be for example a user's navigation on site, purchases they make or participation in a competition or a survey.

These different sources of data and their classification make it possible to enrich data already in the company's possession in order to facilitate targeted marketing campaigns. Further uses of the DMP include: informing product decisions, driving personalised content and enriching business intelligence tools.

FIRST PARTY DATA

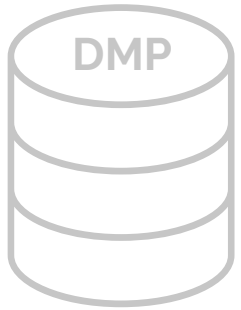
are data belonging to the company. This data has been collected by the company itself (via its CRM - CRM onboarding or cookies).

SECOND PARTY DATA

are data provided by the company's partners.

THIRD PARTY DATA

are data collected via third-party sources (companies that have data mostly from cookies or other tracking technologies and that refine existing segmentation).



DMPs and personal data

In general, a classic DMP will not process personal data unless the personal data is first masked or 'hashed' before it becomes a data point within the platform. In other words personal data is anonymised or pseudo anonymised before it is onboarded.

This 'masked' data is then **assigned an 'ID'** which is synchronised with other data sources to form a unique identifier comprised of the different data sources in the platform.

The classic building blocks of these ID's and their ability to synchronise with one another are cookies and tracking pixels.

Some of the most well known DMPs on the market

DMPs in the face of GDPR and ePrivacy regulations [1]

Does the GDPR therefore apply to DMPs?

The question merits asking since it concerns the ability to identify a natural person and this implies needing to understand how the masking of personal data is happening via cookies and if the data can in some potential way be 'unmasked'.

The only reference to cookies in the GDPR is to be found in recital 30. Recital 30 states *'natural persons may be associated, by the devices, applications, tools and protocols they use, with online identifiers such as IP addresses* ***and cookies*** *or other identifiers, such as radio frequency identification labels'.*

> **"These identifiers can leave traces which, especially when combined with unique identifiers and other information received by servers, can be used to create profiles of natural persons and to identify them."**

The answer therefore is not unfortunately simply arrived at. In practice, it will depend on the measures to protect the privacy of the data, the security measures put in place and, ultimately, the possible connections that may be made between the data and a natural person.

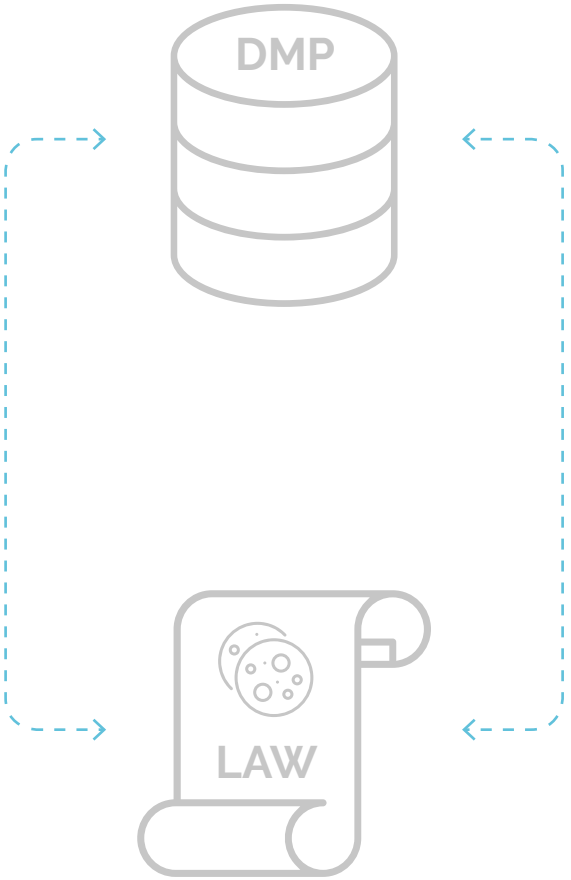
If for example, a connection via a combination of information is possible – remember that IP addresses are considered personal data[2] - and that a natural person can be identified on the basis of the information contained in the DMP, the answer to this question should of course be that the GDPR applies.

What about the draft ePrivacy Regulation?

As the DMP is also enriched by information from cookies or other tracking technologies, in particular from third-party partners, the law of 13 June 2005 on electronic communications should be applied. This law transposes the ePrivacy Directive, which will soon be revised through the adoption of a Regulation.

Since it is established that the GDPR – at least for some of the DMPs – and the ePrivacy Directive apply to these tools, it is necessary to consider the question of the legal bases for processing which may justify the processing of such personal data.

On the basis of the GDPR, for the processing of personal data to be lawful, the processing must be based on article 6.



Basis for lawful processing

Since each type of data included in a DMP comes from different sources, it is necessary to distinguish the legal basis which, in our opinion, could allow the processing of these personal data.

Concerning the first-party data

First-party data is any data collected from the owned and operated properties (offline or online) of a brand or publisher.

A company may therefore base, mainly with regard to the GDPR, the processing of such personal data on one of the three legal bases for processing[3]: consent of the data subject, necessity in the light of the legitimate interests pursued by the company or necessity in order to perform a contract. One of these three legal bases could provide the basis for the processing of personal data with a view to the role of a DMP.

With regard to the current draft of the ePrivacy Regulation, two potential grounds could justify the processing by the company of the data collected. In particular, via the company's cookies: the consent of the end user or, on the basis of Article 8 of the draft Regulation, which states if *'necessary to provide a service [...] requested by the end user'*.

Justification for the legal basis on which the processing of these first-party data is based will ultimately lies the controller under the GDPR. The controller will have to be able to demonstrate either consent, necessity in relation to the performance of a contract or the provision of a service, or finally, proportionality between his legitimate interests and respect for the privacy of the persons concerned.

ONBOARDING CRM DATA IN A DMP

Onboarding CRM data within a DMP consists of creating a link between the information held by a company in its CRM platform – and the information contained in a DMP. This link is possible via the association of information contained in the CRM with an identifier using a cookie. This cookie is used to link to the information held in the CRM and also to 'hash' or 'mask' personal data of the CRM before it enters the DMP.

Concerning the second-party data

Second-party data is received by the company's business partners and integrated into the DMP. In this chain of transmission, each of the protagonists must verify that they are complying with their obligations. Only then can the final processing (i.e. the integration into the DMP) be valid and lawful.

DATA COLLECTED FROM INDIVIDUALS

↓

Business partners collect data and send it to another company

↓

Receiving the Second Party data by the company

↓

INTEGRATION INTO THE DMP

THE LEGAL BASIS FOR THE PROCESSING OF A COMPANY COLLECTING THE DATA

With regard to the purpose of a transfer to a third party company, it will only be possible, in our opinion, to base the transfer on the legal basis of consent or the performance of a contract (e.g. contract for the sale of data).

Indeed, as we know, the GDPR requires clear, transparent, easily accessible and comprehensive information to the data subject regarding the data collected and the purpose of processing that data.

With the exception of the contract for the sale of data (via which the data subject will be informed of the transfer), we believe the legal basis for ensuring the best possible transparency and adherence to the requirements of the GDPR – as well as the draft ePrivacy Regulation – in this respect is the legal basis for consent.

It is worth remembering that the draft ePrivacy Regulations 'conditions for consent' given in this context will be identical to those given in the GDPR[4].

INFORMATION ON THE PROCESSING OPERATIONS OF THE DMP UNDER THE GDPR

The company receiving personal data has not, de facto, collected it itself. Therefore, data subjects should be informed of its processing under Article 14 of the GDPR.

This information should be available in a specific document[5] that deals with privacy protection: a privacy policy.

The information regarding the fact that the company receives and processes data from via third-party partners must therefore be provided to the person(s) concerned in accordance with the requirements of article 14.

Further, with regard to the duty of information and transparency during further processing, the Group 29[6] states that :

> **"the obligation to provide information must ensure that the data subject can reasonably expect, at the time and in the context of the collection of his data, to have a particular processing operation. In other words, the data subject should not be taken by surprise as to the purpose of the processing of his or her personal data.[7]"**

The company (as controller) is also responsible for ensuring the validity of the legal basis used by its partner who collects and transfers personal data on its behalf.

Integration of second-party data into the DMP

Integration of third-party technologies into a DMP, will involve subcontracting or joint liability for data processing[8], In this scenario the processing operation should be governed by 'a contract or a legal act under Union or Member State law'.[9]

In practice, these contracts or legal acts will take the form of DPA ('Data Processing Agreement' or JCA ('Joint Controllers Agreement') signed between the various organisations involved[1].

Concerning the third-party data

Third-party data is any data acquired via 'third-party data' platforms or outside of a company's owned and operated properties (offline or online).

It should be clarified that for this type of data, only data that identifies a natural person or makes a natural person identifiable, fall within the scope of the GDPR.

In addition, since most of this data is acquired via cookies, it will be necessary to verify that they have been lawfully obtained in compliance with current draft of the ePrivacy Regulation.

In general, the DMP provider will integrate third-party data in order to enrich or extend the first and second-party data and to allow a more scalable targeting of the persons concerned.

As with second-party data, the company using the DMP will have to ensure that the processing of personal data is lawful.

[1]This notion of co-responsibility could take an even more important turn if the ECJ were to follow the advice of its Advocate General in the **Fashion ID** case.

Use case

1

FIRST PARTY

Yolanda buys clothes from the company MAS's store which sells all kinds of clothing and sunscreen. Previously, Yolanda had already used MAS's website to buy sunscreen (index between 30 and 50). During her purchase in the physical store, she subscribes to MAS's newsletter by just leaving her email address (yola@gmail.com) and accepting the processing of her personal data.

2

SECOND PARTY

MAS's partner (a company called Birthdaytop) is active in events and organised a party in a club for singles to celebrate a woman's 35th birthday, who confirmed the event using the same email address given to MAS a few days earlier via its app (available on Android).

3

THIRD PARTY

Yolanda searches the internet from her laptop for a cruise for singles in the Caribbean, on the website www.caraibestropcool.com. Again, a series of cookies and pixels are left on her laptop.

Use case

4

MAS carries out the onboarding of its CRM, asks the company Birthdaytop to transmit the data it has on single women (or likely to be) and buys data at www.caraïbestropcool.com to have information on new trends in Caribbean departures to improve their swimsuits offering.

5

MAS integrates and anonymises the data it owns, received and purchased from www.caraibestropcool.com, and synchronises them into a DMP.

6

During this synchronisation, a unique identifier (AABR0976) is created. It corresponds to a woman aged 25 to 35, single and interested in travelling, in need of significant UV protection. Based on this identifier, MAS will be able to personalise the commercial proposals made to Yolanda.

Use case

Consent to the processing of Yolanda's data likely relates to the information she gave when she made the purchase in store. This was obtained directly from Yolanda by MAS. In addition, Yolanda had already purchased sunscreen through the MAS website. Thus, via onboarding of the CRM data, MAS can integrate information from both its physical shop and website.

Information about Yolanda's age and birthday was not included in the 'first-party' information. MAS should therefore, before processing this data, obtain Yolanda's explicit consent – as it relates to the legal basis for the processing of personal data.

In the above example travel data was obtained via cookies. It is therefore necessary to verify that this information has been legally obtained in accordance with the law of 13 June 2005.

MAS, as the data controller, will therefore have to demonstrate that the processing of the profile it establishes, which in the above example contains multiple points of personal data (identification, financial, electronic identification, etc.), is based on consent as per the GDPR.

Conclusion

Owing to the enormous scale and diversity of data it processes, including the onboarding and masking of personal data, the **DMP does not escape the requirements and reach of the GDPR**. Nor will it escape the obligations of the ePrivacy Directive.

The real challenge of using the DMP at present will be to evaluate and ensure consent as per the requirements of a data controller under the GDPR. The challenge is not small given the potential variety of actors and data sources involved in the DMP.

However, whilst the primary responsibility lies with the controller, both the controller and the data processor(s) will have to ensure the legal validity of the data consent if they want to avoid severe sanctions...which have been much discussed since the 25th of May 2018.

About the authors

Frédéric Dechamps is a member of the Brussels Bar since 1997 and is a member of the Brussels Bar's New Technologies Commission.

He regularly participates in conferences and symposiums around his favourite subjects:

- commercial law (commercial practices, company law, etc.);
- intellectual property (copyright, trademark law, etc.);
- new technologies.

Frédéric is also in charge of contract management on **Lawbox**.

Nathan Vanhelleputte is a member of the Brussels Bar since February 2018.

After two years working for the insurance company AIG, he left the American company to help establish a consulting firm specialising in Compliance and Regulatory matters.

After this experience, he decided to join **Lex4u** to work on commercial law, contract law, personal data protection law and new technology law.

Nathan is a DPO certified by Solvay Brussels School.

qualifio

About Qualifio

Qualifio is the leading SaaS in Europe for interactive marketing & data collection. It allows brands and media groups to easily create and publish interactive contents (quizzes, personality tests, polls, and 50+ other innovative formats) on all their digital channels. The goal? Collect data on their digital audiences to better engage, qualify, segment and monetise them.

How does it work?

CREATE

Choose your interactive campaign from 50+ formats, fully customisable and without extra development

PUBLISH

Easily publish it on your websites, mobile apps, social networks or on a dedicated minisite

COLLECT DATA

Run GDPR-compliant data collection campaigns thanks to a set of dedicated features

GET RESULTS

Visualise and extract profiles collected and campaigns statistics in real time

SEGMENT AND MONETISE

Connect the platform to your marketing & data tools (CRM, DMP, SSO, Analytics, etc.)

More content like this one?

SUBSCRIBE TO OUR NEWSLETTER

More about Qualifio?

TALK TO AN EXPERT

www.qualifio.com

References

[1] The ePrivacy Directive has already been in force for a long time in Belgium through its transposition into the law of 13 June 2005 on electronic communications. In order to harmonise the matter, a European Regulation is being adopted and was scheduled for 25 May 2018 (Proposal for a Regulation of the European Parliament and of the Council concerning privacy and the protection of personal data in electronic communications and repealing Directive 2002/58/EC («Proposal for an ePrivacy Regulation»)).

[2] C.J.E.U (2nd Ch.), *19 October 2016, P. Breyer c. Bundesrepublik Deutschland* , ***C-582/14***.

[3] Even if there are six processing bases that can lawfully justify the processing of personal data, we will not review those relating to compliance with a legal obligation, the need to safeguard vital interests and the need to pursue a public service mission in that these three legal bases will be the least used to justify processing via a DMP in the context of private companies.

[4] Article 9 of the Proposal for an ePrivacy Regulation.

[5] In this sense, Opinion WP260 of Group 29, *Guidelines on Transparency under Regulation 2016/679* p. 18 point 33.

[6] Became the ***European Data Protection Board***.

[7] WP260 Opinion of Group 29, *Guidelines on Transparency under Regulation 2016/679* p. 23 point 45.

[8] See the very recent **judgment of the ECJ of 10 July 2018** concerning Jehovah's Witnesses (C-25/17) on the criteria for assessing the status of subcontractor or joint manager.

[9] Article 28(3) of the GDPR.