GENERAL DATA PROTECTION REGULATION

What are the benefits and drawbacks of the new General Data Protection Regulation (GDPR) for the online advertising industry?

Stan de Ruiter
1659289

Docent: Rogier Manten
JDE-SCONE.3V-13
Seminar English

TABLE OF CONTENTS

How is data collection currently regulated in the EU? (1/2)

As of May 25th 2018 the General Data Protection Regulation will replace the old Data Protection Directive (DPD). The Data Protection Directive was the law that came into effect in 1995. It was created to protect the personal data of internet users (Roland, 2017). It will come as no surprise that since 1995 there has been a lot of milestones in technology when it comes to internet and the application of data. Therefore, the European Commission gathered to make some new policies better suited to the current state of the internet. How data collection is currently regulated will be discussed below.

First of all, and probably for most users the most significant difference with the new regulation is about consent. In the past, the Data Protection Directive allowed companies such as advertising agencies to create a certain profile of IP addresses, without informing the user when and what specific data is collected of them. It also didn't give users a chance to look into the data companies have of them. With the General Data Protection Regulation users will be able to look into the information companies have of them and they will be offered to erase some or all of the information companies have of them. In other words, the individual rights of users have increased significantly in such way that companies can not longer be deceiving or ambiguous. In the following chapter the GDPR will be discussed more specifically.

Another important difference with the new regulation is the way personal data is defined. According to SeeUnity (2018) the old directive defines personal data as the following things:

- Name
- Photo
- E-mail address
- Phone number
- Address
- Personal identification number

Of course, with the current state of technology companies can trace back much more information to a user than the stated above. That is why the GDPR widens the definition of personal data so the user is better protected for marketing strategies such as retargeting (SeeUnity, 2018).

The third big difference is about accountability. Within the jargon of data collection there are two parties that have to work together, these are the data processor and the data controller. The Information Commissioner's Office (2017) describes a data controller as "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed" and a data processor as "any person (other than an employee of the data controller) who processes the data on behalf of the data controller." For example: an energy supplier wants to create new types of energy subscriptions based on the data they have collected of their customers. They hire a digital agency to segment the data to make profile groups to get a better understanding of their customers. In this case the energy supplier is the data controller because they determine in which manner the data is to be processed. The digital agency on the other hand is the data processor, because they process the data of the customers on behalf of the energy company. With the Data Protection Directive only data controllers were held accountable for the security of data. In case something went wrong, data controllers were the ones that paid the legal fines. For example: If there is a data breach at a digital agency, and the personal data of their client customers is being exposed, the full responsibility is with the energy supplier. Of course, this causes many problems between the data controller and the data processor. That is why as of May 25th data processors will also be liable with the General Data Protection Regulation.

Another big difference is about what is called "Privacy by Design". With the Data Protection Directive companies weren't obligated to consider privacy as an essential part of their business concept, if their key business wasn't about collecting data, much more was privacy

How is data collection currently regulated in the EU? (2/2)

considered as an addition. According to the General Data Protection Regulation privacy should be at the foundation of the business concept (Danon, 2017).

The last big differences are about what to do when there is a data breach and what kind of penalty to give when a data breach has taken place. With the Data Protection Directive there was no specific procedure to follow when something went wrong. It was hard to say what kind of data was exposed and even harder to define how big the impact would be. With the General Data Protection Regulation there will be one procedure for everyone to follow. Just like there was no standard procedure, there was no standard penalty system as well. Every EU member could decide for their self what kind of penalty they would give the company in question (SeeUnity, 2018).

What does the GDPR contain? (1/2)

The General Data Protection Regulation is the new law which determines how data may be collected and applied. The law will come into effect as of May 25th. In this chapter the difference between the old and the new law will become clearer as the GDPR will be explained and discussed more extensively.

First of all, it is important to put into context why there is a new law. The public debate about the price people have to pay to use the internet is rising. In an era where people are almost always connected to the internet this is an obvious discussion. One of the concerning applications of the discussion is behavioral tracking. Behavioral tracking is a tool for companies to create a certain profile based on the internet behavior of a user (IP address) without any consent of the user. This happens on a big scale and under the Data Protection Regulation it is (in most cases) completely legal. (Domoslawska, Dougherty, & Canada, 2014). Of course, a lot of people don't want this to happen. The current compromise between the use of the internet and the giving out of personal data has made the new law inevitable.

The individual rights of the internet user have increased significantly under the new law. With the General Data Protection Regulation users will be able to see exactly what kind of data companies want to collect of them. The user must be offered to change, erase or even request the data companies have of them (WARC Best Practice, 2017).

With the old directive companies had extremely long terms and conditions with complex law jargon to request the clients consent for the use of their data. Of course no person would spend 20 minutes reading the terms and conditions to check what time his or her train would leave. In most cases people would just accept anyway. This is why the General Data Protection Regulation insists on having clear and short policy agreements. Not only should companies be transparent, they should also keep good recordings of who gave consent and when they did it (Roland, 2017).

"When" is especially important since the the Information Commissioner's Office (2017) advises companies to ask for consent every two years to make sure customers/users are still aware of the things they initially agreed to.

With the new law it's especially important to emphasize the difference between how personal data was and is defined. According to SeeUnity (2018) the new Data Protection Regulation defines personal data as the 15 following data forms:

1. Name
2. Photo
3. E-mail address
4. Phone number
5. Address
6. Personal identification number
7. IP Addresses
8. Mobile Device Identifiers
9. Geo-Location
10. Biometric data
11. Psychological identity
12. Genetic identity
13. Economic status
14. Cultural Identity
15. Social identity

Where the Data Protection Directive only protected the first 6 data forms from the list, the General Data Protection Regulation covers all the 15 data forms.

As claimed in the previous chapter; the data controller and the data processor will both be liable in the event of a data breach under the General Data Protection Regulation. In the past, under the Data Protection Directive, the regulation of data that is being collected and the procsessing of that data was a gray area between the data processor and the data controller. This is why under the General Data Protection Regulation a data protection officer has to be appointed. If one of the core activities of a company is related to the collection or processing of data in any possible way on a systematic base, the data protection officer will make sure that there are no misunderstandings regarding accountability between the

What does the GDPR contain? (2/2)

two parties and keep track of all the recordings (SeeUnity, 2018).

Privacy by design requires companies to think of privacy of personal data as if it is the core of their business. That is why under the General Data Protection Regulation every company is obliged to apply it to their business. Cavoukian (2009) created 7 foundational principles for privacy by design:

1. Proactive & preventive

This principle requires companies to think ahead of problems like data breaches. Instead of reacting on them, prevent them. The business should always be aware of the risks and threats that come paired with collecting and processing of personal data. The responsibility is fully within the company.

2. Default

This principle exists to ensure that the user shouldn't undertake any action to protect his privacy. The data is private by default until the user gives his consent to the company to use his or her data.

3. Embedded

This principle requires companies to integrate privacy in the design and code of their websites. Rather than losing functionality because a user didn't give his/her consent, privacy notices should be incorporated in the design of the website.

4. Full functionality

This principle pleads that when it comes to privacy, there can never be a compromise. Every objective of the website should be fully functional.

5. Full Lifecycle Protection

This principle requires that every part of the data collection and data processing is being done in a safe manner. The data is being collected safe, stored safe and destroyed safe.

6. Visibility & transparency

This principle requires companies to stay transparent to the user about the purpose of the data collection and processing. This way the company can not just change the purpose of it.

7. User centric

The last principle requires that the interests of the user is always above the interests of the company.

In the case of a data breach, companies have to inform the supervisory authority within 72 hours after discovery. This is one of the guidelines for what to do in case of a data breach under the General Data Protection Regulation (Bird & Bird, 2017). With the Data Protection Directive there were multiple guidelines to follow which made companies choose those who suited them best. Not only the supervisory authority should be notified by the data protection officer, also the individuals that are in risk of having their personal information exposed. In this notification the data protection officer must most importantly explain how the company is going to fix the problem and tell how they are going to compensate for the harm that is done. And just like there are uniform guidelines under the General Data Protection Regulation, there are also uniform fines to be paid if a data processor or data controller didn't follow legislation. These fines can be as high as 20 Million Euros or 4% of the global turnover of a company (SeeUnity, 2018).

How is data collection regulated elsewhere?

The General Data Protection Regulation brings a lot of changes in the EU. But data collection is not only happening in EU, this rises the question: how is data collection regulated in the rest of the world? And more specifically; will the GDPR affect the rest of the world. To put the situation with the General Data Protection Regulation into context, this chapter concerns primarily on how data collection is regulated in the United States of America.

First of all, it's important to give some explanation about the American legal system. The United States of America consists of over 50 states. In the United States there are federal laws which serve and are effective for the whole country, but there are also state laws which only serve and are effective in the state they belong to (Widerman & Malek, 2016). Because of these two legal systems there are a lot of different laws to take into account when it comes to privacy, and it is decided by the state what kind of rules companies should comply to. Besides federal laws and states laws, the authority called the Federal Trade Commission regulates companies to see if they are not involved in any ambiguous or deceptive practices.

A big difference between data collection in Europe and the United States is how personal data is defined in the United States and how it is defined in Europe. According to DLA Piper (2017), the Federal Trade Commission defines personal data as: "information that can reasonably be used to contact or distinguish a person, including IP addresses and device identifiers." But most of the federal and state laws don't use this definition of personal data, because they don not include data forms that do not directly identify a person, such as an IP address (DLA Piper, 2017). This is in contrast with the General Data Protection regulation which considers almost every form of data that can be traced back to a user as personal data.

However, recently there was a milestone in terms of privacy by the Digital Advertising Alliance. They made it harder for marketers to follow customers by obstructing a practice called "cross-tracking". This practice makes it possible to follow the web behavior of a user over all his devices and create a certain profile of him/her. This way marketers know best in what stage of the purchasing process you are and refine the sort and the intensity of ad's you see (Field, 2017). For example; if you looked up a new pair of sneakers for the first time on your laptop, chances are that the next day you will get an ad on your Instagram feed showing the same pair of sneakers with some comparable options. Now customers have to give their consent before this practice can be initiated, and if the customer wants to change, erase or adjust his consent they should be given the option to do this anytime (Field, 2017).

In the United States there are no laws that obligate companies to register the data they have collected. Just like there are no requirements to appoint a data protection officer (DLA Piper, 2017). For the collection and processing of data the regulations are in general quite similar with the old Data Protection Directive in the European Union. In most cases companies have to ask for consent with an opt in or opt out request and the possibility to delete the collected data (DLA Piper, 2017). But, now that the General Data Protection Regulation is coming into effect, companies from the United States have to be careful as well. Reed Freeman, a Partner at Wilmer-Hale described the situation as following: "It applies to you if you're processing the information of somebody in Europe – [if] you touch it, you process it.... If it's a European resident's data, the GDPR applies to you, wherever you sit" (Whiteside, 2017). For example; if an American company targets a European customer they should comply with the General Data Protection Regulation, even if it was not intended. In other words, even businesses outside of the EU have to find a way to comply to the General Data Protection Regulation.

How does the GDPR affect online advertising firms how should they deal with it?

The General Data Protection Regulation brings along setbacks for the clients of advertising firms. But how does the General Data Protection Regulation hit advertising firms? And what are the opportunities for these firms?

A frequently mentioned argument about the General Data Protection Regulation is that marketers can enhance consumer trust with the new law. Roland (2017) describes in her article GDPR: an opportunity to build consumer trust that because of data breaches in the past, consumers lost their trust in marketers, especially because of their irresponsible attitude towards the customer. By ensuring the safety of the customer's data and showing them that the firm is well prepared for any threats the trust of the customer can be enhanced.

Another argument, to see it as an opportunity, is that the firm has another chance to go over the data they are collecting. If you are already obligated to have a critical view on your data collection the firm might as well reconsider if they are doing the best to their ability to push conversions. Cristian van Nispen (2018), team lead insights at Dept (an international digital agency), stated: "take the GDPR as an opportunity instead of a threat. We are forced to think about it, but it means we have the opportunity to take a service-driven approach and take a moment to think about it."

The most important key takeaways for online advertising firms from this research are described below:

1. Consent must be seen as a first priority.

For example, inactivity of a customer by not updating his subscription on a newsletter does not constitute consent.

2. Make everything as clear as possible.

If the company is really clear about what they are going to do with the data and they are really transparent about the collected data of customers towards customers, they should not have any concerns about the regulations.

3. Do not ask for data that is not going to be used.

Companies have to ask themselves if there is a business value in collecting particular data. If there is not, they shouldn't collect it. This will be more efficient for companies because they don't have to monitor their data all the time, and this way they don't have to worry about regulations.

4. Don't be ambiguous.

For example, a lot of companies apply pre-checked subscription boxes. This kind of manipulative practices are being punished by the EU regulators.

In general, it's expected that the deadline of the 25th of May is a soft deadline. But for most companies it's a good incentive to finally take a good look at how data is collected and processed within their company. If companies just make sure they are transparent and take a good look at the consent of the customer, they are already halfway and regulators won't be knocking at the door right away.

Sources

Bird & Bird. (2017, October 3). Personal data breaches and notification. Retrieved March 3, 2018, from **https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/42--guide-to-the-gdpr--personal-data-breaches-and-notification.pdf?la=en**

Cavoukian, A. (2009, August). Privacy by Design: The 7 Foundational Principles. Retrieved March 3, 2018, from **https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf**

Danon, S. (2017, February 10) Privacy by Design and by default. Retrieved March 3, 2018, from https://www2.deloitte.com/nl/nl/pages/risk/articles/gdpr-top-ten-6-privacy-by-design-and-by-default.html

DLA Piper. (2017, January 25). Data Protection Laws of the World: United States. Retrieved March 22, 2018, from **https://www.dlapiperdataprotection.com/index.html?t=authority&c=US**

Domoslawska, M., Dougherty, H., & Canada, M. (2014, September). Tracking the footprint of the digital consumer: A global benchmark for consumers' habits across web, mobile, GPS locations and social media. Retrieved March 3, 2018, from **https://www-warc-com.hu.idm.oclc.org/content/article/esomar/tracking_the_footprint_of_the_digital_consumer_a_global_benchmark_for_consumers_habits_across_web_mobile_gps_locations_and_social_media/102680**

Field, A. (2017, June). The new data privacy law that could have major repercussions for marketers. Retrieved March 20, 2018, from **https://www.warc.com/content/article/ana/the_new_data_privacy_law_that_could_have_major_repercussions_for_marketers/112058**

Information Commissioner's Office. (2017). Data controllers and data processors: what the difference is and what the governance implications are. Retrieved February 24, 2018, from **https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf**

Roland, L. (2017, May). The global impact of GDPR and what brands need to do. Retrieved February 24, 2018, from **https://www-warc-com.hu.idm.oclc.org/**

Roland, L. (2017, May). The lowdown on GDPR: consent is king. Retrieved March 3, 2018, from https://www-warc-com.hu.idm.oclc.org/SubscriberContent/Article/The_lowdown_on_GDPR_consent_is_king/111694

Roland, L. (2017, February). GDPR: an opportunity to build consumer trust. Retrieved March 20, 2018, from **https://www.warc.com/content/article/event-reports/gdpr_an_opportunity_to_build_consumer_trust/110857**

SeeUnity. (2018). The main differences between the DPD and the GDPR and how to address those moving forward. Retrieved February 24, 2018, from **https://seeunity.com/whitepapers/main-differences-dpd-gdpr/**

Van Nispen, C. (Director). (2018, January 31). Your top GDPR questions: A Q&A with Dept's Cristian van Nispen [Video file]. Retrieved March 23, 2018, from **https://www.youtube.com/watch?v=GExLt3CBFhg&t=1s**

WARC Best Practice. (2017, July). What we know about data protection and privacy. Retrieved March 3, 2018, from **https://www-warc-com.hu.idm.oclc.org/content/article/bestprac/what_we_know_about_data_protection_and_privacy/111995**

Whiteside, S. (2017, June). What the EU's GDPR and ePrivacy Regulation mean for US marketers. Retrieved March 20, 2018, from **https://www.warc.com/content/article/event-reports/what_the_eus_gdpr_and_eprivacy_regulation_mean_for_us_marketers/112002**

Widerman & Malek. (2016, February 11). Different State, Different Law. Retrieved March 3, 2018, from **http://legalteamusa.net/law/2016/02/11/different-state-different-law/**