MARTECH & GDPR

Finding the balance between compliance and competitiveness

May 20th 2022 • Version: 1.0

STITCHD
Jente De Ridder
+32 474 78 21 49
Jente.deridder@stitchd.be

Veldkant 33A
2550 Kontich
www.Stitchd.be
BE0677 416 326

deJuristen
Kris Seyen / Larissa De Keyser
+32 473 74 06 45
hallo@dejuristen.be

Heernislaan 19
9000 Gent
www.deJuristen.be
BE0844 098 750

Table of Contents

Preface by Kris Seyen

We all want our business to thrive. We all want to know our customer. And in our digital society, there are great tools available to achieve that.

It is therefore frustrating when there are important limitations set to our ability to deploy such tools. And yet, this is the case for US-based martech tools used by European entrepreneurs. Our GDPR (privacy) regulation sets requirements that are hard to meet.

So, starting from that frustration, the good intentions to offer value to the customers, and the obscurity of GDPR: why not be creatively pragmatic?

For those who still want to broadly bend the GDPR rules to their own marketing needs: you might be making a strategic mistake. Consider the data subject in the privacy landscape as the vulnerable road user in traffic: in case of doubt, they have at least an edge.

The temptation is great not to see the problem, especially now that rumours about a Privacy Shield 2.0 are buzzing. Be aware that this was merely a political announcement, and that the European Data Protection Board has already issued a diplomatic, yet very clear warning: “The EDPB looks forward to assessing carefully the improvements that the new framework may bring in light of EU law, CJEU case law and previous recommendations of the Board, once the EDPB receives all supporting documents from the European Commission.” We are not there yet …

In the meantime, our task is to create awareness and to guide you as an entrepreneur so that the right assessments can be made

Introduction

The past decade has seen a proliferation of new marketing technologies (+5.000% growth since 2011). Whereby the focus has mainly been on ever more far-reaching ways of data collection and consumer profiling. This testifies to the two major trends within the marketing landscape:

- *On the one hand, companies are increasingly competing in terms of customer experience and are continuously looking for tooling that will enable them to offer relevant customer experiences.*
- *On the other hand, FAANG (Facebook, Apple, Amazon, Netflix & Google) have made it clear that data brings power. The one who manages to collect the most consumer data puts competitors out of the game.*

Today, we see that the MarTech industry is being forced to become more responsible quickly. The cowboy years, when anything was possible and the sky was the limit, are over. Legislators are stepping in and are trying to protect consumers from the data collection frenzy. The EU took the lead with the GDPR legislation (in force since May 2018). And we are seeing similar initiatives in the US, South Africa, India and other countries.

This legislative framework gives privacy activists the weapons they need to expose abuses and force the MarTech industry to change. A good example of this are the 101 complaints filed by NOYB to alert European companies to the illegal data transfers in which they are currently participating. Most complaints concern the use of American MarTech solutions like Google Analytics, Facebook Ads, etc.

In this guide, we explain our interpretation of the recent court decisions on the use of marketing technologies. What is the impact of these judgements? And how can organizations deal with them?

The legislation

The complexity and uncertainty surrounding the use of marketing technology can be reduced to 3 key elements within the GDPR legislation. It is important to understand these elements properly before looking for solutions.

Key elements of the GDPR

Definition of personal data

The GDPR applies when personal data is processed. Personal data is very broadly interpreted (Article 4 GDPR). In simple terms, it refers to **every piece of information, that can be linked to an individual person. This can be direct or indirect.**

The existence of a direct link, refers to data that can in itself identify an individual. Data with an indirect link refers to data which can lead to an individual, not really by itself, but by combining it with other data.

In summary, the golden criterion for speaking of personal data is that data, on its own or in combination with other data, allows an individual to be singled out. Singling out means to be able to point out someone out of a certain crowd. Therefore, regardless of whether you actually know who the person is, the mere fact that it is possible to individualize someone, to distinguish them from a crowd, is enough to speak of personal data.

Consent

While being one of the more well-known legal bases for processing personal data, consent is only one of six bases mentioned in the GDPR. The others are: contract, legal obligations, vital interests of the data subject, public interest and legitimate interest as stated in Article 6(1) GDPR.

The basic requirements for the effectiveness of a valid legal consent are defined in Article 7 and specified further in recital 32 of the GDPR. Consent must be freely given, specific, informed and unambiguous.

In order to obtain **freely given consent**, it must be given on a voluntary basis. The element “free” implies a real choice by the data subject. Any element of inappropriate

pressure or influence which could affect the outcome of that choice renders the consent invalid.

For consent to be **informed and specific**, the data subject must at least be notified about the controller's identity, what kind of data will be processed, how it will be used and the purpose of the processing operations. The data subject must also be informed about his or her right to withdraw consent at anytime. The withdrawal must be as easy as giving consent.

Last but not least, **consent must be unambiguous**, which means it requires either a statement or a clear affirmative act. Consent cannot be implied and must always be given through an opt-in, a declaration or an active motion, so that there is no misunderstanding that the data subject has consented to the particular processing.

Data transfers

The next concept is the **transfer of personal data outside the European Economic Area (the EEA)**. The EEA includes every EU member state, plus Norway, Iceland and Liechtenstein. A country outside the EEA is called a "third country". A transfer of personal data to a third country is only lawful under the GDPR insofar as **an adequate level of protection** is ensured with that transfer. This means adequate in relation to the protection of personal data that is guaranteed within the EEA.

According to the GDPR, such adequate level of protection can be guaranteed in three possible ways:

1) **An adequacy decision exists for the third country** (art. 45 GDPR).
This means that the European Commission has confirmed that the third country offers an adequate level of protection.

2) **Appropriate safeguards are in place** (art. 46 GDPR).
In the absence of an adequacy decision, appropriate safeguards must be provided. The most efficient and practical means that the GDPR indicates is the conclusion of standard contractual clauses (SCCs) approved by the European Commission with the entity in the third country to whom personal data are transferred.

3) **One of the exceptions of art. 49 GDPR applies**.
In case you cannot provide appropriate measures either, there is a last resort and that is the presence of one of the exception situations of Art. 49 GDPR. Only one option is really

relevant for our story and that is when the data subject has explicitly consented prior to the concrete transfer. But, beware, in order for this to be a valid consent under the GDPR, quite a few conditions must be met.

We already know that consent must be explicitly, freely, specifically, informed and unambiguously given by the data subject. In addition, the GDPR explicitly states that for a transfer, the data subject must be informed in advance of the possible risks of such a transfer. In concrete terms, as a controller, you must inform the data subject that, by giving his/her consent, there is a risk that US authorities will be able to access his/her personal data.

Schrems judgments

For data transfers to the US, we had two adequacy decisions in the past. We had one on the Safe Harbour framework and subsequently one on the Privacy Shield framework. However, both frameworks were successively declared invalid by the European Court of Justice (or the ECJ) in its Schrems I and respectively Schrems II judgment. Named after the main plaintiff, the Austrian lawyer and data protection activist "Max Schrems", who persistently works with his data protection organization NOYB to enforce the data protection regulation in Europe.

These declarations of invalidity were due to the fact that the ECJ concluded that **the US does not offer an adequate level of protection due to the existence of surveillance legislation**. After all, there are laws in the United States, such as Section 702 of the FISA act, which allow US authorities to request access to all personal data that US electronic communication service providers hold on EU citizens.

Conclusion, at present, for a transfer to the US, one cannot invoke the existence of an adequacy decision. So, what about a standard contractual clause (SCC) then?

In the Schrems II judgement, the ECJ ruled that the conclusion of SCCs is not sufficient to guarantee appropriate safeguards where the third country is the United States. Precisely because of the existence of this surveillance legislation. In the case of a transfer to the US, the ECJ states that **additional protective measures** must be taken.

Such additional measures can principally be of an organisational, technical or contractual nature. But contractual measures however, will in the case of the US not be a real solution, since contractual obligations are only legally binding for the parties of the contract themselves and will not extend to US authorities. According to the

European Data Protection Board (EDPB) organisational measures will also not be sufficient by themselves. But **as technical measure, you can think of anonymisation, encryption or pseudonymisation** done by the EU controller or EU processor before the data ends up with the US entity.

Impact on MarTech

The Schrems indictments have always focused on big tech's marketing technology. After all, they say, it is these parties that enable mass surveillance of European citizens.

The MarTech sector used to hide behind the definition of PII (Personal Identifiable Information). The user agreement of many of these players stated that the collection of PII within their solutions was prohibited. With PII they meant data elements that can be directly linked to a specific person (for example: name, telephone number, e-mail address, etc.). The definition of personal data under the GDPR, however, has removed this argument: just about any data item is considered personal data in a digital context.

With every interaction between someone's browser and the servers of a MarTech vendor, a lot of meta-information is exchanged such as IP addresses, user agent, etc. Despite arguments from the technology sector that this kind of information exchange is purely functional and that it is usually very complex to trace it back to a person, the legislator still regards it as personal data (the upcomming e-privacy legislation is expected to clarify this). Therefore, you see GDPR consent banners popping up everywhere and using US MarTech vendors is considered an illegal data transfer.

Despite the ruling in Schrems II, BigTech was not really impressed. They added a few paragraphs to their user agreements and thought that was the end of it. Business as usual continued. Max Schrems then decided to take a different approach: with his non-profit organisation NOYB, he filed 101 complaints against European websites using American MarTech (specifically focusing on Facebook and Google). So, instead of going after the Big Tech companies themselves, he now focuses on the users of their technology (the data controllers).

These are the complaints in which we currently see rulings from the Data Protection Authorities of the respective countries. The Austrian Data Protection Authority was first on December 22, 2021, with the French Data Protection Authority CNIL following on February 10, 2022 and on March 2, 2022. They both declared the use of Google Analytics illegal. Since the European Data Protection Board (EDPB) "coordinated" the reaction to the complaints by noyb.eu supposedly with a model response, more such "copy & paste" decisions are to be expected.

Considering the fact that more than 50% of MarTech solutions are headquartered in the US and that they are the dominant players in the market, one cannot help but **conclude**

that many organisations will have to rethink their current marketing approach. Continuing to use the industry standard solutions has suddenly become a liability.

The positive side of this is that it forces everyone to **think critically about the technology they use**. What value do we actually get out of the technology? And do we really know how much data we are sharing with this third party? Simply using a solution "because everyone else is doing it" is no longer advisable.

The downside, of course, is that we lose some of the functionalities and methods we were used to in marketing. The impact of this will be for each organisation to decide. For example, it may be that an organisation will suffer a major competitive disadvantage if it is no longer able to personalise its customer experience. Or ad spend may rise as remarketing is no longer possible.

Thus, there is no unequivocal answer to the question of whether an organisation should switch to an alternative solution or not. This will always depend on the **perceived value of the original technology, balanced against the expected costs** associated with a migration. For example, a new implementation must take place, employees must be re-trained, internal processes must potentially be adapted and licensing costs must be recalculated.

Ultimately, as an organisation, you will need to do a **risk assessment**: what risks do we think we are running by using the tool in question? And do the benefits we experience when using the tool outweigh the estimated risks? The risk can be twofold: the chance that you will actually be fined and the chance that your public relations or brand image will be damaged by the attention that might be drawn to a complaint.

Decision tree

To help you evaluate what to do with a certain MarTech solution, we have made a decision tree (see figure 1) that guides you through the questions that you should ask yourself about the tool.

Eventually, you will end up with one of these four decisions:

- *Continue to use the solution as it is.*
  - *We believe that the benefits of the tool outweigh the risk of receiving a complaint.*
  - *Be aware that this involves an actual (potentially high) risk and is not advisable from a legal point of view.*

- *Mitigate the risk by taking additional measures.*
  - *We feel confident enough that the extra measures will be sufficient to defend our case in court if it comes to a complaint.*
  - *Be aware that this approach does not completely eliminate risk. In particular, the potentially negative PR associated with a complaint remains difficult to eliminate.*

- *Migrate towards European alternatives*
  - *We believe that we will get the same benefits from a European based solution, without having to deal with the complexity of data transfers to the US.*
  - *Only migrating one solution (ex: Google Analytics) does not solve it. Be consistent and find an EU alternative for all cloud-based solutions your organization uses.*

- *Stop using the solution*
  - *We came to the conclusion that we did not experience many benefits from the tool. It is not worth looking for an alternative or taking complex measures.*

Performing a risk assessment requires good knowledge of the specific technology. Just like the correct configuration of additional measures to make a solution as compliant as possible. That is why we always recommend to be guided by a specialised partner, who understands both the technology and the legal context.

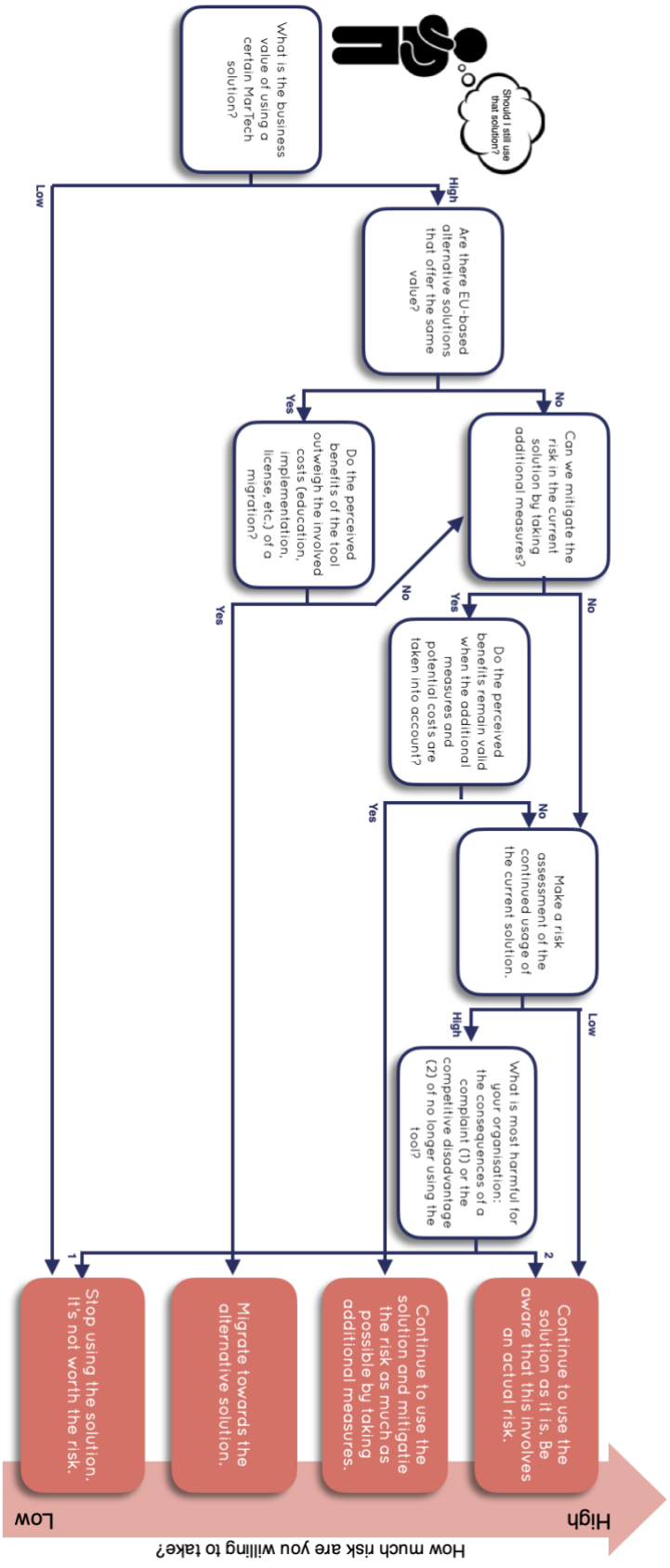

Figure 1 – MarTech Data Transfers Decision Tree

What about...

In this chapter, we discuss specific marketing disciplines. How is each discipline impacted by the GDPR legislation and the lack of a legal framework for data transfers between the EU and US?

Digital Analytics

Digital analytics encompasses the collection, measurement, analysis, visualisation and interpretation of digital data illustrating user behaviour on websites and mobile applications.

It enables organisations to understand how their sites and apps are being found and used. Using digital analytics data, companies can optimise the customer experience on their websites and mobile apps, and also optimise their marketing ROI, content offerings, and overall business performance.

There are many different digital analytics tools available. The largest market share is held by Google Analytics (85% of the market), which is why it is often considered as the "default solution". And that is also why it is being targeted in the recent court rulings. Google Analytics is not the only US based digital analytics solution, but it is definitely the one with the largest reach.

Consent needed?

There is a great deal of confusion as to whether the use of digital analytics solutions is subject to consent or not. It is clear that a digital analytics solution can be used to store personal data. However, it is less clear whether it is possible to really anonymise digital analytics data.

Most vendors claim that it is possible to anonymise the collected data by applying IP annonymisation features etc. The French DPA has compiled an overview of measurement solutions that can be used without consent, provided you stick to a certain configuration. The Dutch DPA published an advice on how to set up Google Analytics so it can be used without consent.

However, there are also examples that state the opposite: every solution that places cookies and is not strictly necessary for the proper functioning of an application, must

ask for consent. This reasoning was followed by the Belgian DPA in the ruling against Jubel.be and also the Planet49 judgment in Germany.

So be aware that whether or not consent is required for the use of digital analytics solutions may vary from country to country. In any case, as a website owner you are responsible for the correct configuration of the privacy settings for these kinds of tools.

Data transfers

In addition to the consent aspect, it is of course also important to consider the potential transfers of personal data outside the European Economic Area that may occur when using digital analytics solutions. The recent rulings in Austria, France and Liechtenstein specifically target Google Analytics and state that it should not be used due to the lack of a data transfer framework.

Google has responded to these rulings by stating that Google Analytics data always remains under the control of the website owner, that the data is not used for profiling across the internet and that they have never received a data access request from the US intelligence services. In addition, they also refer to the many measures that Google takes in the field of privacy and data security.

Despite this reaction from Google, the DPAs in France and Austria seem to stand by their decision. This means that the use of a digital analytics solution from an American vendor can currently be considered a violation of the GDPR legislation. Of course, it is important to realise that this is not just about Google. Other widely used technology vendors such as Adobe, SAS, Microsoft or Salesforce face the same problem.

Our advice

Within the current context, we recommend that organisations think carefully about why they are using a digital analytics solution. What is the value of this data for the organisation? Only when you know the value, you can make an informed decision about whether to switch to an European alternative or look for ways to continue using the current solution.

After all, there are many technical measures that can be taken to anonymise data. You have the built-in features within your digital analytics solution. And another example are vendors like Jentis, that offer pseudo-anonymisation as a service. Each tracking call

that goes to the servers of an American vendor is first sent via their own (European) servers and all possible personal data is hashed. In this way, the American vendor receives anonymous data and is no longer subject to the GDPR legislation. This is of course a very technical fact and in theory the reasoning seems to be correct. However, it remains to be seen whether the legislator will follow this reasoning in court.

European alternatives

If you prefer to switch towards an European alternative, you might want to consider one of the following solutions. We have divided them into 4 categories, based on the needs they fulfil.

- ***Simple KPI dashboards***
  These kinds of solution can best be described as stripped-down web analytics tools: only the most essential KPIs are retained and are displayed in a dashboard that is fairly static. There are little or no filtering and segmentation possibilities. These solutions are aimed at website owners who only need high-level insights such as: how many visits in a certain period, how often pages are visited and how often certain interactions take place. In-depth analyses, custom variables and integrations with other platforms (e.g. advertising tools) are not required.

  - *Plausible.io*
  - *Pirsch.io*
  - *Visitor-analytics.io*
  - *Simpleanalytics.com*

- ***Default web analytics solutions***
  These kinds of solutions are best described as alternatives to the free version of Google Analytics. These web services provide you with the platform you need to measure all your website performance and get the right insights from it. These tools allow you to not only collect basic site metrics such as sessions, time on site, pageviews etc. They also allow you to set up custom things such as measuring events, creating segments, ecommerce measurements, setting up filters, cross-domain tracking, etc. The flexibility of these platforms offers countless extra possibilities for data collection and insights, when compared to the solutions in the simple KPI dashboards category.

- *Piwik.pro*
- *Matomo.org*

- ***Advanced web analytics solutions***
  These solutions can best be described as alternatives to the paid version of Google Analytics: GA360. They offer a lot of customisation possibilities (custom dimensions and metrics), access to raw data, extensive range of integrations with other platforms and tools, extensive data governance functionalities, extensive user governance functionalities, possibility to conclude SLAs, etc. Typically, these types of solutions are aimed at enterprise-level organisations. Organisations where the digital analytics data is not only used for reporting. The collected data plays an essential role in the functioning of the (marketing)organisation. Think for example of personalisation, targeted advertising, customer services, etc.

  - *Piano.io*
  - *Stormly.com*

- ***Tracker only***
  With this type of solution, you create a web analytics environment yourself. You use an event tracker to measure the interaction data on digital platforms. This data is stored in a data warehouse that is under your control, on which a data visualization or BI tool runs to provide insight. So for each functionality you look for a "best-of-breed" solution, instead of looking for an all-in-one solution. This type of solution is only suitable for organisations that have a clear architectural vision of their data landscape, have the technical resources in-house to maintain such a set-up and where the reporting users are able to query data tables.

  - *Snowplowanalytics.com*
  - *Segment.io*

Behavioural retargeting

Behavioral retargeting (also known as remarketing) is a form of online targeted advertising by which the advertising is targeted to consumers based on their previous browsing behaviour. This behaviour is traditionally tracked by the use of marketing pixels (tracking scripts installed by the website owner) and third party cookies (to display advertisments on other domains).

There are many ad exchanges that enable these kind of targeting. The most well-known are Google Ad Manager, Google Display & Video 360, Facebook Ads Manager, Microsoft Advertising, The Trade Desk, Xandr, etc.

Consent needed?

Since with behavioural retargeting you share data of your website visitors with a third party (the advertising platform), it is clear that the only lawful bases can be consent. An identifier is sent (usually a cookie id or a hashed e-mail address) in combination with behavioural data. And regardless of whether you interpret a cookie ID as personal data or not, the fact that you are sharing the data with a third party to build up targeting profiles, means you have to be extra cautious. Therefore, we recommend to never fire ad pixels until the proper permission has been obtained.

This is also explicitly mentioned in the User Consent Policy of Google Ads: "*You must ensure that certain disclosures are given to, and consents obtained from, end users in the European Economic Area*."

Data transfers

The discussion around data transfers within a real-time bidding context is even more complex than that of digital analytics. The current way AdTech works is complex and it is a tangle of too many different parties exchanging data. It is impossible to communicate this in a transparent and understandable way to a visitor of your website.

Moreover, almost all major players in this market are American vendors. In recent years, due to strict regulations, we have seen many European start-ups in the AdTech space. However, they do not yet succeed in generating sufficient volume to be able to replace the Googles and Facebooks of this world. When it comes to behavioural targeting, volume and match rate are the most important criteria.

Our advice

Within the current context, it is difficult—and perhaps impossible—for website publishers and real-time-bidding companies to meet the GDPR's transparency and security requirements. It is clear that a drastic change in the technology (for example Google's proposal for "Topics" – a contextual based targeting mechanism) or more clarification from legislators is needed for publishers to advertise with a clear conscience.

So again, we recommend that organisations think carefully about why they are using behavioural retargeting and what type of data they are sharing with these third parties. Be aware that uploading email addresses to an American AdTech platform (ex: Custom Audiences feature in Facebook Ads Manager) is a practice that is difficult to defend within the current legal framework. Even if you can demonstrate the necessary consent. Maybe you are better off with contextual targeting that does not depend on profiling and data exchanges?

European alternatives

For behavioural retargeting, we strongly recommend investigating the European alternatives. There is still a lot of uncertainty about whether or not these are entirely compliant with GDPR (just think of the condemnation of the IAB consent framework), but at least you will rule out the issue of trans-Atlantic data transfers.

The European DSP platforms that you might want to consider:

- ***AdForm*** *(headquarters in Copenhagen, Denmark)*
- ***Criteo*** *(headquarters in Paris, France)*

A/B testing

A/B testing is a method of comparing two versions of a webpage or app against each other to determine which one performs better. The goal is to optimize the customer journey against a certain business objective. A/B testing technology will help you create different variants, assign website visitors to one of those variants and provides statistical analysis on which variant performed best.

Consent needed?

Whether A/B testing falls under the lawful bases of consent or not depends very much on the type of experiment you want to run.

A research design in which website visitors are randomly assigned to one of the variants can, in principle, take place without the need for explicit consent. Please note that most A/B testing solutions work with cookies and that the user will have to grant permission for these cookies to be placed.

However, an experiment that is based on certain profile characteristics of a visitor or on historical behavioural data falls under profiling. This does require consent.

Since most A/B testing solutions offer the possibility of setting up tests based on a profile, it is safer to assume that consent is required before the A/B testing scripts can be loaded.

Data transfers

Since A/B testing solutions largely have the same tracking capabilities as offered by digital analytics solutions, it is advisable to assume the same reasoning applies: for the European DPAs, tracking of conversions in combination with a cookie ID, will be sufficient to consider it an illegal data transfer to the US.

However, this remains a theoretical discussion and the chance that this type of data is actually relevant for the surveillance services is very small.

Our advice

Think critically about what A/B testing technology is used for within your organisation: is it purely about randomly assigned experiments or is it used to personalise the user experience?

If the former, you could apply the same rules to the use of A/B testing technology as you do to your digital analytics solution.

If the latter, you could provide a specific consent category for the use of A/B testing technology. After all, the user has the right not to be approached personally. And there is a difference in purpose between reporting and personalisation.

In terms of data transfers, the same logic applies as with digital analytics solutions: they collect cookie IDs and have access to the User Agent and IP address. However, A/B testing technologies are less well known to the general public and they are also considered less intrusive by privacy activists. Therefore, the chance of receiving complaints because of an A/B testing solution is smaller than with digital analytics solutions.

European alternatives

If you prefer to switch towards an European alternative, you might want to consider one of the following A/B testing solutions.

- ***Kameleoon*** *(headquarters in Paris, France)*
- ***Ablyft*** *(headquarters in Kiel, Germany)*

- ***Optimizely*** *(EMEA headquarters in Stockholm, Sweden)*
- ***Convert*** *(headquarters in Delaware, USA – but all data is stored in Frankfurt and they claim that none of the data is transferred outside the EEA)*

Conclusion

The MarTech domain is evolving at an accelerated speed. The main driver for these developments is nowadays no longer the new technological possibilities, but the stricter privacy legislation and the corresponding consumer awareness. In this guide, we tried to explain how recent court decisions impact the use of common marketing technologies and how organizations should deal with them.

It is clear that this is a complex topic to which there is no single answer. From a legislative point of view, one could say that it is better to stop any kind of data collection. However, the economic reality is that this often puts you at a competitive disadvantage. It's up to your organization to seek a balance between compliance, ethics and economic interests.

We hope this white paper has given you the tools to have an informed discussion within your organisation. Be it through a better understanding of the legal framework, our handy decision tree to determine whether or not you should continue using certain solutions or the introduction of alternative solutions.

Please realise that the context in which we work today will continue to evolve. It is therefore important that you approach this topic from a strategic point of view and do not see it as a one-off thought exercise. It is time to take responsibility when collecting data. However banal it may sometimes seem. Make sure you have the right knowledge of the technologies you use and stay abreast of new developments both legally and technologically.

Does all this seem very challenging to you? Then do not hesitate to call on specialised parties. For example, we (deJuristen and Stitchd) support many organisations, both large and small, specifically in this area.

About the authors

This white paper is the result of a cooperation between deJuristen and Stitchd. Two companies within the Cronos group, each with their own area of expertise. **deJuristen** is a contemporary niche legal firm, and very proud of its unique pioneering role in Internet law on the Belgian market. **Stitchd** is a boutique consultancy firm, specialised in digital tracking and data-driven marketing use cases.

The following experts worked on this whitepaper.

Kris Seyen

Experienced business lawyer with strong analytical yet hands-on mind set enabling business processes from "outside in" perspective.
Track record of providing legal services to multinational companies and recognised for cross-industry consulting.

Larissa De Keyser

Thorough and knowledgeable privacy expert, with a mindset to take a 360° view of a problem, and an empathy towards business drivers and how to combine these with "privacy by design".

Jente De Ridder

Digital tracking & MarTech expert. Passionate about the role of data in marketing and digital.

Founder of Stitchd, a team for hire of world-class digital analytics experts. With a track record of supporting multinational organisations to get their MarTech set-up right.

References

In developing this white paper, we have built on valuable information from many researchers, regulators, vendors and marketing/legal experts. Most of these have already been referenced in the above text via a link. Below you find an overview of each source.

https://support.google.com/analytics/answer/11999096

https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers.pdf

https://blog.google/around-the-globe/google-europe/google-analytics-facts/

https://www.vischer.com/en/knowledge/blog/how-to-legally-use-google-analytics-in-europe-39512/

https://www-dury-de.translate.goog/datenschutzrecht-blog/privacy-shield-2-0-erste-reaktion-von-dury-legal

https://gdpr-info.eu/issues/consent/

https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform

https://www.itm.nrw/wp-content/uploads/document-dsb.pdf

https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply

https://noyb.eu/en/101-complaints-eu-us-transfers-filed

https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=221913

https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434

https://www.natlawreview.com/article/gdpr-usa-new-state-legislation-making-closer-to-reality

https://cloud.netapp.com/blog/ccs-blg-popia-compliance-do-we-need-to-comply-with-south-africas-version-of-the-gdpr

https://portswigger.net/daily-swig/indias-answer-to-gdpr-data-protection-legislation-set-to-pass-this-year

https://ec.europa.eu/info/law/law-topic/data-protection_en

https://chiefmartec.com/2020/04/marketing-technology-landscape-2020-martech-5000/

https://www.superoffice.com/blog/customer-experience-statistics/

https://insidebigdata.com/2021/04/23/facebook-and-the-power-of-big-data-and-greedy-algorithms/

https://iabeurope.eu/eu-us-privacy-shield/

https://www.atinternet.com/en/glossary/digital-analytics-2/

https://w3techs.com/technologies/details/ta-googleanalytics

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_privacyvriendelijk_instellen_google_analytics_april_22.pdf

https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies-solutions-pour-les-outils-de-mesure-daudience

https://www.standaard.be/cnt/dmf20191229_04786147?articlehash=31C1FE51991F6035A45F461B257A2E3223668C8C27C8E8661629F674A3FC54E1CA24773D7409129F86FDCAA853AE9BFA53F931B255DFA7F34D32FA26D7F61CB7

https://www.datenschutzstelle.li/aktuelles/google-analytics-und-der-datenschutz

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896855

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694680/IPOL_STU(2021)694680_EN.pdf

https://iapp.org/news/a/belgian-dpa-fines-iab-europe-250k-euros-over-consent-framework-gdpr-violations/