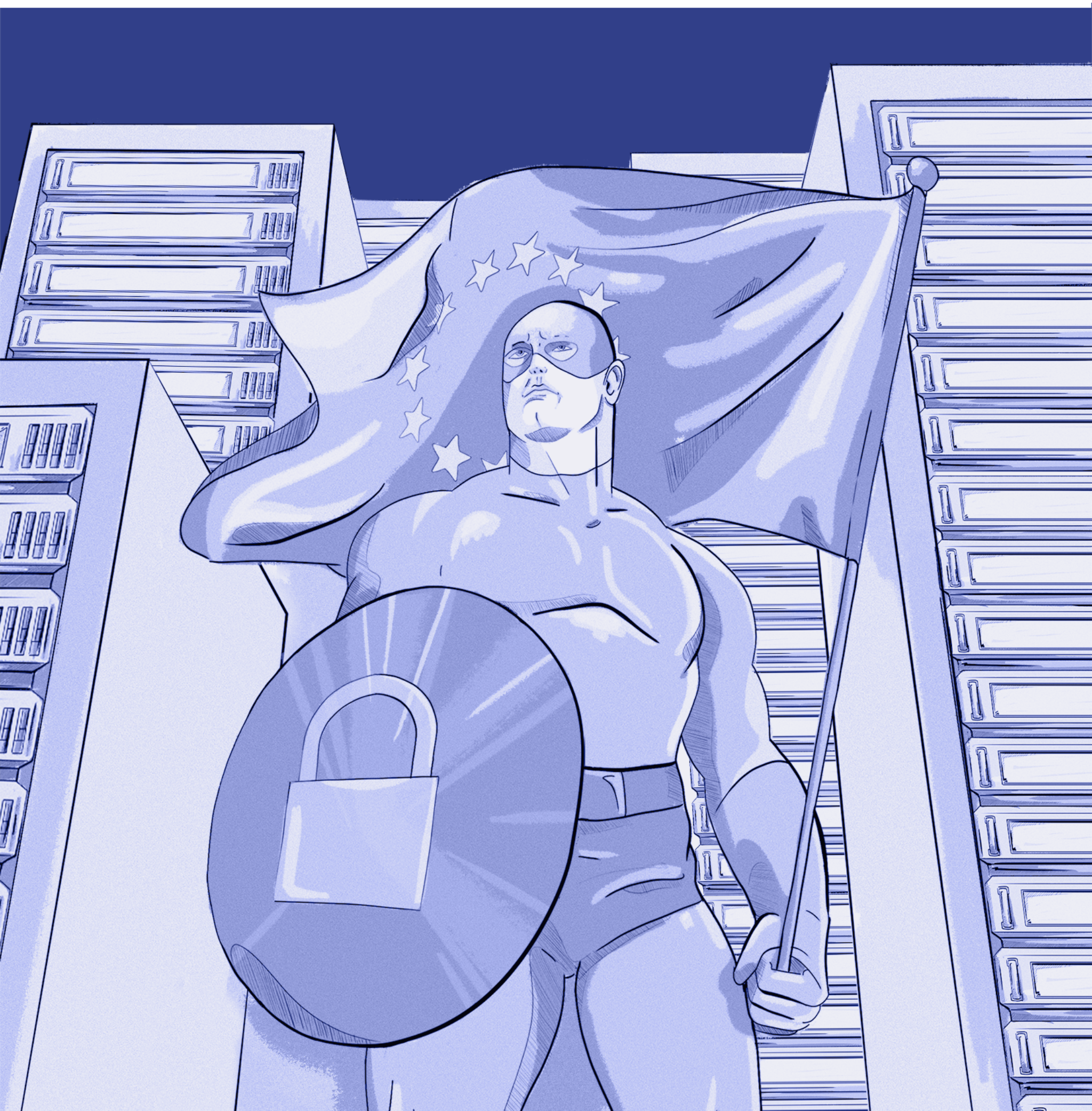
CLEARCODE

GDPR & ePrivacy:
The Effect on AdTech & MarTech From a Technical Perspective



GDPR & ePrivacy: The Effect on AdTech & MarTech From a Technical Perspective

On April 27, 2016, the European Union's General Data Protection Regulation (GDPR) was adopted and triggered the start of a two-year countdown towards its enforcement on May 25, 2018.

During those two years, all companies that collect data about European citizens and residents had to make a number of changes to their policies and agreements with their partners to ensure they comply with the rules outlined in the GDPR.

In addition, there's also the ePrivacy regulation, which is awaiting trialogue (aka trilogue) negotiations between the European Parliament and the European Council and the European Commission

As online advertising and marketing companies collect vast amounts of user data every day, both the GDPR and ePrivacy will have a substantial impact on their business operations.

Much has been written about the GDPR and ePrivacy as well as the legal requirements online advertising and marketing companies must meet in order to become compliant, and rightly so.

However, as the online advertising and marketing industries are powered by technological platforms and processes, the GDPR and ePrivacy will require companies to make changes to the way their AdTech and MarTech platforms operate to comply with these two regulations and adhere to their newly updated policies.

In this guide, we outline the main areas of the GDPR and ePrivacy regulations that will have a direct effect on the online advertising and marketing ecosystem and explain what it means from a technical perspective.

Legal disclaimer: Clearcode is a software development company, not a law firm.
The information provided in this document is designed to provide an overview of the technical implications of the GDPR and ePrivacy and should not be taken as legal advice.

Table of Contents

Table of Contents 2

Information Boxes Used in This Guide 3

What is the GDPR? 4

What is ePrivacy? 5

The Current State of ePrivacy 6

Key Terms of the GDPR 9

Data Subject 9

Data Controller 10

Data Processor 10

4 Main Areas of the GDPR & ePrivacy and What They Mean for AdTech and MarTech From a Technical Standpoint 11

1. Personal Data 11
2. User Consent and User Rights 19
3. Data Breaches 35
4. Data Protection by Design and by Default 38

The Cost of Not Complying With the GDPR 40

The GDPR and ePrivacy Will Fuel Technological Innovation 43

About Clearcode 44

Information Boxes Used in This Guide

Throughout this guide, we've included information taken directly from the official GDPR documentation, current ePrivacy draft, and other related sources.

Blue information boxes represent definitions, recitals, and articles from the GDPR.[1]

Red information boxes represent recitals from the current ePrivacy draft.[2]

Orange information boxes represent information from other sources.

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

[2] Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

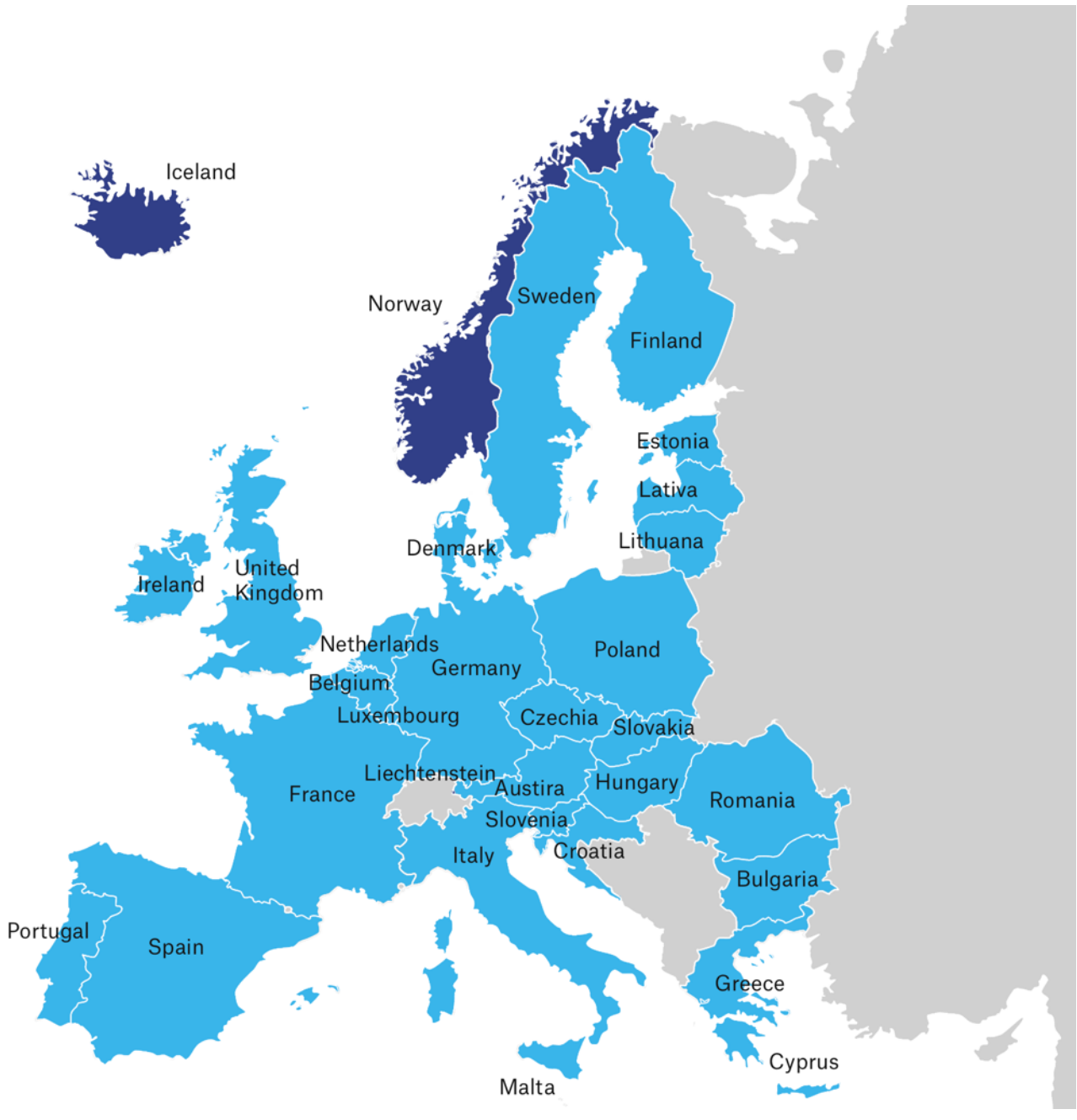
To help make the legal concepts in this guide easier to grasp, we've also included a summary, in simple terms, of each point.

What is the GDPR?

The General Data Protection Regulation (GDPR), or Regulation (EU) 2016/679 as it's known in official contexts, is a regulation spearheaded by the three legislative European Union institutions: the European Parliament, European Commission, and Council of the European Union.

It replaced the Data Protection Directive (Directive 95/46/EC) when it came into force on May 25, 2018.

The goal of the GDPR is to return control to data subjects in the union over their data and make the regulatory environment simpler for international business.



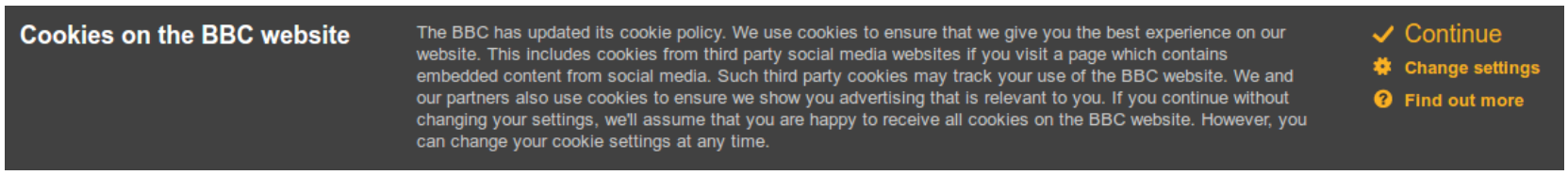
The GDPR aims to protect the data and privacy of citizens and residents of the European Union member states (highlighted in light blue). Even though Norway, Iceland, and Liechtenstein (highlighted in dark blue) are not EU member states, they are European Economic Area (EEA) members and are also included in the GDPR.

What is ePrivacy?

The ePrivacy directive is a piece of EU legislation that also aims to protect the data and privacy of EU and EEA citizens and residents, but with a focus on respecting their private lives when using electronic communications.

Within the online advertising and marketing industries, the current ePrivacy directive is often conversationally referred to as the **cookie law** because it regulates the usage of cookies, among other identifiers. However, it relates to the protection of privacy in the electronic-communications sector as a whole, not just the usage of cookies for online advertising and marketing.

One of the most prominent consequences of the ePrivacy directive (officially known as the Privacy and Electronic Communications Directive, 2002/58/EC) is the cookie-consent notices — also known as **cookie bars** — like the one below from bbc.co.uk:



A common identifier of the current EU ePrivacy directive is the cookie-information banners displayed to EU citizens, which will likely be superseded by a new user-consent form under the GDPR and ePrivacy regulations.

Currently, ePrivacy is a directive, but is in the process of being transformed into a regulation, which will also repeal the current directive.

The new ePrivacy proposal is also known as the Lauristin report, named after the draftee and rapporteur, MEP Marju Lauristin. However, Lauristin's work in the European Parliament has since concluded, so the trialogue (i.e. the discussions between the three legislative EU institutions) will be headed by MEP Birgit Sippel.

Once adopted, ePrivacy will regulate the processes of placing, accessing, and using identification technologies on users' devices based on the broadened definition of personal data as recognized by the GDPR (e.g. cookies, device advertising IDs, and IP addresses).

It is not known when the ePrivacy regulation will come into force as the proposal is set to be be negotiated between the three EU legislative institutions (see below), but it's likely that it will be passed as a law in 2019 or 2020, depending on whether there's a grace period or not.

Given that it is still in progress, the final version of the ePrivacy regulation may still affect how AdTech and MarTech platforms interact with online identifiers based on the GDPR itself and the current state of ePrivacy.

What's the Difference Between the GDPR and ePrivacy?

Both the GDPR and ePrivacy are based on Articles of the EU Charter of Fundamental Rights, a document containing the rights and freedoms protected in the EU.

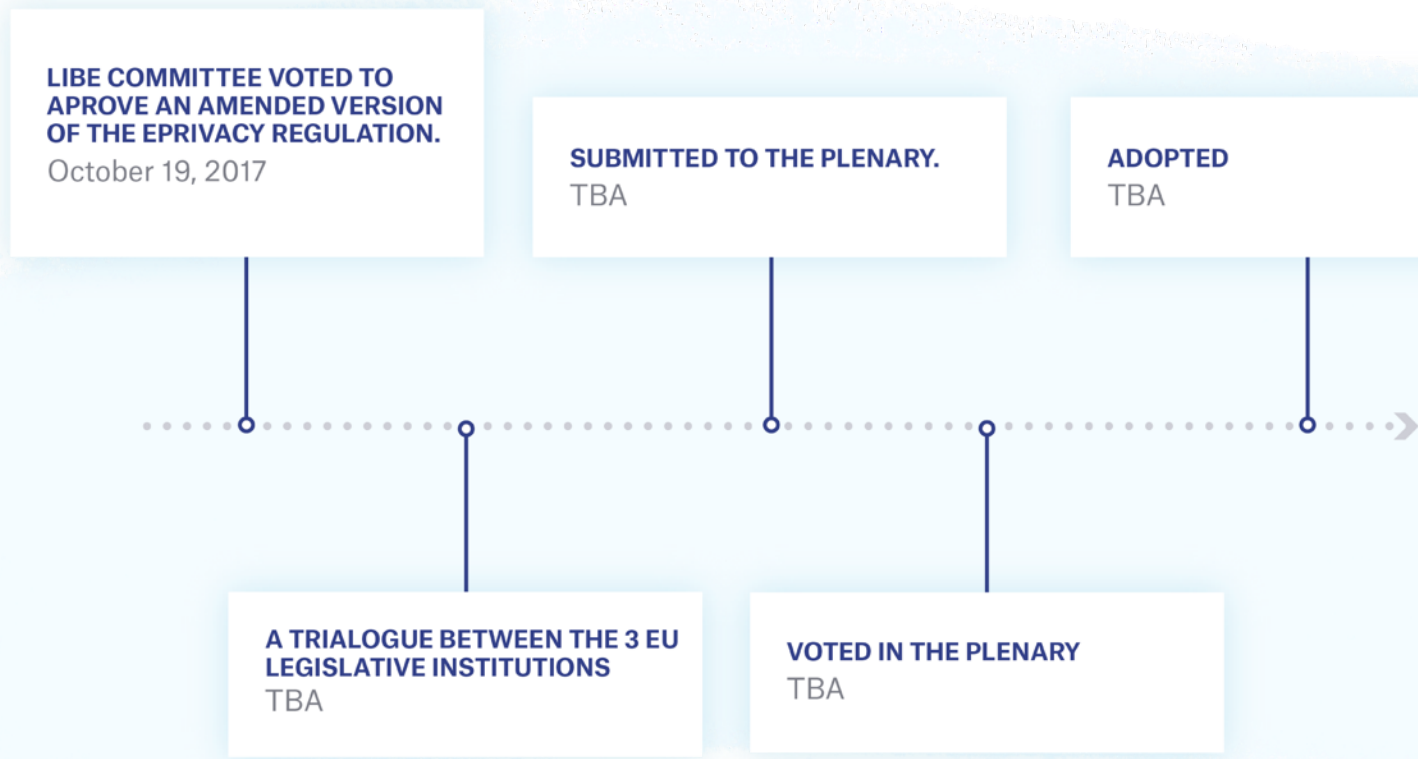
The GDPR is based on Article 8 and relates to the protection of personal data, whereas ePrivacy is based on Article 7 and relates to respect for private life.

In simple terms, the GDPR is focused on data protection, and ePrivacy is focused on the right to respect a data subject's private and family life, home, and communications.

Also, ePrivacy is lex specialis of the GDPR, meaning that when the two regulations cover the same situation, ePrivacy will override the GDPR.

The Current State of ePrivacy

On October 19, 2017, the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs (aka LIBE Committee) voted to approve an amended version of the ePrivacy regulation. This amended version was then approved by members of the European Parliament during a plenary session (a meeting of the whole Parliament).



The next stage involves trialogue negotiations between representatives of the European Parliament, the Council of the European Union, and the European Commission. Once the proposal is finalized and approved by way of voting, it will be adopted and enforced.

In December 2016, a draft of the proposed ePrivacy regulation was leaked, with the first official draft formally released by the European Commission in January 2017. The most recent version of the draft was released in October 2017, with revisions and amendments released in March 2018.

The drafts have been met with some strong opposition from various advertising and marketing organizations, including the Interactive Advertising Bureau Europe (IAB Europe) and Digital Europe — whose members include Google, Apple, Microsoft, and IBM — with their main concerns centered around the lawfulness of data processing based on the notion of legitimate interest. *See the section titled "Processing Personal Data Based on Legitimate Interests" for more information.*

The recent advancement towards adoption spelled a huge blow for advertising and marketing lobbyists. Their last chance at any sort of victory lies with the Council of the European Union and EU member states, which is where their focus will surely be.

What's the Difference Between EU Directives and EU Regulations?

Both EU directives and regulations are designed to achieve a common goal across all EU member states; however, there are a few small differences:

Directives: A directive is a piece of EU legislation that outlines a goal all EU members must achieve. However, it doesn't define the path that each member must follow to achieve it. This provides each member with more flexibility with implementing new laws.

Examples:
Data Protection Directive (Directive 95/46/EC), which was replaced by the GDPR on May 25, 2018.

Privacy and Electronic Communications Directive (2002/58/EC), which will be replaced when the current draft of the new ePrivacy regulation is adopted.

Regulations: A regulation is also a piece of EU legislation that outlines a common EU goal, states the exact path members must follow to achieve the goal, and supersedes any existing laws in EU member states, unlike a directive, which leaves it up to each member state to decide on the path to achieve compliance.

Examples:
The General Data Protection Regulation (EU 2016/679)

Once the current draft of ePrivacy has been adopted, it will become a regulation.

CHAPTER 1

Key Terms of the GDPR

There are a number of definitions located in the GDPR. Below are three key terms that relate to online advertising and marketing: **data subject**, **data controller**, and **data processor.**

Data Subject

> A natural person whose personal data is processed by a controller or processor.

Meaning: Any online visitor.

Examples: EU and EEA citizens and residents.

When we make reference to users or visitors in this guide, we are referring to data subjects in EU member states and the EEA.

Data Controller

> The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Meaning: Any person or company that collects data about EU citizens and residents.

Examples: Publishers, ecommerce stores, individual bloggers, brands, and companies that collect data about users either directly or indirectly via another company.

Data Processor

> A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Meaning: Any person or company that provides services or technology and collects data on behalf of data controllers.

Examples: AdTech and MarTech vendors.

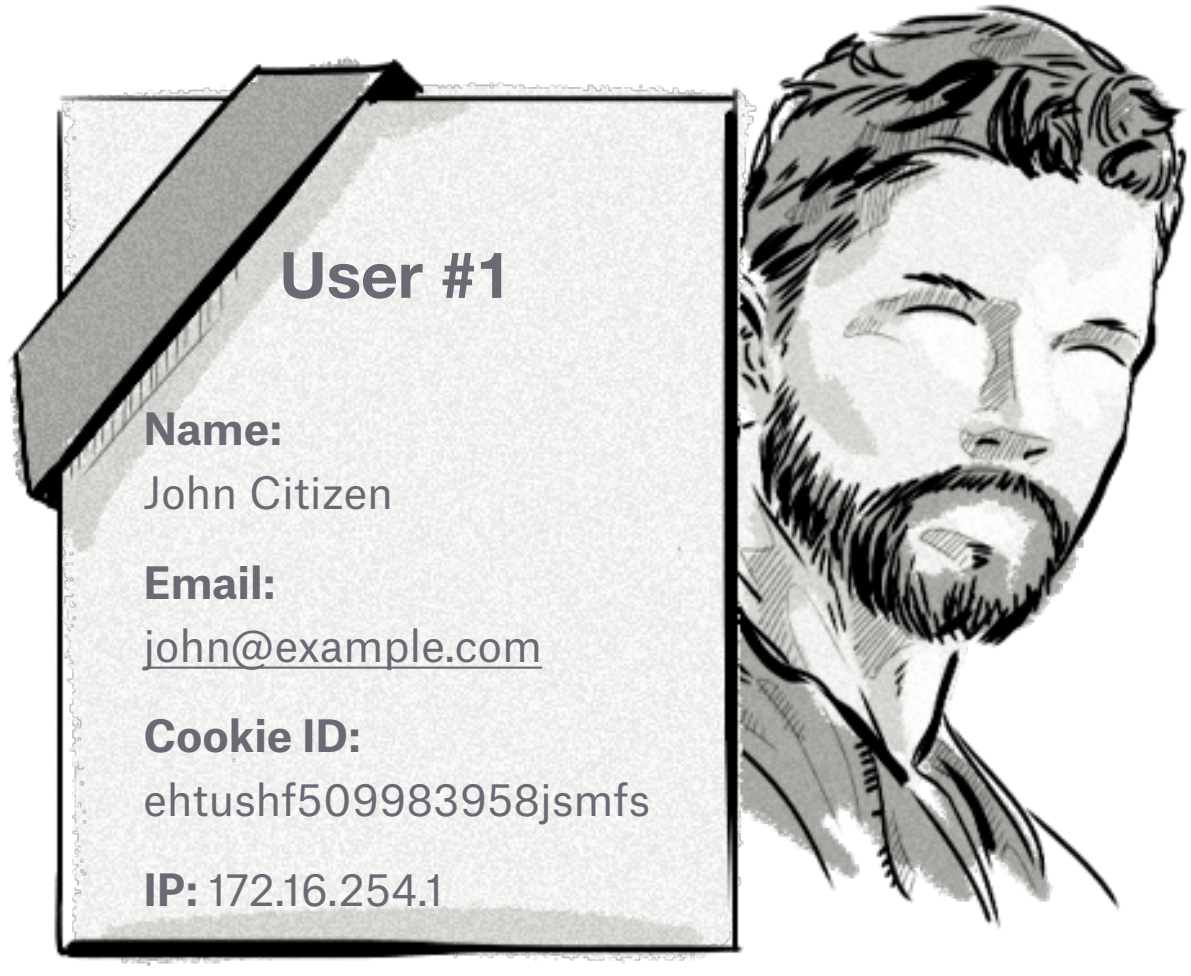
CHAPTER 2

4 Main Areas of the GDPR & ePrivacy and What They Mean for AdTech and MarTech From a Technical Standpoint

Out of all 99 articles and 173 recitals, there are some areas of the GDPR that apply specifically to online advertising and marketing companies.

Below, we outline the four main areas of the GDPR that will have an immediate and substantial effect on digital advertising and marketing companies from a technical standpoint, from brands to technology vendors and publishers.

1. Personal Data



What Does the GDPR Say About Personal Data?

In simple terms:

If a piece of information, either separately or combined with other pieces of data, can be used to identify a person, then it's classed as personal data.

Identity in this sense doesn't just refer to knowing a person's name. It also refers to identification, meaning if a user visits your website or sees one of your ads, they are considered identifiable if you can later recognize them (by identifying and recognizing via their cookie ID or other identifier) if they return to your website or see another one of your ads.

The same principle applies to singling out an individual based on several data points, such as their postal code, gender, and age. In this case, even though you don't know the person's name or have an identifier (for example, a user ID in a cookie assigned to them), you could still potentially identify them.

Official wording:

> 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
>
> Article 4 (1)
> **GDPR**

Typically, AdTech vendors and most MarTech vendors have based their privacy policies on the fact that they are not collecting or dealing with personal data. The reason for this is because up until this point, online identifiers, such as cookie IDs, IP addresses, device advertising IDs, and device fingerprints were not considered examples of personal data.

However, under the GDPR and ePrivacy, essentially any piece of data or information that can in some way identify a person is classed as personal data.

Apart from personal data, the GDPR also refers to two other types of data: anonymous and pseudonymous.

Anonymous Data

Anonymous data means that it can't be used to identify a person, which, for this reason, offers little value to online advertising and marketing companies as they are in the business of identifying people and targeting them with ads and marketing messages.

Due to its inability to identify a person, anonymous data is not subject to the rules of the GDPR, meaning if a company collects anonymous data, they don't have to obtain user consent.

> ...The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not, therefore, concern the processing of such anonymous information, including for statistical or research purposes.
>
> Recital 26
> **GDPR**

Pseudonymous Data

Pseudonymous data refers to data that's been changed into a non-identifiable format, rendering it unable to identify a person without the use of additional data, such as the hashing function or encryption keys.

> 'Pseudonymization' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
>
> Article 4 (5)
> **GDPR**

A Comparison of the 3 Types of Data

Below is a comparison table that provides examples of personal, anonymous, and pseudonymous data.

Type of Information Collected	Personal Data	Anonymous Data	Pseudonymous Data
Device information	AEBE52E7-03EE-455A-B3C4-E57283966239 *Device advertising identifier (e.g. Apple's IDFA -Identifier for Advertising)*	Apple iPhone 7 *Device brand and model*	e69a1078552e13f2734c22322708bd95 *Device advertising identifier* Using a one-way hash function to convert the data into a non-identifiable format. The device can be re-identified by applying the same hash function to the original value and comparing it to the pseudonymous hash
Email address	john.smith@company.com *Email address*	company.com *Domain of the email address*	1bc5edb4799fd8eec67c66122f47eb73 *Email address* Similar to the advertising identifier, the output of the one-way hash function.

Type of Information Collected	Personal Data	Anonymous Data	Pseudonymous Data
Web activity (e.g. pageviews)	213.86.17.58 https://clearcode.cc/ https://clearcode.cc/about/ https://clearcode.cc/contact/ (URLs visited) *A list of page URLs visited on a website along with an IP address of the visitor.*	500+ pageviews http://clearcode.cc/about/ *An aggregated number of times a given page was viewed* https://clearcode.cc/ https://clearcode.cc/about/ https://clearcode.cc/contact/ (URLs visited) *A list of the page URLs visited on a website without containing cookie IDs, IP addresses, or any other personally identifiable information.*	8d61a1f53fdc1b74.1495187199.51.1505818713.1505817299. https://clearcode.cc/ https://clearcode.cc/about/ https://clearcode.cc/contact/ (URLs visited) *A list of page URLs visited on a website along with a randomly generated unique identifier that has been set in the visitor's browser cookie.*
Address and DOB	742 Evergreen Terrace Henderson, NV 8901 USA *Address* November 24, 1971 *Date of birth*	89** *Suppressing certain parts of the data, e.g. removing the last two digits of a postcode.* 45-54 *Age range instead of the exact age.*	1971 NV 8901 *The year of birth and a postal code.* By using an external database, a data subject can be re-identified, hence the data cannot be considered anonymous.

From the table above, it appears that anonymous data is the least likely to expose the identity of a data subject.

While that is true in most cases, it's important to keep in mind that the anonymized data could still be linked to an individual if enough pieces of data are combined together. For example, having a single data point, like an age range of 40–50, out of a sample size of 1,000 couldn't be linked to an individual, but when you add in other anonymized data sets (e.g. postcodes and the year of birth) and combine with other sets of data (e.g. public records or data), it can easily become personal data and could be used to identify an individual.

There have been a number of situations of this in the past, with one example being Netflix's 2006 contest in which the company put up a $1 million prize for the person or team who could significantly improve their recommendation algorithm. As part of the content, Netflix released 10 million movie rankings by 500,000 customers, which included the following information:

- A unique subscriber ID
- Movie title
- Year of release
- The date on which the subscriber rated the movie

Even though personally identifiable information, such as customer name, was replaced with a unique ID, two researchers at the University of Texas at Austin, Arvind Narayanan and Vitaly Shmatikov, were able to de-anonymize some of the data and identify certain users by comparing user ratings and the date on which they rated the movies with information from the site Internet Movie Database (IMDB).

A Side Note About Sensitive Data

The GDPR also includes another type of data class: sensitive data.

Examples of sensitive data include religious or philosophical beliefs, racial or ethnic origin, political opinions, trade-union membership, and data concerning health, sex life, and sexual orientation.

Sensitive data is typically not collected by advertisers or marketers as it requires stronger grounds for processing and is subject to additional protections, meaning the payoff just isn't viable. Advertisers and marketers wishing to collect, store, and use sensitive data should be aware that they will need to obtain explicit consent from the data subject.

What Does This Mean for AdTech and MarTech From a Technical Perspective?

The definition of personal data is somewhat unchanged from the definition given in the Directive; however, it broadened the scope of the data-protection law. One example of the change in scope is that the GDPR now considers online identifiers and location data as personal data.

As most online advertisers, marketers, and publishers collect and use online identifiers, such as those mentioned above, as well as location data, they will now have to take additional steps to ensure they are compliant with the GDPR's rules regarding the collection, storage, and usage of personal data.

Examples of personal data include:

- Names
- Email, home, and work addresses
- Phone numbers
- Cookie IDs (visitor identifiers stored in cookies)
- IP addresses
- Device IDs
- Device fingerprints

The GDPR states that companies collecting personal data should implement measures to ensure the data is protected at all times, via encryption and pseudonymization, for instance. Although most companies already do this with obvious examples of personal data, such as emails, phone numbers, and IP addresses, they now have to apply this to all types of data they collect.

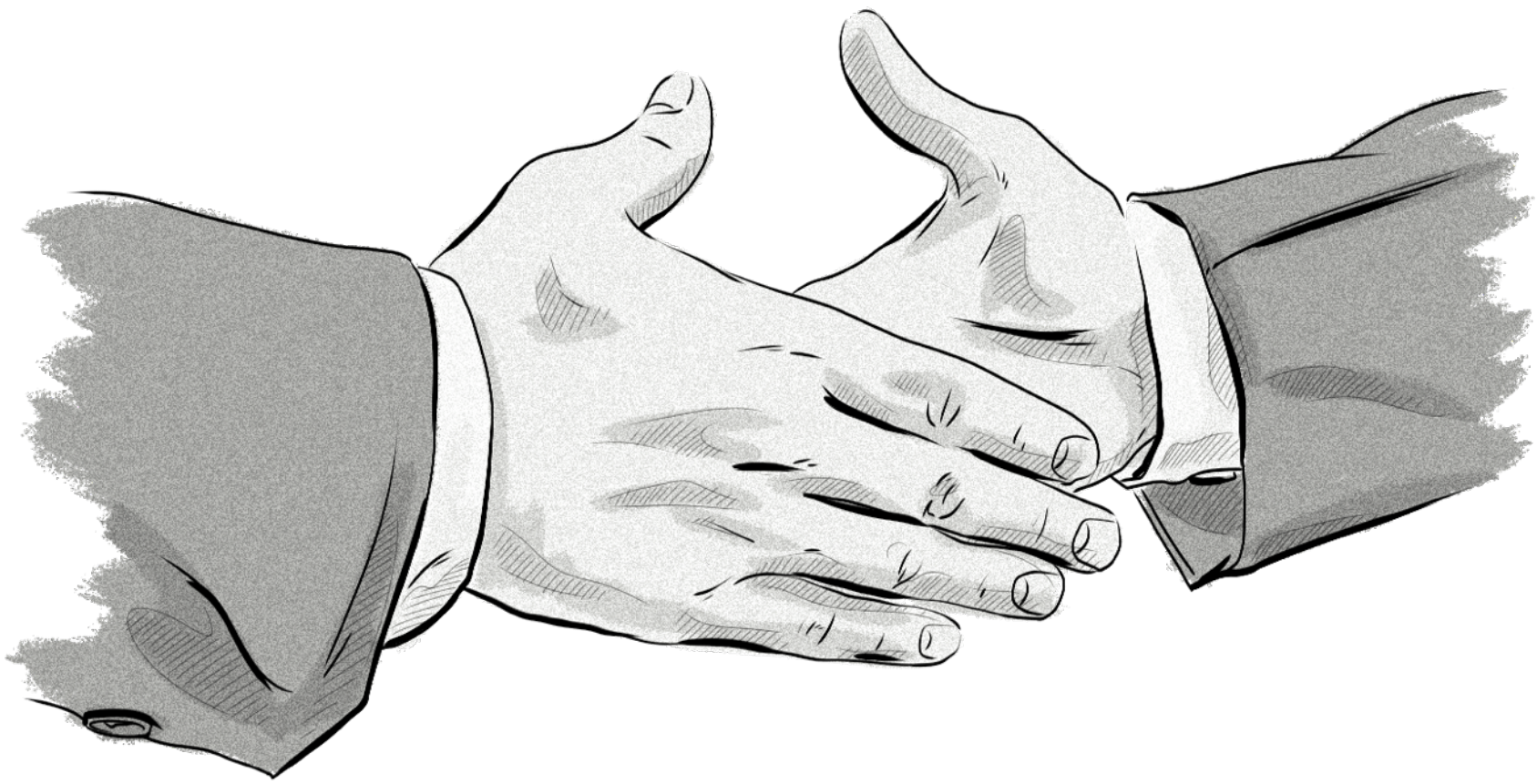
While these measures will help online advertising and marketing companies mitigate risks associated with data security, encrypted and pseudonymized data are still classed as personal data, meaning companies still have to obtain user consent and carry out various data-protection measures if they wish to collect and use the information.

The main challenges advertising and marketing companies face with personal data are collecting it in the first place (i.e. obtaining consent), ensuring its security, and creating a chain of responsibility with their partners when they exchange with them.

The real test for both the AdTech and MarTech industries will be to update their current platforms so they can anonymize and pseudonymize data to meet their data-protection obligations, and create future-proof businesses that allow clients to run effective and successful advertising and marketing campaigns that respect user privacy and limit their exposure to the GDPR and ePrivacy regulation.

2. User Consent and User Rights

User Consent



What Does the GDPR Say About User Consent?

In simple terms:

Companies operating in the online advertising and marketing industries need to be completely upfront with online users about what they plan to do with their data, with whom they wish to share it, and how long they'll keep it for, while at the same time getting clear agreement from online users to collect their data.

Official wording:

> Consent should be given by a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

> This could include ticking a box when visiting an internet website, choosing technical settings for information society services, or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes, or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise, and not unnecessarily disruptive to the use of the service for which it is provided.
>
> Recital 32
> **GDPR**

The GDPR and ePrivacy draft make it pretty clear that if companies want to collect personal data from users, use it to track their behavior around the web, display ads based on their data, and trade or sell it to other companies, they will have to get consent from the user before they can do so.

Also, publishers **won't be able to deny users access to their website** if they don't provide consent or refuse to consent to the specified purposes, for example, using their data for online behavioral advertising (OBA), like some do now when they detect the user is employing ad-blocking software. On a side note, it's unclear at the moment whether these anti-ad-blocking tactics (i.e. when publishers deny users access to their content if they detect ad-blocking software) are illegal, but it will likely become a hot topic in the near future.

What do companies need to do with the data they collected prior May 25, 2018?

To add further insult to injury, apart from obtaining proper consent from May 25, 2018, data controllers need to analyze whether the user data they had in their databases (e.g. CRM systems, DMPs, and DSPs) prior to May 25, 2018, was collected according to the rules set out in the GDPR.

> Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation.
>
> Recital 171
> **GDPR**

For marketers, this means obtaining permission again from data subjects in their existing databases if they hadn't done so via the GDPR's rules regarding consent, which is highly unlikely. For the most part, this involves sending out, most likely via email, a GDPR-compliant consent request asking data subjects to re-consent to usage of their historic data.

For advertisers, on the other hand, this process of re-consenting is much tougher due to the indirect relationship they have with users who are exposed to their ads — just think about all the cookies advertisers collect via processes such as cookie syncing. The solutions to this conundrum are quite extreme, ranging from mass deletion of user data to doing nothing at all, with the latter being the least attractive and subject to severe financial consequences. *See the section titled 'The Cost of Not Complying with the GDPR' for more information.*

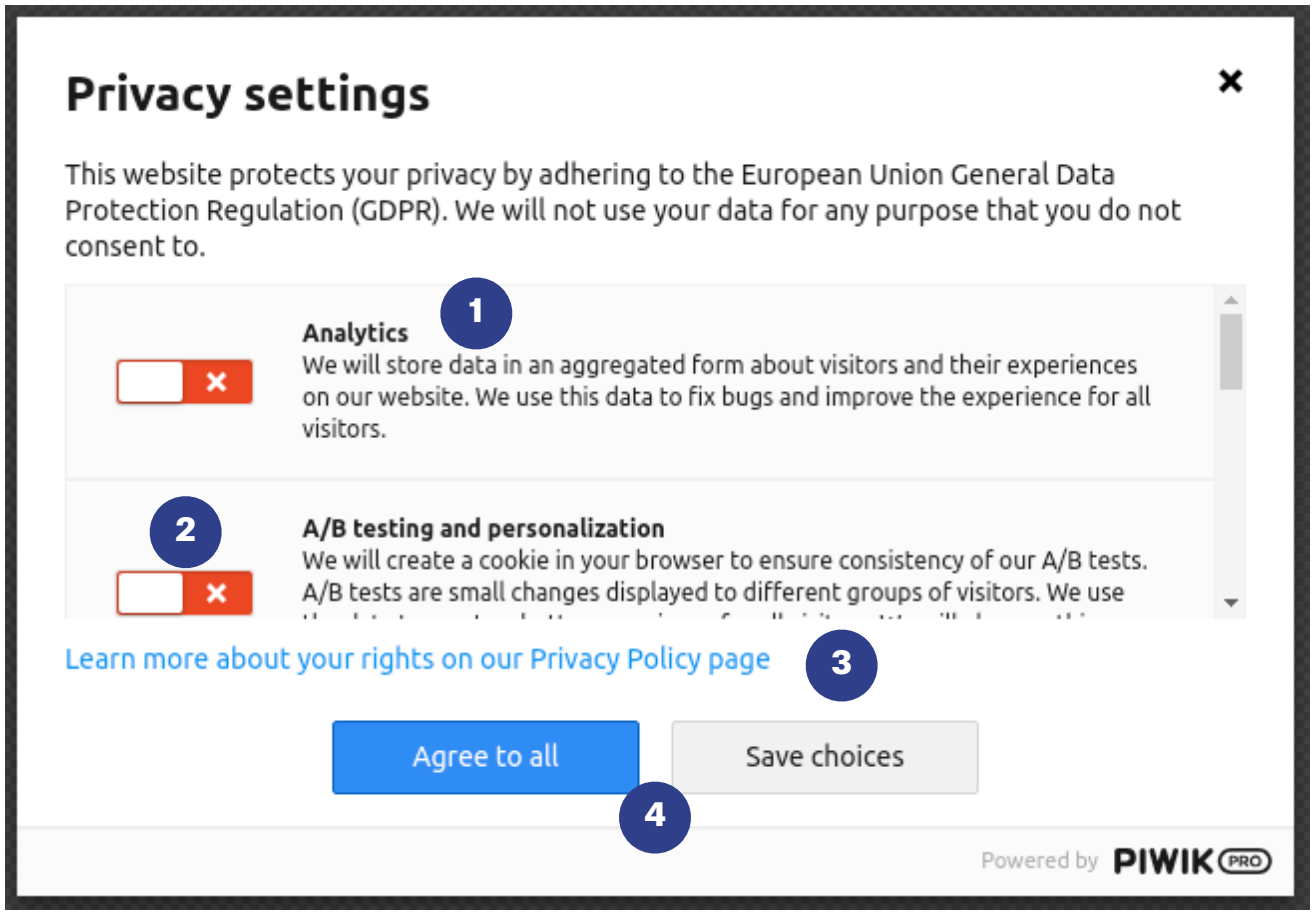
For AdTech/MarTech vendors and advertisers wanting to run targeted campaigns (e.g. online behavioral advertising and retargeting campaigns) based on personal data, obtaining user consent is paramount, because without it, no advertising or marketing company will be able to collect, use, or store user data.

An Example of a GDPR-Compliant User-Consent Form

The most obvious way of obtaining a user's consent is by asking them via a popup of some sort, similar to the cookie bars that you see on EU-based websites, but with a few key differences.

Below is an example of the type of user-consent request form publishers could use to obtain user consent.

The message in the form is based on the recitals and articles listed in the official GDPR document and the ePrivacy draft.



Source: Piwik PRO Consent Manager, www.piwik.pro

The Anatomy of a User-Consent Form

1. A clear and unambiguous message explaining the purpose of the data collection.
2. Settings that require users to opt in (i.e. make the user opted out by default)
3. A link to the tool that allows the user to manage their consent decisions and exercise their rights.
4. A choice to agree or disagree to their data being collected.

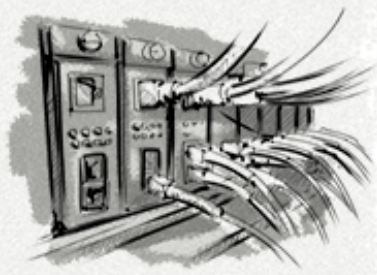
Relevant recitals and articles from the GDPR regarding user consent: Recital 32, recital 65.

There are three possible outcomes for any given user:

- **Consent given:** The user gave their consent (selects Agree to all or opts in to individual purposes and then selects Save choices).
- **No consent given:** The user refused to give consent (selects Save choices).
- **No answer given:** The user hasn't stated whether they accept or reject (closes the consent form). This inactivity does not constitute consent.

DATA SUBJECT
Website visitor

DATA CONTROLLER
Publisher

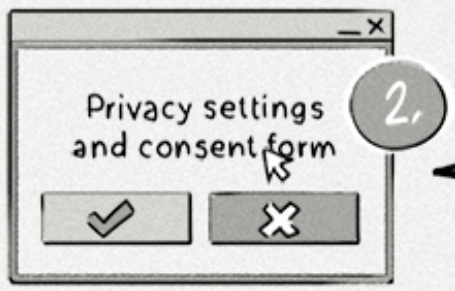


DATA PROCESSOR
AdTech/MarTech vendor

A user accesses the data controller's website

WEB SERVER

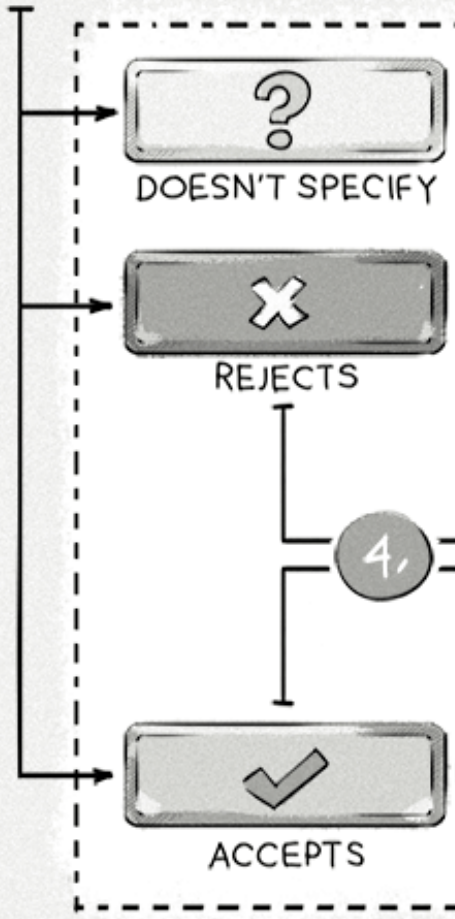
The website renders in the data subject's browser.



Show the consent request form to collect and use the data subject's data for a specific purpose(s) (e.g. personalization and retargeting).

Ask again (non-intrusively, e.g. via a sticky notification bar).

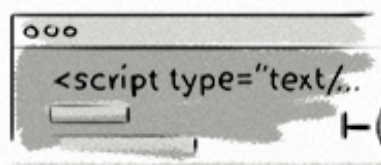
3.



The controller can take no further action towards collecting the user's data.

CONSENT MANAGER

Store the status of the consent and keep a record of the user's decision in the data controller's systems.



6.

Fire all relevant tags based on the processing activities listed in the user consent form.

ADTECH/MARTECH PLATFORM

The data is collected and processed on behalf of the data controller.

Here's a basic example of how the process would look when a user accesses a website where a company (data controller) wants to collect and use their data via AdTech/MarTech platforms (data processors).

This new form of obtaining user consent is in direct contrast to the cookie bars under the current ePrivacy directive, which allow websites to simply inform users about the use of cookies. Not only is this cookie-bar method completely ineffective at introducing any sort of data protections or improving user privacy, as it allows for data to be leaked and shared without the users' knowledge, but it also creates a poor user experience.

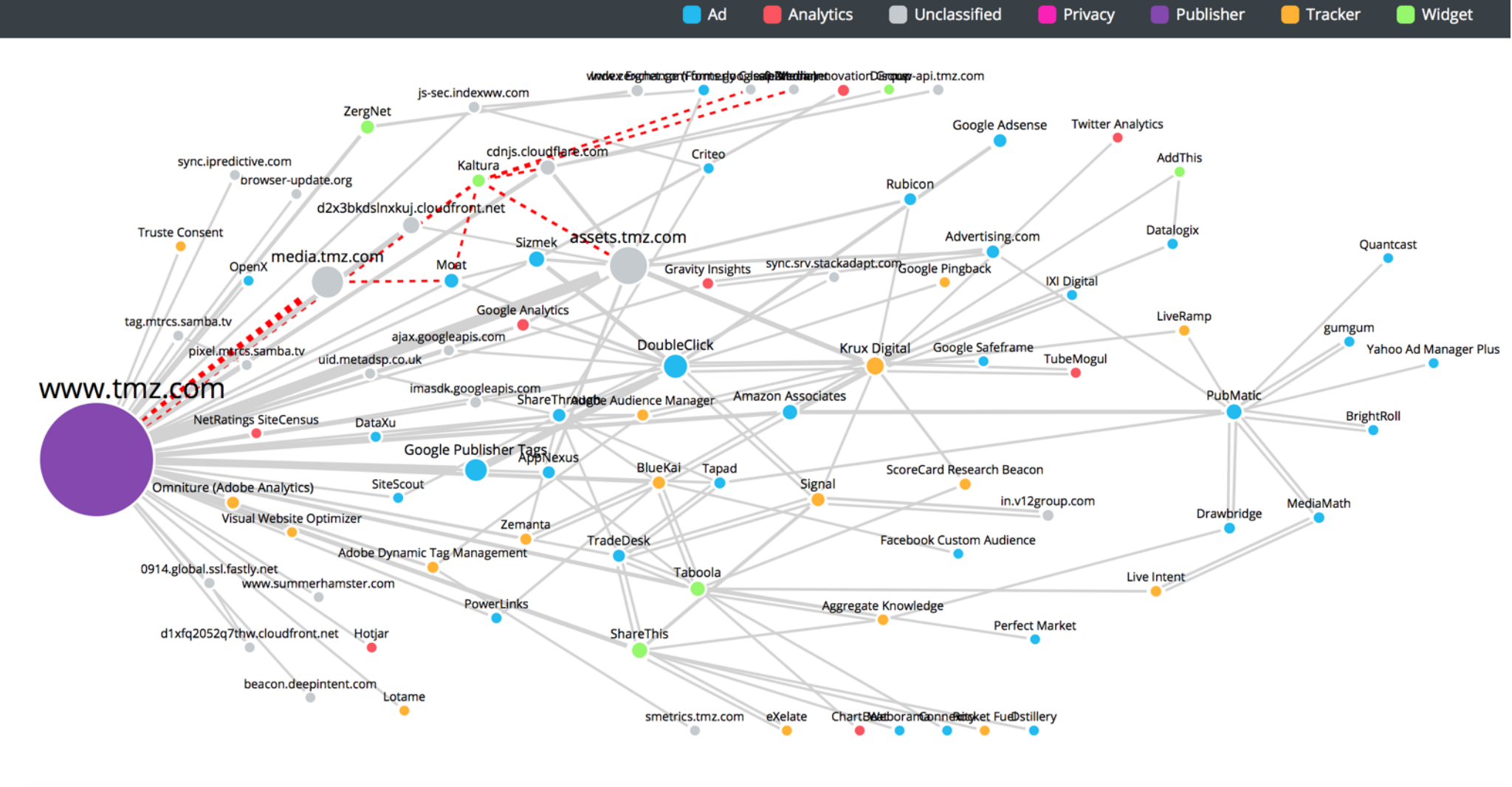
> This Regulation should prevent the use of so-called 'cookie walls' and 'cookie banners' that do not help users to maintain control over their personal information and privacy or become informed about their rights.
>
> Recital 22
> **Current ePrivacy draft**

The current draft of the ePrivacy regulation will require data subjects to clearly specify which option they choose, and even if they don't state their preferences, their inactivity won't be classed as consent.

Obtaining User Consent in the Current Programmatic Ecosystem Is a Real Conundrum

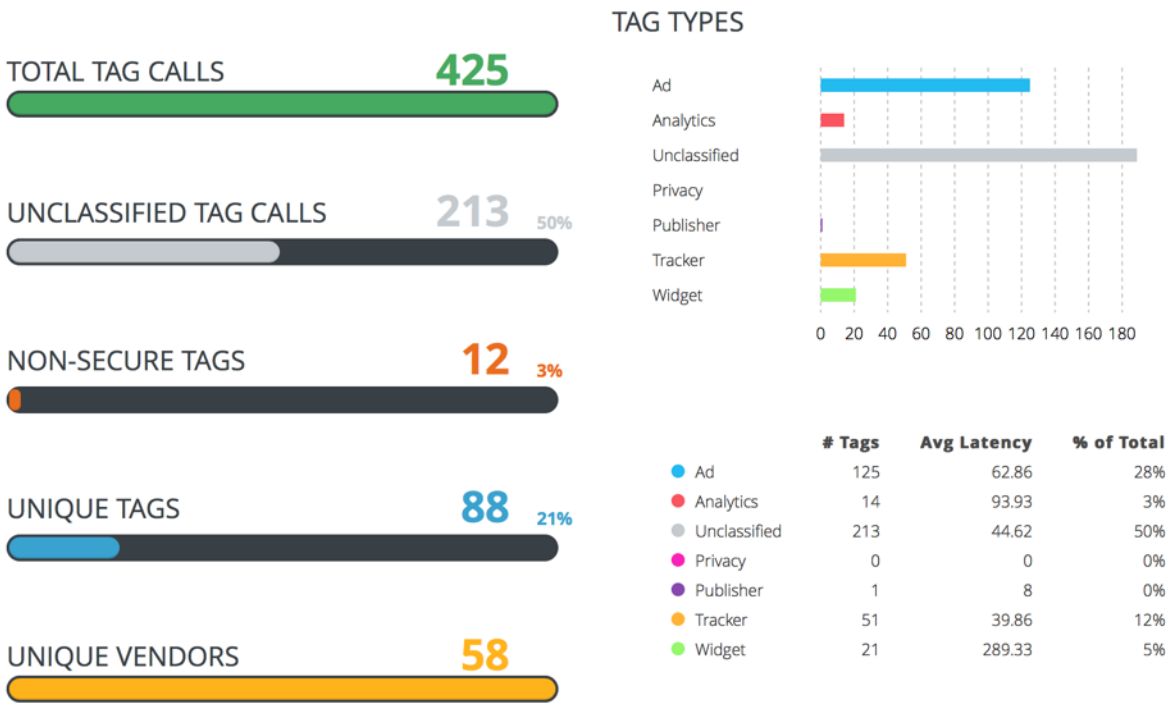
The process of obtaining user consent for each partner a publisher works with is made even more challenging by the sheer number of third-party tags most medium- to large-sized publishers run on their sites.

As an example, the images below illustrate how many third-party tags are running on the popular celebrity-news site, TMZ.



A visual illustration of the number of third-party tags found on tmz.com.
Source: https://www.evidon.com/resources/trackermap-samples/

In the eyes of the GDPR and ePrivacy regulation, publishers are liable for all scripts, tags, and pixels on their websites, including third-party ones. Therefore, as part of their compliance program, they'll need to have certain agreements with their partners, such as a data processing agreement (DPA).



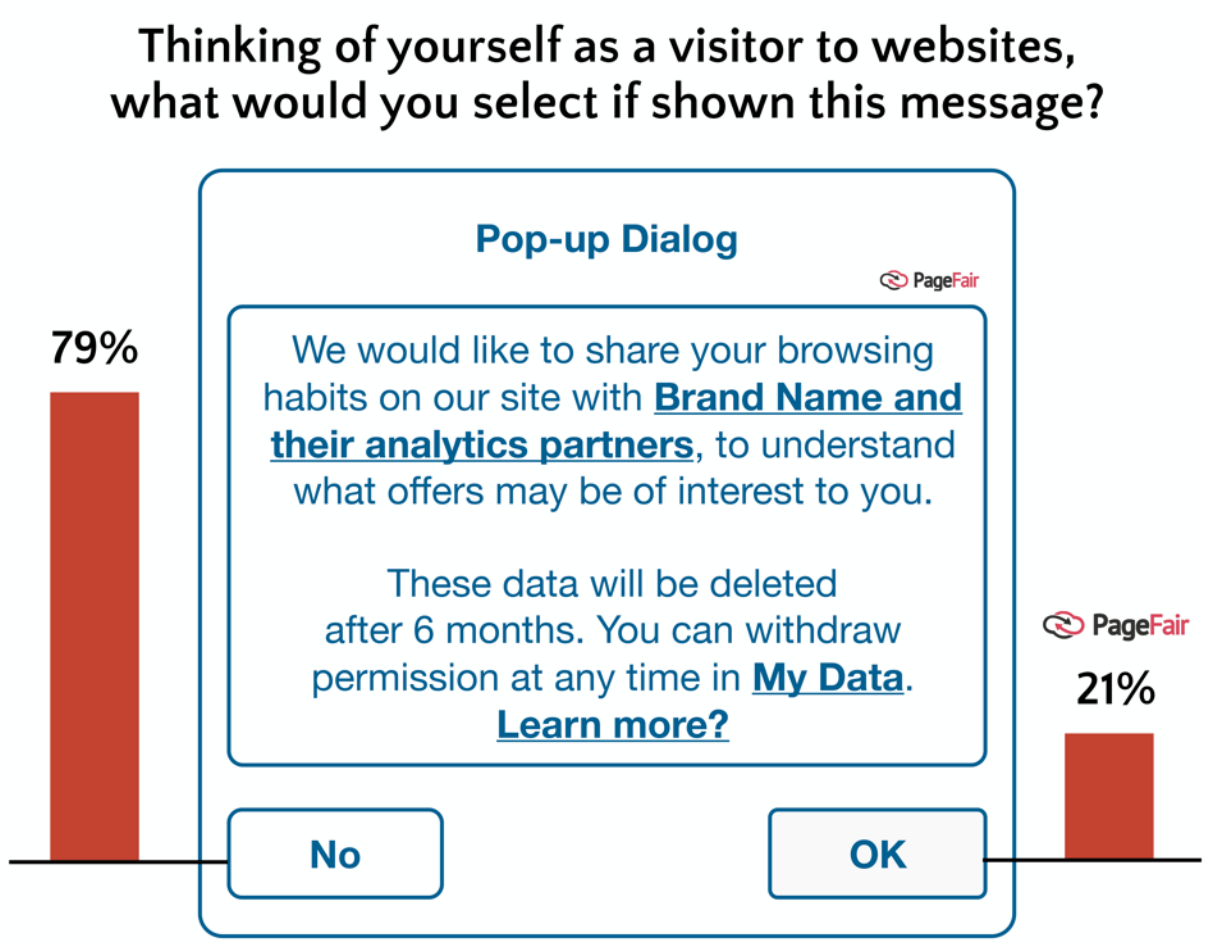
An *overview of the type of digital technologies found on tmz.com.*
Source: https://www.evidon.com/resources/trackermap-samples/

These third-party tags include ad tags, analytics tags, and widgets, all of which can be used to track a user's behavior on TMZ and across the web on other sites. It's not uncommon for publishers, especially large ones, to have this many trackers on their site.

Under the GDPR and ePrivacy regulation, if a publisher wants to collect and share a user's data with third-party companies and software vendors (e.g. AdTech and MarTech companies), they will have to get clear consent from the user, explain the purpose of the collection, and list the names of the companies involved in the collection process.

If we use the above image as an example, then in this particular case, the publisher would have to ask the user for consent to collect their data on behalf of 58 different companies (because there are 58 unique vendors) and update their cookie policies to match this.

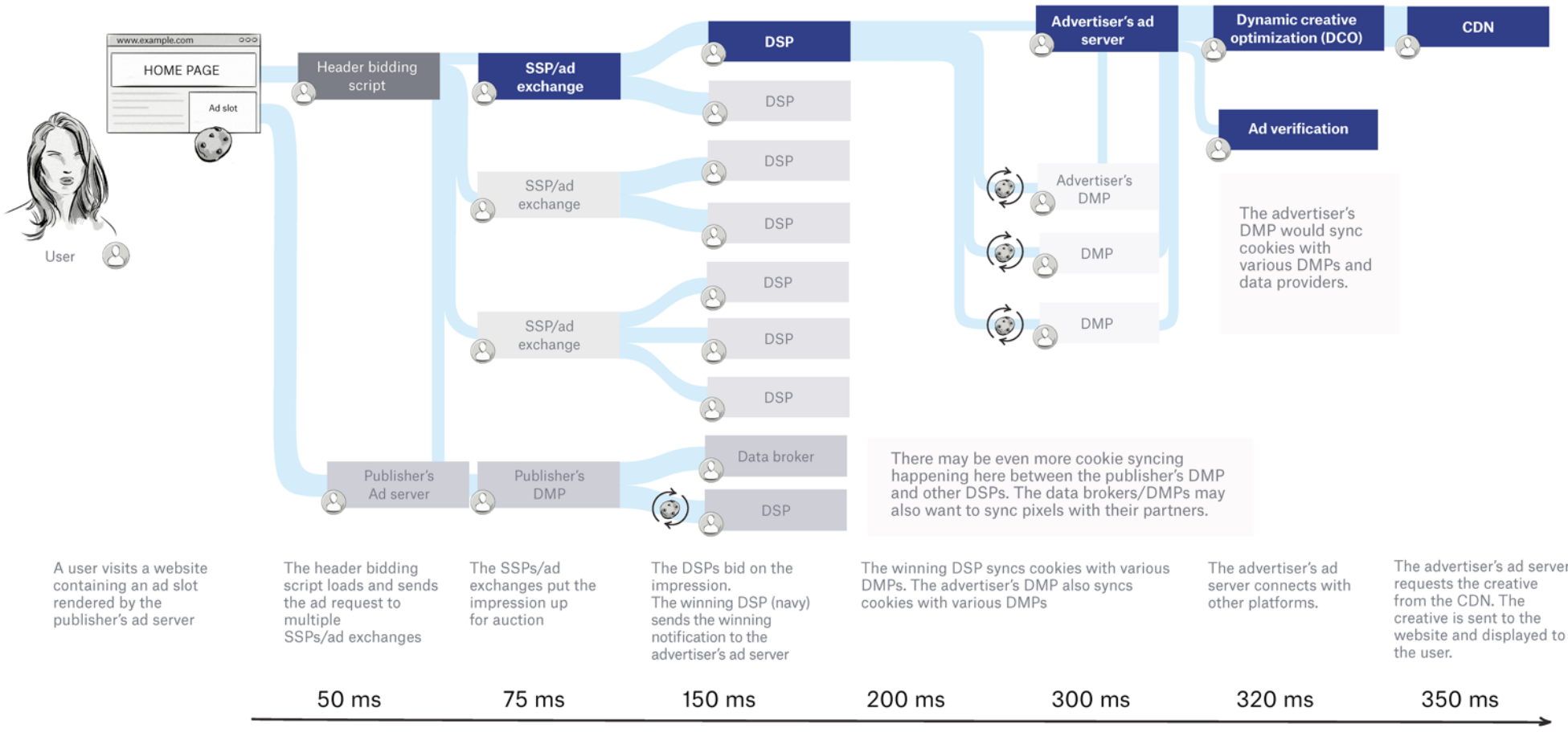
Not only would this produce a terrible user experience, but according to a study released by PageFair in September 2017, it's also likely to be refused by the user.



PageFair surveyed 300+ publishers, AdTech, brands, and various others, on whether users will consent to tracking under the GDPR and the ePrivacy Regulation.
Source: *Research result: what percentage will consent to tracking for advertising? PageFair, September 12, 2017*

The above results from the PageFair survey paint a pretty grim picture of the online advertising and marketing world after May 25, 2018. However, despite the many challenges, there are numerous opportunities. *See the section titled 'The GDPR and ePrivacy Will Fuel Technological Innovation' for more information.*

In addition to the challenges surrounding obtaining user consent on behalf of dozens of vendors, there's also the issue of data leakage in real-time bidding (RTB) auctions.



The image above illustrates how user data is shared (aka leaked) to various platforms during an online media transaction. Under the GDPR, each platform in the diagram has to obtain consent from the user to collect and process their data — something that will prove incredibly challenging for all AdTech vendors and agencies.

User Consent via Browser Settings

Apart from the new conditions for obtaining user consent, the EU Commission has also suggested a new mechanism for identifying a user's data-collection preferences, which are outlined in the ePrivacy draft.

Here are a few of the key points in the ePrivacy draft that refer to a user setting their privacy preferences via the browser, or a similar tool:

The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers thus helping end-users to prevent information from their terminal equipment (for example, smartphone, tablet, or computer) from being accessed or stored.

Recital 20
Current ePrivacy draft

Recital 20 of the current ePrivacy draft is essentially saying that instead of using popups to ask for consent, web-browser vendors should implement some sort of setting that will allow users to set their consent preferences at the browser level.

However, as this is simply a recommendation by the EU Commission, there is no guarantee that browser vendors will implement these privacy settings.

What the industries really need, with regard to process of obtaining consent, are standards all parties can mutually agree upon. Currently, there are no such standards, but it’s likely they will emerge in the future.

To be on the safe side and in compliance for the time being, publishers should implement their own mechanism for collecting user consent for activities where the user's data is passed on to third parties, such as for tracking and behavioral targeting. In this situation, a tag manager would prove useful in managing this process.

Processing Personal Data Based on Legitimate Interests

Apart from the topic of obtaining user consent for processing personal data being referenced throughout the GDPR, there is also a reference to something called **legitimate interests:**

> Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
>
> Article 6, 1(f)
> **GDPR**

More information about legitimate interests can be found in recital 47, which finishes with this sentence:

> ...The processing of personal data for direct-marketing purposes may be regarded as carried out for a legitimate interest.
>
> Recital 47
> **GDPR**

Many people within the online advertising and marketing industry have interpreted this to mean that AdTech and MarTech companies will be able to collect data without obtaining user consent on the grounds of legitimate interests.

However, it is not yet known if this **legitimate-interests** area will apply to the business operations that are currently carried out by advertising and marketing companies, such as online behavioral advertising and retargeting. Given the amount of data that flows through the online advertising ecosystem without the user's knowledge, it is highly unlikely.

Also, there are a couple of references to the legitimate-interests concept from the Article 29 Data Protection Working Party and the ePrivacy regulation draft that eliminate any hope advertisers or marketers had regarding collecting user data without consent based on legitimate interests:

1. The Article 29 Data Protection Working Party, which will become the European Data Protection Board (EDPB) with the enforcement of the GDPR, had this to say in Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" about using the concept of legitimate interest for data processing:

> ...This does not mean that controllers would be able to rely on Article 7(f) to unduly monitor the online or offline activities of their customers, combine vast amounts of data about them from different sources that were initially collected in other contexts and for different purposes, and create—and, for example, with the intermediary of data brokers, also trade in—complex profiles of the customers' personalities and preferences without their knowledge, a workable mechanism to object, let alone informed consent. Such a profiling activity is likely to present a significant intrusion into the privacy of the customer, and when this is so, the controller's interest would be overridden by the interests and rights of the data subject.
>
> **Article 29 Data Protection Working Party**

This essentially means that if advertising and marketing companies wanted to continue using the same data-collection and usage processes they do today, they will need to get consent from the user to do so.

However, Opinions from the Article 29 Data Protection Working Party are non-binding in EU law, but under their new role of EDPB, they will become a more prominent body. For now, this Opinion from Article 29 WP should be taken as a sign of things to come.

Techniques that surreptitiously monitor the actions of users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the users' terminal equipment **pose a serious threat to the privacy of users.** Therefore, **any such interference with the user's terminal equipment should be allowed only with the user's consent and for specific and transparent purposes.** Users should receive all relevant information about the intended processing **in clear and easily understandable language.** Such information should be provided separately from the terms and conditions of the service. **Terminal equipment of users of electronic communications networks and any information relating to the usage of such terminal equipment**, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, **are part of the private sphere of the users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms.** Given that such equipment contains or processes very sensitive data that may reveal details of the behavior, psychological features, emotional condition, and political and social preferences of an individual, including the content of communications, pictures, **the location of individuals by accessing the GPS capabilities of the device, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection.** Information related to the user's device may also be collected remotely **for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these users.** Furthermore, **so-called spyware, web bugs, hidden identifiers, and unwanted tracking tools** can enter users' terminal equipment without their knowledge in order to gain access to information or to store hidden information, to process data and use input and output functionalities such as sensors, and to trace the activities.

Amended Recital 22
ePrivacy draft, October 2017

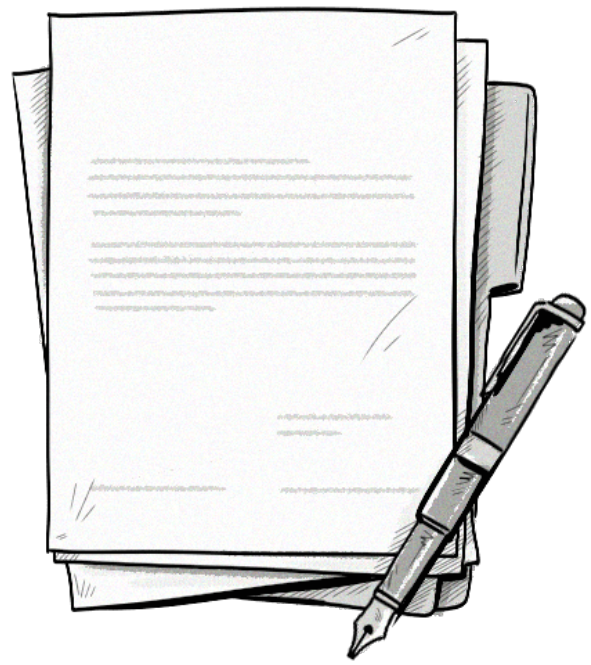
The above recital essentially means that if advertising and marketing companies want to collect their data by using many of the identification and tracking methods they use today (e.g. device fingerprinting and third-party trackers), then they are required to inform users about this directly and obtain their consent to do so.

As mentioned earlier, various advertising and marketing lobbying groups are pushing for the inclusion of legitimate interest to be included in the final version of the ePrivacy regulation. The reason they are lobbying comes down to this:

Currently, the ePrivacy draft doesn't mention anything about the lawfulness of data processing based on the notion of legitimate interest; it's only mentioned in the GDPR. In order for advertising and marketing companies to collect and process data lawfully without the need for consent, the final ePrivacy regulation needs to contain a section about this and state that data collection and processing for advertising and marketing purposes is classified as a legitimate interest.

However, even if your company wishes to rely on the legitimate-interests concept and not ask for consent when collecting data, which is highly risky and could prove extremely costly (see the section titled *'The Cost of Not Complying with the GDPR'* for more information), it does not change the fact that you will still need to fulfill all the other obligations mentioned in this guide, as you'll still be dealing with personal data.

User Rights



What Does the GDPR Say About User Rights?

In simple terms:

The GDPR has given users a number of rights relating to their data and states that companies will need to allow users to exercise these rights without delay (within one month).

Official wording:

> Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.
>
> Recital 59
> **GDPR**

Specifically, users have the following rights under the GDPR:

The right to be informed about the existence of profiling, the consequences of such profiling, the processing operation, and its purposes.

The right to access confirmation from the controller as to whether or not personal data concerning them is being processed. *This right was already part of the Data Protection Directive.*

The right to rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

The right to erasure ("right to be forgotten") of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.

The right to restrict processing if the accuracy of the personal data is contested by the data subject, the processing is unlawful, and the controller no longer needs the personal data for the purposes of the processing.

The right to data portability, meaning they have the right to receive personal data that's been collected about them by a controller. The data must be in a structured, commonly used, and machine-readable format.

The right to object at any time to processing of personal data concerning them.

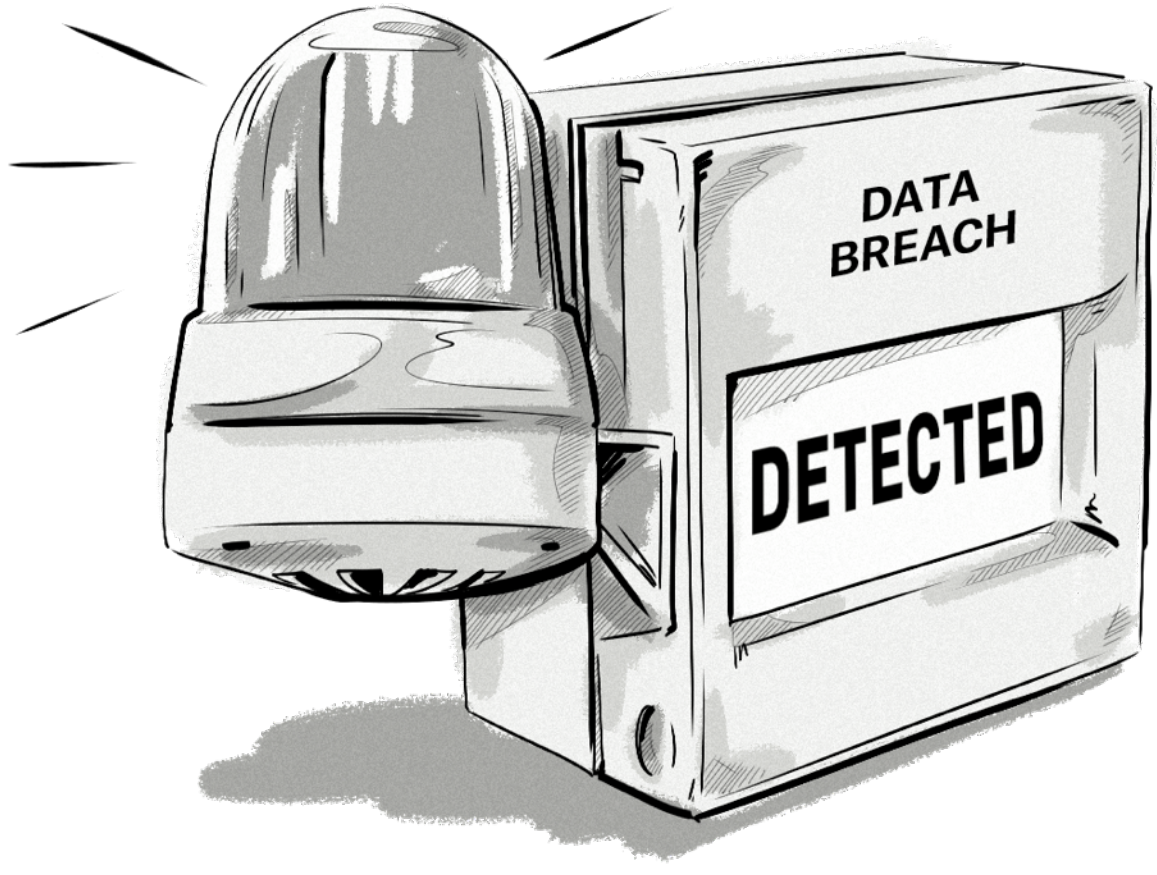
What Does This Mean for AdTech and MarTech From a Technical Perspective?

All companies that have a website, from brands to publishers, not only have to implement a user-consent popup, or something similar, to gain voluntary consent from online users, but they also have to store and manage these consent requests, which, depending on the size of the company, could be a few thousand or tens of millions.

In addition, companies have to implement technological changes that:

- Identify users and their consent decisions, and then take the appropriate actions based on them — for example, fire tags to pass data to certain platforms and tools (based on the purposes outlined in the consent request, of course), or refrain from firing tags.
- Provide users with a current status of the activities they've consented to and allow them to exercise their rights (listed above) within one month from the time of request.
- Set the data to expire within a certain timeframe — e.g. six months from the time the user accepts the request.
- Pass the user's consent decision to all parties involved in the consent request — e.g. if a publisher asks a user if they, their AdTech partner, and the AdTech partner's client can use their data for advertising, then the user's decision will need to be sent to all those parties. This is particularly challenging in online advertising, as for any given ad request, a user's information could be accessed by dozens of third parties (as seen in the image above in the User Consent section).
- Possibly respect the user's privacy settings they've configured in their browser if and when this type of option is made available by browser vendors.

3. Data Breaches



What Does the GDPR Say About Data Breaches?

In simple terms:

A data breach essentially means whenever a data subject's personal data has been accessed, transferred, or used by someone who wasn't authorized to do so.

Official wording:

> 'Personal-data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
>
> Article 4(12)
> **GDPR**

In today's online world, data breaches seem to be unavoidable, which makes applying the data-protection measures outlined in this guide paramount for all AdTech and MarTech companies.

Notification of a Personal-Data Breach to the Supervisory Authority

In the case of a personal-data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal-data breach to the supervisory authority competent in accordance with Article 55, unless the personal-data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Article 33
GDPR

The article above refers to notifying the supervisory authority, which is the principal EU regulator responsible for enforcement of the GDPR in each member state, of a data breach within 72 hours. With regard to notifying data subjects about a data breach, as outlined in Article 34 of the GDPR, the regulation states that when the personal-data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal-data breach to the data subject without undue delay.

What Does This Mean for AdTech and MarTech From a Technical Perspective?

All advertising and marketing companies may need to change the way their platforms collect data to ensure they contain appropriate security standards to protect them from unauthorized or unlawful processing and accidental loss, similar to the measures outlined in the previous section.

There will also be a number of technological challenges companies will face, including:

> Informing the supervisory authorities and other relevant parties in the supply chain — e.g. other AdTech and MarTech vendors and their clients — about a data breach within 72 hours.

While simply informing these parties about a data breach isn't challenging, it's something that most companies avoid for long periods of time. A notable example includes Uber, which recently disclosed that it had been the subject of a data breach in October 2016, but did not reveal the details of the data breach in November 2017.

> Informing data subjects without undue delay after having become aware of a data breach.

This will prove extremely challenging, even impossible in some cases, for AdTech companies due to the indirect relationship they have with data subjects.

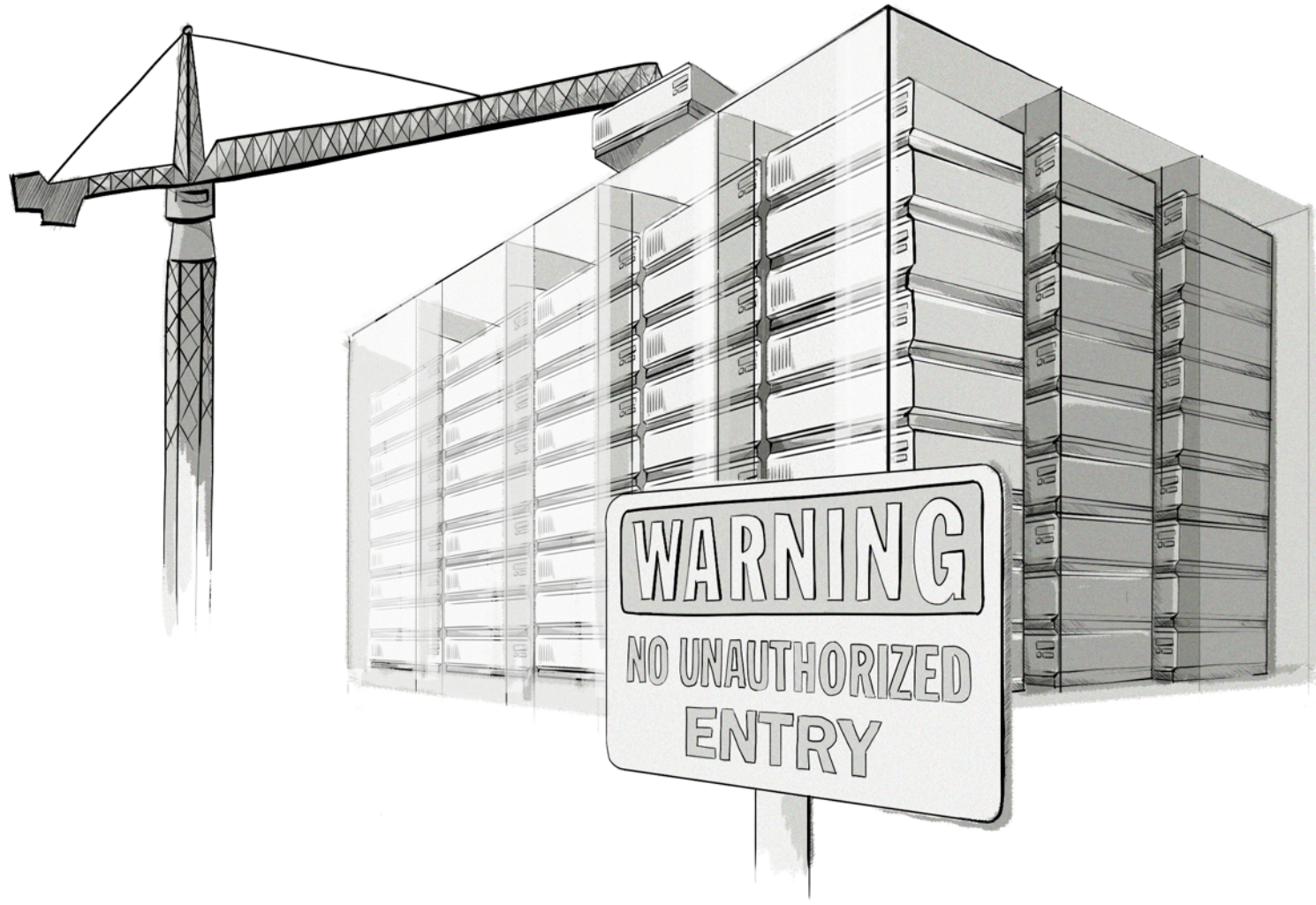
MarTech companies will have an easier time informing data subjects, as their clients (companies that use their MarTech platforms) typically have a direct relationship with data subjects, and therefore can inform them about a data breach (by sending out an email, for instance). AdTech companies don't have this option as contact information isn't collected in online advertising campaigns.

> Knowing how the breach occurred and identifying the security vulnerabilities.

In some cases, companies are unaware of how they were hacked, meaning their platforms could still be vulnerable to further attacks. This point highlights the need for proper data security and protection measures, such as those mentioned in this guide.

On a more positive note, the GDPR states that companies aren't required to inform data subjects about a breach if the appropriate technical and organizational protection measures, such as encryption, have been put in place and applied to the data.

4. Data Protection by Design and by Default



What Does the GDPR Say About Data Protection by Design and by Default?

In simple terms:

Companies should put data protection and user privacy at the forefront of all their activities, from collecting user data to designing and building new software.

Official wording:

1. Taking into account the state of the art, the cost of implementation, and the nature, scope, context, and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time the

of the determination of the means for processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Article 25
GDPR

The introduction of the concept of data protection by design and default, which is based on Ann Cavoukian's 7 Privacy by Design Principles, to the GDPR moves the notions of user privacy and data protection from being afterthoughts to key components of the design and development of new software applications, such as AdTech and MarTech platforms, and the creation of policies and agreements.

In short, data protection by design and default means building software with privacy features which gives users a choice regarding how their data is collected and used, and making the software's default settings or configuration data-protection friendly.

What Does This Mean for AdTech and MarTech From a Technical Perspective?

For many AdTech and MarTech companies that have taken a lax approach to user privacy and data protection, this new requirement means making a considerable number of both technical and legal changes to ensure they are compliant, such as:

- Pseudonymizing, anonymizing, and encrypting data to provide added levels of protection.
- Enabling platforms to carry out a process known as data minimization, which involves only processing the amount of data absolutely needed to complete the given activity — something that will be hard for advertisers to define given how many different pieces of data they collect about online users.
- Building both hardware and software that doesn't collect unnecessary user or device information and store it when it's not needed, as well as sets the default settings to protect a user's privacy. This point applies to AdTech, MarTech, OS, SDK, and browser vendors.
- Conducting a Data Protection Impact Assessment (DPIA) to assess privacy risks to data subjects when collecting, storing, and using their personal data, and to identify and fix possible security issues, such as the possibility of a data breach. While this assessment is a legal process, it will require assessing the technical configurations and settings of a company's AdTech and MarTech platforms.

The GDPR states in Recital 81 that data controllers should only work with data processors that provide *sufficient guarantees, in particular in terms of expert knowledge, reliability, and resources, to implement technical and organizational measures which will meet the requirements of this Regulation, including for the security of processing.*

CHAPTER 3

The Cost of Not Complying With the GDPR

The GDPR has two tiers of fines depending on the severity of the infringements:

Tier 1

Administrative fines up to **10 000 000 EUR**, or in the case of an undertaking, up to **2% of the total worldwide annual turnover** of the preceding financial year, whichever is higher, for violations and infringements related to:

- Obtaining consent from a child to use their data (Article 8)
- Processing which does not require identification (Article 11)
- Designating a data-protection officer (DPO) and their tasks (Article 39)
- Obligations of certification bodies and obligations of monitoring bodies (Article 41, 42, and 43)
- Data protection by design and by default (Article 25)

Tier 2

Administrative fines up to **20 000 000 EUR**, or in the case of an undertaking, up to **4% of the total worldwide annual turnover** of the preceding financial year, whichever is higher, for violations and infringements related to:

Processing personal data and the lawfulness of that processing (Articles 5 and 6)

- Conditions for consent (Article 7)
- Processing of special categories of personal data (Article 9)
- User rights (Articles 12–22)
- Transferring user data to recipients in a third country (Articles 44–49)

CHAPTER 4

The GDPR and ePrivacy Will Fuel Technological Innovation

The GDPR and ePrivacy regulation will require all companies operating in the online advertising and marketing industries to make changes to their policies and contracts with partners to become compliant. However, as we've mentioned in this guide, they will also have to make a number of changes to their technology platforms to ensure they align with their policies.

While this will help companies become GDPR-compliant, smart companies will focus on creating future-proof businesses through innovation. For the most part this will involve developing technologies that respect user privacy, limit their exposure to the GDPR and ePrivacy, and perhaps don't collect personal data at all, but at the same time allow advertisers and marketers to run targeted and effective campaigns.

Since the GDPR's enforcement, we've already seen advertisers and publishers move towards more privacy-friendly targeting and advertising methods, such as contextual advertising and programmatic direct media buying. There's an opportunity for AdTech companies and agencies with their own technology to incorporate these methods into their platforms to offer their clients a safer and more efficient way of running online advertising campaigns.

When you look back throughout history at the impact new regulations have had on certain industries (think the Clean Air Act and the introduction of clean technologies, like the catalytic converter), you can see, despite the initial challenges, the companies that focused on innovation prevailed and thrived.

In the face of all the challenges that the GDPR and ePrivacy bring, advertising and marketing companies can prevail and thrive as well.

Since the GDPR's enforcement, we've already seen advertisers and publishers move towards more privacy-friendly targeting and advertising methods, such as contextual advertising and programmatic direct media buying. There's an opportunity for AdTech companies and agencies with their own technology to incorporate these methods into their platforms to offer their clients a safer and more efficient way of running online advertising campaigns.

CLEARCODE

About Clearcode

Trusted AdTech and MarTech Development Partner

Clearcode is a privacy-focused, full-service software-development company specializing in AdTech, MarTech, and data-analytics platform development.

Based in the EU with offices in the US, our teams partner with startups and publicly traded companies to design, build, and maintain high-performance platforms that meet the demanding and ever-changing needs of advertisers and marketers and solve various technological challenges.

Being a EU-based company means we have a strong understanding of how the GDPR and ePrivacy regulation will impact companies operating both inside and outside of the EU. This insight, combined with our experience, allows us to provide clients with sound advice on how to properly comply with the GDPR and develop software that protects and respects user privacy.

Questions?

Contact us

EMAIL

sales@clearcode.cc

PHONE

US: (800) 615-0584
Europe: +48 71 881 766

WEB

clearcode.cc