



Whitepaper
October 2020

Legally sound Consent Management - everything you need to know

Classification, checklists and practical tips for the correct approach to cookies and other web technologies.

Table of Contents

1. Privacy as a Competitive Advantage	3
2. User consent as a success factor	4
3. Legal and regulatory guidelines	5
4. Consent becomes an integral part of the contract	10
5. Manage consent across the board with a Consent Management Platform	13
6. Checklist: What does GDPR-compliant consent look like?	14
7. Checklist: What a Consent Management Platform must deliver	16
8. Make your data fit for the future!	18
9. About Usercentrics	19

1. Privacy as a Competitive Advantage

Recognise GDPR-compliant consent management as an opportunity

Consent in everyday life consists mainly of a “yes or no” question. In contrast, the General Data Protection Regulation (GDPR) adopts a far more multi-layered term for consent and links strict requirements to valid consent.

A simple situation which becomes complex under GDPR is visiting a website. This is because when a website has incorporated technologies such as cookies, pixels or other external sources, prior consent is required from the website visitor in certain cases. In particular, when the intended purpose is to carry out tracking, retargeting and profiling.

So-called Consent Management Platforms (CMPs) have emerged in the context of the GDPR and this regulatory necessity. Their service offering encompasses the obtaining, processing and documentation of consent.

Only those who take the principle of user-side data sovereignty seriously and carefully integrate appropriate mechanisms into their processes can profit from the current and, more importantly, future legal situation. This practice enables companies to prevent rejection from lawmakers, obtain reputable advertising technology partners and users themselves.

Companies who pursue clean Consent Management secure themselves the trust of their users and make use of privacy as a competitive advantage.

On the following pages we will give you an insight into the world of Consent Management. Our aim is to ensure clarity regarding the current legal situation and conviction with the use of a Consent Management Platform.



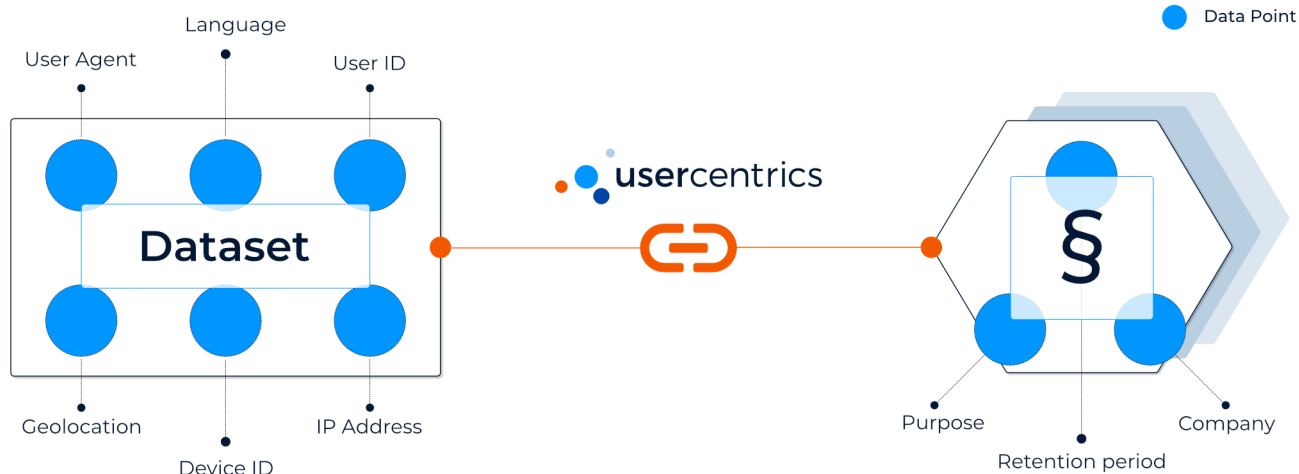
Mischa Rürup
Founder & Director
Usercentrics GmbH



2. User consent as a success factor

Why Consent Management for advertising companies is critical for revenue

Data with consent is the currency of the future



When consent has been given the data record may be used.

Since the GDPR came into force on 25th May 2018, no term has been the focal point as much as the word “consent”. This regulation fundamentally regulates the processing of personal data.¹ Furthermore, as established by the ECJ in 2016, IP-addresses were already regarded as personal data even before the GDPR.

As one of the six legal bases according to Article 6 GDPR, consent is the central instrument in marketing. In the context of web technologies this recognition can, for example, be a unique ID allocated to every visitor in order to recognise them again in subsequent visits. According to the GDPR these include cookies, pixels, fingerprinting and comparable technologies. These include familiar ad-

vertising technologies such as web tracking, multi-channel tracking, audience targeting or retargeting, especially to the extent that 3rd party tracking and 3rd party cookies are in use. So-called “piggybacking” (of their third-party cookies) must also be mentioned.

Short & concise

- The GDPR regulates the processing of personal data.
- The consent of the user is essential for the processing of personal data according to Article 6 of the GDPR.
- User consent must satisfy strict criteria.

¹ see <https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-10/cp160112en.pdf>

Why obtaining user consent is so important

The following factors play a role in deciding whether to draw upon user consent as a legal basis. Our tip: Embrace the technical changes of the adtech world now rather than wait for the first court rulings.

1



Guidelines through vendors

Technology providers such as Facebook and Google as well as IAB vendors will need a consent ID in the future - they are even required now in some situations. Personalised ads will no longer be displayed without them (see also Chapter 4).

2



Guidelines through authorities

Data protection authorities all over Europe have published statements detailing the cases in which user consent is to be obtained. Certain interpretations are establishing themselves (also see Chapter 3).

3



Legal Guidelines

Consent must have been obtained prior to running tags, to the GDPR. Consent Management Systems connect with the Tag Management System being used so that this guideline can be implemented.

4



Burden of proof for consent

As an advertiser you must obtain consent and be able to prove you have done so (server side, not in the cookie). In this regard it is important to check whether your company has a consent database with consent IDs.

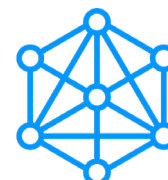
5



Threat of Warnings

Companies without a clean consent management concept can be issued warnings by various stakeholders. The German fair trade law (Ger. Gesetz gegen den unlauteren Wettbewerb) may be applied in the event of a potential data protection breach.

6



IAB Transparency and Consent Framework (TCF) Compliance

Many vendors e.g. Criteo in the near future, will no longer support advertisements which are not adhering to the IAB Consent String ("TC String"). An IAB certified Consent Management Platform guarantees compliance.

Personal data without consent will be **worthless** in the future.

3. Legal and regulatory guidelines

Why keeping an eye on current developments is worth it for staying on the right side of the law.

Legal interpretation of data protection is continuously in flux: new laws are passed, changed, amended or substantiated through rulings. A cleanly set up CMP creates a solid foundation for maintaining full visibility at all times of all gathered data and its storage - and therefore be able to react directly in the event that the legal situation or the company's own data strategy change.

Website operators are not only on the safe side in the legal sense and protected from fines but also respect the data sovereignty of the user, thereby strengthening trust in your brand and the company's image.



The following legal guidelines and rulings offer, amongst other things, further orientation to ensure a GDPR compliant data gathering.

The position paper of the German data protection conference

The German data protection conference (DSK) published the ["Orientation help for providers of telemedia"](#) in March 2019 in which it explicitly states that the GDPR takes precedence over the provisions of the Telemedia Law (TMG). It also details when "tracking" can be used legally and how "consent tools" help.

The guidelines and recommendations of the European data protection authorities

Various other data protection authorities such as the Danish Data Protection Authority (DPA) [Datatilsynet](#) or the French one, [CNIL](#), have already issued guidelines and position papers regarding concrete implementation of the GDPR. Although these papers primarily serve as orientation for the interpretation and implementation of the GDPR in the respective member state, they do however point the way for its implementation and the reaching of verdicts in the entire European Union. That said, it is important to note that these guidelines are adapted

over the course of time. Rulings, bringing clarity are decided and guidelines therefore re-considered e.g. Cookie Walls decision by the CNIL .

When considering fine proceedings, it is also worth keeping an eye on our European neighbours. For example, the [Spanish data protection authority](#) levied a 30,000 Euro fine against the airline Vueling because its cookie banner violated the national data protection law. This ruling can be regarded as setting a precedent for all other EU countries although specifically issued in Spain.

As a superior, independent body, the European Data Protection Board (EDPB) contributes to ensuring a consistent implementation of the data protection law across the entire European Union and promotes cooperation between individual EU data protection authorities. In its updated ["Guidelines on Consent in the Use of Internet Sites"](#) from May 2020 it provided a clear statement on, amongst other things, the subjects of "implicit consent through continuing to scroll" and "cookie walls".

ECJ Ruling July 2019

Site operators are (jointly) responsible for Facebook “Like” buttons on websites

According to the [ECJ ruling](#) on the case of German eCommerce firm, Fashion ID (29th July 2019), website operators who integrate a Facebook “Like” button are jointly responsible for data processing through Facebook. Since data processing is initiated by visiting the website, their operators are obliged to obtain prior consent from the user. This is because user data is passed on to unknown third parties during the visit, without the user’s awareness and potentially against the user’s will. A further challenge is that data is forwarded on regardless of whether the visitor has a Facebook account or not. The user does not even have the chance to object or prohibit the forwarding of data on the website. The only opportunity available to the user is to surf using special plugins or browsers in order to protect his or her own private sphere. Nonetheless, users cannot be expected to do this. In fact, the website operator has the duty to ask for the user’s consent beforehand and couple the forwarding of data to this consent.

More information regarding the Fashion ID ECJ ruling from July 2019 and how to protect yourself as a website operator can be found [here](#).

ECJ Ruling October 2019 / BGH Ruling May 2020

Explicit active consent required for cookies on websites

On 1st October 2019 the ECJ ruled in the [case of “Planet49”](#) regarding requirements for consent when placing cookies. In this particular case, German company Planet49 had organised a prize draw in 2013, long before the GDPR came into force. The main issue in this case was the fact that the tick for consenting to cookies being placed on the user’s device had been preselected, although it could be removed (opt-out process). The decision of the judges: Pre-ticked boxes do not count as consent. The judges demanded not only an explicit but also a concrete action performed by the user in the form of an opt-in. These conditions are also to be valid independent of whether the information contained within the cookies is personal or not. Furthermore, the website visitor must be informed in detail about which data is gathered and how this is processed.

The German Federal Supreme Court (BGH) also strengthened the position of the ECJ in its [ruling from 28th May 2020](#) on the case of “Planet49”: Companies wishing to use cookies on their website for advertising purposes may only do so with the informed, explicit and above all prior consent of its users. Pre-ticked declarations of consent are not sufficient according to the BGH.

Ruling from the Bavarian Administrative Court (VGH)

Forwarding of hashed emails only with consent

Hashed email addresses may only be given to Facebook for advertising purposes with the consent of the affected persons as ruled by the Administrative Court in Munich on 26th September 2018 (5 CS 18.11578). The Administrative Court ruled that the forwarding of hashed email addresses to Facebook as part of the services “Facebook Custom Audience” does not occur as part of contract data processing in the spirit of § 11 BDSG (old version), but is to be regarded as forwarding to a third party (§ 3 Section 8, sentence 2 BDSG old version) which requires appropriate consent from the affected party or legal permission for forwarding data, as stipulated in § 4 Section 1 BDSG old version.

The ePrivacy Myth

The ePrivacy Regulation is not a valid argument against a Consent Management Platform

Originally the ePrivacy Regulation was to come into force at the same time as the GDPR. However, the EU Council of Ministers has been unable to reach an agreement so far on a legal text which is why the old ePrivacy guideline from 2002 and the cookie guideline from 2009 are yet to be replaced. This has probably given rise to the misunderstanding that cookies will first be regulated by the new ePrivacy regulation. This is already the case with the GDPR.

Background: The ePrivacy regulation encompasses all electronic communication data including that without any connection to an actual person. As a so-called *lex specialis* of the GDPR, the ePrivacy regulation will, however, substantiate certain matters relating to the GDPR when it comes to personal electronic communication data - including cookie data. Since cookie data is fundamentally personal data, the stipulations of the GDPR are already fully applicable.

Our tip: Do not wait for the new ePrivacy Guideline. This will likely not come into force until 2023-25 - and fully revised at that. Protect yourself today to ensure you are not subject to a warning in the loophole between the GDPR and ePrivacy Guideline.



Good to know:

When the ePrivacy Guideline comes into force it will not only be users given the right to sue due to breaches of its provisions but also competitors - and this explicitly in order to protect their legitimate business interests.

Jurisdiction on international data transfer

The transfer of personal data from the EU to third countries requires a legal basis. The transferring company must ensure that the data is stored and processed in the destination country in accordance with European data protection standards. Since the jurisdiction in this field is currently constantly changing, website operators should definitely keep an eye on the current legal situation, e.g. with regard to the latest European Court of Justice rulings on the Privacy Shield/Schrems II.

The California Consumer Privacy Act (CCPA)

It is not just Europe experiencing new development in data protection but also the USA

The California Consumer Privacy Act (CCPA), the data protection law of the US State of California, came into force on 1st January 2020 and regulates how personal data is to be handled in the consumer sphere. It guarantees all residents of California the right

- to know whether and, if so, which data about them has been gathered (Right to Know) and
- to know whether their data is passed on or sold to other companies or persons,
- to view the information gathered about them at any time (Right to Information),
- to prohibit the sale or forwarding of their data (Right to Opt-out) and
- to demand that a company delete the data which has been gathered about them (Right to Delete).

DO NOT SELL MY PERSONAL INFORMATION - opt out instead of opt in

Unlike the GDPR, a CCPA-compliant website needs to have an unambiguous and prominent text on the landing page bearing the following text: „Do not sell my personal information“. This link must not only be shown in the privacy statement but also in the footnote of the website. The goal of this link is to give consumers the opportunity to prevent the sale of their personal data. Unlike the GDPR (opt-in principle), the CCPA assumes an opt-out principle. Companies who do not process or pass on personal data are exempt from this obligation.

For whom does the CCPA apply?

It applies to profit-making companies, service providers and enterprises who gather personal data, have their registered addresses in California or that processes the personal information of consumers in California. That said, a company is obliged to comply with CCPA if it fulfils one or more of the following points:

1. Gross revenues of 25 million US dollars or more.
2. More than 50,000 data objects (per year) gathered from customers, households or devices connected to networks for commercial purposes (harvesting, purchase, sale or other forwarding).
3. More than half of the annual revenues achieved with the sale of personal data from Californian customers, households or devices connected with networks.

Important!

European companies who have their headquarters in California can also be affected by the CCPA if they fulfil one or more of the following criteria. Further information regarding the CCPA and how you can design your website to comply with it can be found [here](#).

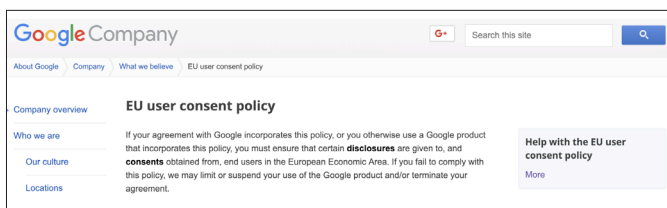


4. Consent becomes an integral part of the contract

How Google, Facebook and the IAB framework are making consent the new currency in online marketing

A. Google's Position on Consent

Google has a separate consent policy² describing what is necessary for a user's consent. Detailed information can be found in the guide to consent policy³.



The guideline stipulates that obtaining consent is necessary when cookies are used as well as processes connected with personalized advertising:

Properties under your control

For Google products used on any site, app or other property that is **under your control, or that of your affiliate or your client**, the following duties apply for end users in the European Economic Area.

You must obtain end users' legally valid consent to:

- the use of cookies or other local storage where legally required; and
- the collection, sharing, and use of personal data for personalization of ads.

When seeking consent you must:

- retain records of consent given by end users; and
- provide end users with clear instructions for revocation of consent.

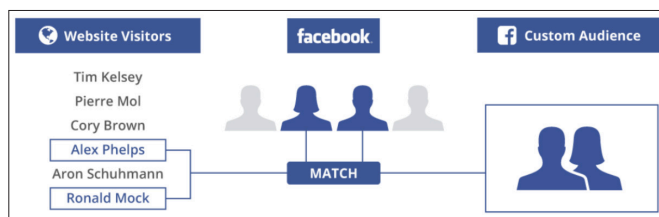
This consent must satisfy the requirements of the GDPR and, above all else, must be objective, trackable, documented and revocation clearly explained:

When seeking consent you must:

- retain records of consent given by end users; and
- provide end users with clear instructions for revocation of consent.

B. Facebook's Ranking of Custom Audiences

The use of Facebook Custom Audience was already critical from a legal standpoint, even before the GDPR came into force⁴. The reason for this is that a detailed profile of the user is put together. This is particularly true when a website operator integrates a Facebook pixel because the user's surfing behavior is then enriched with his or her Facebook profile information:



For this reason, the Facebook Custom Audiences Pixel, under the GDPR, is only permitted with the express consent of the affected person. Facebook passes the responsibility for obtaining the consent of the website visitor on to the website operator who has integrated the Facebook pixel:

Who is responsible for obtaining consent when personal information is used to place ads on Facebook?

Facebook is the data controller when an advertiser places ads based on information that people provide directly to Facebook, or on data received through the Facebook pixel and SDK. The advertiser is the data controller when they place ads using data file Custom Audiences or upload peoples' personal information through other Facebook measurement and analytics services. If an advertiser is acting as a data processor, they must ensure compliance for processing personal data. That said, even where we are a data controller, you may have certain obligations under our terms and the law.

Facebook has, like Google, issued its own guidelines details on how to obtain this consent: Handbook for Cookie Consent⁵:

Cookie Consent Guide for Sites and Apps

If you operate a website or app, you probably use cookies or other storage technologies to offer people a better user experience, understand what kinds of visitors use your service and show them more relevant ads. In many instances, you are required to obtain consent from people before using these technologies.

We created this page to help digital publishers like you find resources and tools that may help you meet consent requirements.

² see <https://www.google.com/about/company/user-consent-policy.html>

³ see <https://www.google.com/about/company/user-consent-policy-help.html>

⁴ Please also refer to the detailed instructions and requirements of the Bavarian State Data Protection Authority (July 2017) and a ruling from the Bavarian Higher Administration Court which stated that use was permissible according to the old Federal Data Protection Act

⁵ see <https://developers.facebook.com/docs/privacy/>

C. Industry Standard IAB Transparency and Consent Framework (TCF)

Any company gathering user data on its website must inform the user in detail about how and for what purpose the data will be used. The International Advertising Bureau (IAB) Europe has developed the “GDPR Transparency and Consent Framework (TCF⁶)” to illustrate this process in a technically sound manner – and provides a possible answer to the question of how consent in actual practice should look. The expanded version 2.0 was published in September 2019 (binding from 15th August 2020).

The framework offers a technical standard infrastructure for the querying and transmission of consent between advertisers, publishers and their technology partners. As a vendor you can be obliged to support this framework.

Numerous essential players and technology providers from the adtech landscape have already done so. Most notably Google, but also Criteo, Xandr, Addition, Quantcast, Taboola, MediaMath, etc.

In this context, many vendors are no longer supporting any advertising which does not adhere to the IAB TC string.

This is shown in the original email from TheTradeDesk to its customers in May 2018:

“Do you have a significant amount of EU users that you target or track via 1st party data segments/audiences in TTD, using the TTD cookie sync (e.g., https://match.adsrvr.org/track/cmf/generic?ttid_pid=examplepartnerid&ttid_tpi=1)?”

Parameter	Possible Values	Description
gdpr	0 or 1	Indicates if the request is GDPR regulated. e.g gdpr=1
gdpr_consent	base64url-encoded GDPR consent string. Only meaningful if gdpr=1	This is the consent string that has information regarding vendor consent (including TTD). e.g gdpr_consent=BOEFBi5OEFBi5AHABDENAI4AAAB9vABAASA

If you don't cookie sync on EU users, you won't be affected by our GDPR cookie sync changes. If you do, please read on, as TTD is changing what we expect to receive in cookie syncs URLs as it pertains to any user in the EU, and TTD will begin to stop returning cookie syncs where we don't have consent for an EU user, starting 5/25 UTC.

Beginning 5/25, if the IAB GDPR cookie sync request parameters are not sent in cookie syncs with EU users, then TTD will drop the request, and not return a TTD cookie ID (TDID). If consent parameters are sent in the EU user cookie sync, TTD will process the cookie sync, determine if we have consent to read/write cookies, and if so, we'll send back a TDID.

For all non-EU users, the cookie syncing process will remain unchanged.

1. If you're syncing with TTD on EU users, will TTD have consent to write cookies to the EU user's browser?

A) Yes, TTD will have consent.

i. Please confirm that you'll use the following IAB consent parameters in the cookie sync URL where you initiate:

https://match.adsrvr.org/track/cmf/generic?ttid_pid=partnerid&ttid_tpi=1&gdpr={0|1}&gdpr_consent={IAB_consent_string}

ii. e.g., https://match.adsrvr.org/track/cmf/generic?ttid_pid=partnerid&ttid_tpi=1&gdpr=1&gdpr_consent=BOEFBi5OEFBi5AHABDENAI4AAAB9vABAASA

B) No, TTD will not have consent to write cookies to EU user's browsers.

i. Do you plan on not passing any EU cookie syncs to TTD?

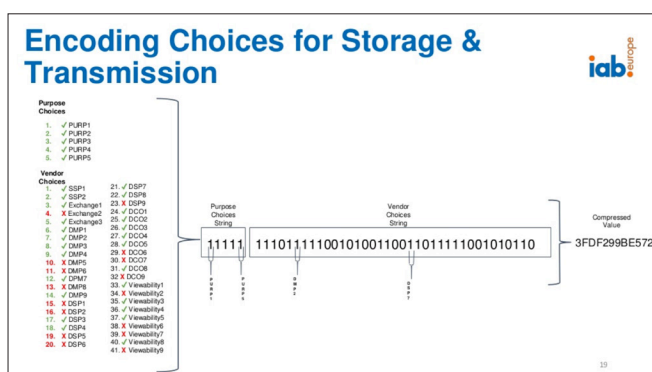
ii. Will you continue to pass EU cookie syncs and have TTD's logic filter out writing cookies on EU users?"

⁶ see <https://iabeurope.eu/tcf-2-0/>



It can be expected that this process will be established by more vendors with time. For example, Google is planning to integrate version 2.0 from August 2020 ([current status](#)).

If a vendor demands an IAB certified TC string, the advertiser must guarantee the following transmission of user consent:



Short & concise

- Industry giants such as Google and Facebook are making user consent the new currency in online marketing.
- The “GDPR Transparency & Consent Framework” issued by the IAB (International Advertising Bureau) defines a possible standard as to how consent in adtech practice should look.
- More and more vendors are supporting the IAB framework which, in plain terms, means that they are only running adverts satisfying the requirements of the framework.

A valid TC string can only be generated with a certified Consent Management Platform (CMP) and forwarded on to vendors.

If advertisers wish to work with vendors who require a TC string, they will not be able to get around the use of a CMP.

The reason: No consent reduces ad performance. No ad performance means less advertising revenue!

5. Manage consent across the board with a Consent Management Platform

Obtain, manage and document consent using technology - how it works

Consent Management Platforms function as a programmatic solution by querying and establishing the consent status of the user and/or storing and managing it in accordance with the law. Furthermore, CMPs can make the consent status available to a third party via technology.

The exact sequence: If a user visits a website or an app, he or she will be shown a banner or pop-up window. Users will be able to decide which data gathering and processing they agree to via a simple and attractive interface and determine which information may or may not be forwarded. The user consent will then be stored in accordance with GDPR and accessible for an audit so that authorities can check if required. Also, web technology providers wishing to use data for advertising campaigns

can check via interfaces to the Consent Management Platforms in real time whether they are authorised to track a particular user for specific purposes.

In Chapter 7 we have summarised for you how a good Consent Management Platform should look.

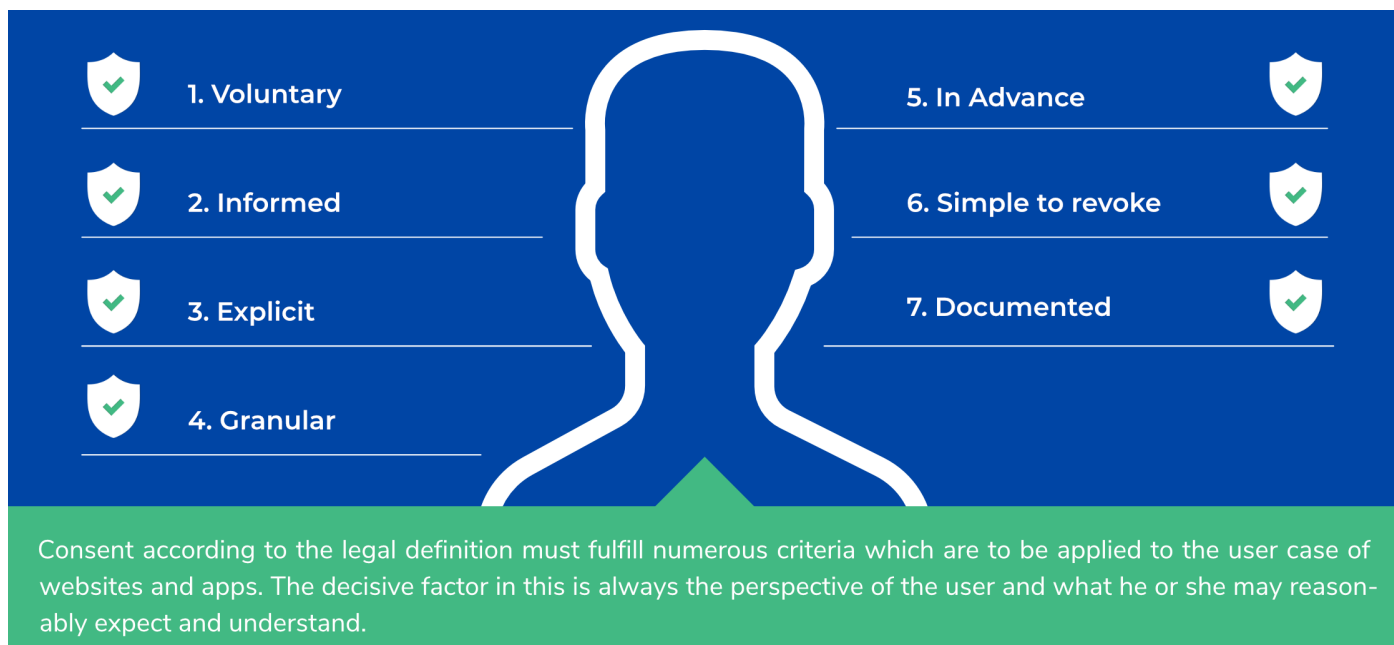


Short & concise

- A Consent Management Platform obtains user consent using technology; managing and documenting this consent in accordance with the law.
- Upon visiting a website, the user can determine in a few clicks the extent to which they allow the processing of their data.
- Advertising technologies receive information in real time via interfaces regarding whether they may track a particular user or not.

6. Checklist: What does GDPR-compliant consent look like?

Criteria for user-friendly consent management according to the GDPR.



Voluntary

"Accept" and "Reject" button

Consent is granted voluntarily when the person is given real freedom of choice in their decision.⁷ For the website this means: There must be the possibility to reject the processing of data but to use the website anyway. This voluntary nature in particular is tightly interpreted by rulings from the authorities to the consumers' advantage. Banning access to the website merely because the user did not consent to the placing of marketing tags may hardly have a leg to stand on in practice.⁸

Informed

Who, what, why, how long?

Informed consent occurs when the affected person is aware of all facts in connection with his or hers data processing and consciously consents to it.⁹ Information regarding the right to revoke consent is also essential to being informed.

Explicit

Yes, I want to!

The user must actively agree to the processing of his or her personal data. What this essentially means is that, what is commonly known as "implicit consent" or what is the same, "continuing to surf", is not a compliant practice if tags are loaded immediately at the beginning of the visit.

Granular

Consent to Google, Facebook etc.

The consent must be technology or cookie-specific. This means that the user must know at the granular level for which data record and for which third party provider they are granting or revoking their consent. General consent in general references to not satisfy this information principle¹⁰ as consent should be tied to each specific purpose.

⁷ Recital 42 GDPR; Guidelines on Consent under Regulation 2016/679 (WP259)

⁸ see Recital 42 P. 5 GDPR; Wybitul/Böhm: Email checks for compliance purposes and for internal investigations, CCZ 2015, 133, 136.

⁹ Wybitul/Strobel/Rueß: Transmission of personal data to third countries, ZD 11/2017, 503, 507.

¹⁰ Wybitul/Böhm: Email checks for compliance purposes and for internal investigations, CCZ 2015, 133, 136.

In Advance

No data to be collected before opt-in

Data may only be collected once permission has been obtained. There must also be a technical linkage between the cookie banner and the technology built into the page. Otherwise data will be processed without a valid legal basis resulting in a breach according to Article 83 Paragraph. 5 lit. a) of the GDPR. If the user does not provide consent, a technical guarantee must be put in place to ensure that no data is collected or passed on from that point onward.

Simple to revoke

Opt-out on the page

The user has the right to revoke previously granted consent at any time and without needing to provide a reason. The process of revocation must be as simple as that of providing consent.¹¹ When referring to tags this means that the user must be able to view individual tags and revoke their consent to some or all of them easily, with just a few clicks.

It cannot be expected that the user must search for the respective opt-out option in the data protection provisions and potentially be redirected to a third party website. A click-out in the data privacy statement which is linked to an opt-out on a third-party website is not technically sufficient in any case. The reason for this is that subsequent forwarding of data from the website operator must be prevented should the user revoke their consent. Reading out the cookie ID - even for the purpose of establishing the opt-out - already represents an unauthorised transmission of data to third parties (in this case to the processor). The tag may no longer be activated after consent has been revoked. Consequently, this means that the combination of OK banner and opt-out notice in the data privacy statement does not satisfy the GDPR, neither legally nor technically.

Documented

Burden of proof should an audit take place

According to Article 7 Section 1 GDPR all consent must be documented. Website operators have the burden of proof according to the GDPR and must be able to present the consent history in the event of an audit or warning from a data protection authority. To ensure that consent

would stand up to an audit, various data points should be stored e.g. time stamp, user agent or the version of the consent text. Placed URL calls should also be logged in order to prove that no cookies were run before consent was obtained.



Short & concise

- Legally sound user consent must fulfil numerous criteria in accordance with the GDPR.
- The prime focus in this is that the obtaining of consent should be as user friendly as possible.
- GDPR compliant consent must be granted voluntarily and in advance and must be documented in accordance with applicable laws. Furthermore, the consent must be informed, explicit and granted at the granular level. Revocation of such consent must also be easily possible at any time.

How is consent obtained from minors?

Strict requirements apply for valid user consent regarding minors to ensure an extra degree of protection. According to Article 8 GDPR this must be obtained from the parents or legal guardians. Since this is not possible for practical reasons whilst surfing the internet, websites using tags for which consent is required must first ask for and document the age of their visitors. This can be integrated into the text of the general banner message. Tags may only be loaded into the browser once it has been verified via the message that the visitor is aged 16 years or older. However, who counts as a minor is regulated differently in every member state.

¹¹ Art. 7 Paragraph. 2 P. 4 GDPR.

7. Checklist: What a good Consent Management Platform must deliver

Are you planning on using a consent management platform? You should consider the following criteria when evaluating individual providers so that you make the right

choice for your company. Explanations regarding the individual criteria can be found on the next page.

Criterion 1

Full integration into the data privacy statement

Criterion 2

Saving the consent

Criterion 3

General consent prohibited

Criterion 4

Loading procedures after revocation

Criterion 5

IAB-Consent standard and further

Criterion 6

Flexibility

Criterion 7

Server location

Criterion 8

Privacy-by-Design

Criterion 9

Business purpose

Criterion 10

Integration into tag management and the website

Further information about choosing the right CMP can be found in our [Buyer's Guide](#).

1. Full integration into the data privacy statement

The CMP should make it possible to integrate data protection texts of the technologies used into the data privacy statement. Likewise, the privacy statement must name all of these technologies and parameters due to the reporting requirement. Merely displaying the cookies is not sufficient as documentation. What is more, plug-ins, hosting providers and integrated content such as videos also come under this reporting requirement.

2. Saving the consent

The requirement to prove consent enshrined in the GDPR applies in particular to its documentation. Consent should therefore (also) be stored on the website operator's servers. Saving on the user's terminal devices alone is not sufficient because the proof can be deleted without the knowledge of the website operator and satisfying the competent authorities will be impossible.

3. General consent prohibited

Legally valid consent can only be obtained for technologies which are actually used on a website. Obtaining common consent for a complete list from all possible providers runs contrary to the specificity requirement and the minimum principles of the regulation. General consent is therefore not possible under the GDPR.

4. Loading procedures after revocation

The loading processes of the technologies requiring consent may only be started after consent has been granted (opt-in) - which may already be the case. Only technologies for which the user has granted consent may be loaded. This applies likewise in the case of opt-outs: the rejected technologies are prohibited from collecting data and parameters from the moment of revocation.

5. IAB-Consent Standard and Others

It is important that the CMP offers the opportunity to support industry standards such as the IAB Consent Framework. Many large web technology companies are already following this framework. Personalised advertising in programmatic ad trading will only be possible in the future with a consent ID. It is expected that further standards will emerge over the course of time. A CMP should therefore be developed to fulfil standards and requirements which are yet to come.

6. Flexibility

It must be possible to customise the CMP to the individual design of the website at any time, even after significant changes. This includes both the design and layout as well as the technologies used. When, for example, the analysis tool or a web technology is changed, the CMP must be able to display this without confusing the user.

7. Server location

A secure CMP distinguishes itself with a server location on EU soil. The reason for this is the consistency of the EU as a jurisdiction and the legal complexity involved when data is transmitted to third countries.

8. Privacy by design

The end user's data must be stored separately for each website on which the CMP is used to prevent the CMP from becoming the next data leech. Otherwise the CMP has already begun creating a profile of online behaviour. It is imperative to note that consent obtained on one website may not simply be transferred to other websites without further steps. This is only possible under certain conditions, e.g. within companies, and should also be configurable via the CMP.

9. Business purpose

The CMP provider should only pursue the obtaining of consent as the business purpose. Otherwise it can be assumed that consent data can also be used for other business purposes, each of which will require separate consent.

10. Integration into tag management and the website

All advertising and marketing tags require explicit and voluntary consent from the user. Since you are only allowed to load after the user has opted in, it is important that a CMP can be seamlessly integrated into existing tag systems. Furthermore, the CMP must manage codes built directly into the website or those which control embedded technologies, such as scripts or videos, so that these do not load if consent is not sufficient. There are already reports of the first warnings in relation to Google Fonts.

8. Make Your Data Fit for the Future!

Act now and secure yourself a competitive advantage

Data protection compliance will become a success factor for every data-driven business model. The risk of receiving a warning and the risk of losing advertising revenues is intolerable for all the company's stakeholders. Do not allow data protection to damage your business. Act with foresight!

One thing is clear: Websites and digital platforms are generally one of the most vulnerable parts of an organisation as a breach of compliance or data protection rules can be proved by any observer with little effort and rudimentary technical means.

Data processing not covered by Article 6 GDPR represents a finable breach according to Article 83 Section 4a GDPR. In addition to that, it entitles the affected party to issue a warning or claim compensation in some cases. Competitors are also entitled - according to the UWG - to issue warnings and, cease and desist orders against a company in the event of relevant data protection breaches relating to competition law.

Every advertiser should therefore grapple with the question about which consent should be obtained and how it is to be documented. To automate these processes and to be on the right side of the law at all times it is worth investing in a good Consent Management or Consent Permission Platform (see checklist in Chapter 7).

The reason: Consent or the "opt-in rate" are the new currency in online marketing.



The opt-in rate as the new KPI

A good CMP will always offer additional features such as individualisation, AB testing or contextual consent to continuously improve a website's opt-in rate. The opt-in rate can be improved by as much as 39% through measures such as active AB testing and the regular evaluation of opt-in reports. Detailed information and current study results on the subject of "opt-in optimisation" can be found in our [white paper](#).

**Reduced ad performance without consent.
No ad performance means less advertising revenue.**

9. About Usercentrics

Compliance & Marketing in Harmony



Munich technology company Usercentrics is a market leader in the field of [Consent Management Platforms](#) (CMP). The SaaS solution from Usercentrics enables companies to gather, manage and document consent provided by users on all digital channels such as websites or apps - and achieve high opt-in rates in the process. This guarantees compliance with current and future international data protection guidelines such as GDPR, ePrivacy Regulation and CCPA and enables it to be integrated into the marketing and data strategy.

Since its founding in 2017, the company has grown strongly and now has over 300 enterprise customers. Further information can be found at [usercentrics.com](https://www.usercentrics.com).

Contact

Usercentrics GmbH

Sendlinger Str. 7
DE 80331 Munich
contact@usercentrics.com
+49 89 21 54 01 20
www.usercentrics.com

Your contact persons

Mischa Rürup

Founder & CEO
mr@usercentrics.com
Sendlinger Str. 7
DE 80331 Munich

Jana Krahforst

Head of Legal
legal@usercentrics.com
Sendlinger Str. 7
DE 80331 Munich

Franz Stare

Director Sales
fs@usercentrics.com
Sendlinger Str. 7
DE 80331 Munich