Guidance from the Conference of Independent Data Protection Authorities

of the federal and state governments of December 20, 2021

(as of December 20, 2021)

Guidance from regulators

for providers of telemedia

from December 1, 2021

(OH Telemedia 2021)

Contents

I

introduction

Technologies are regularly used in the operation of telemedia – often by

Third-party service providers1 - for use, which enable personal data from

to process users for various purposes. A very practical one

Examples of such technologies are so-called cookies. Using cookies and similar

Technologies can store information on users' devices,

are enriched and managed using unique identifiers

(UIDs) allow identification or assignment to a natural person. In the

In practice, these processes often serve to change the individual behavior of the users

– sometimes across different websites and devices

and, if necessary, to create profiles about a person.

Regardless of the technical design or the purposes pursued, the

Collection and further processing of this information usually as a uniform

life situation perceived. Legally, however, there are two steps to this

differentiate. First, the storage of and access to information in the

Terminal equipment and secondly, the processing of personal data that

often with the use of cookies and similar technologies. The

The lawfulness of this (follow-up) processing depends on the requirements

of the General Data Protection Regulation (GDPR). The upstream technical processes

- in particular the setting and reading of cookies - also affect the

Integrity of the terminal equipment and are thus originally subject

in the

Scope of directive 2002/98/EG2 in the directive 2009/136/EG

amended version (so-called ePrivacy-RL3).

According to the assessment of the supervisory authorities, that for telemedia has been since 2009

applicable Art. 5 Para. 3 ePrivacy-RL through § 15 of the Telemedia Act (TMG).

sufficient

implemented into national law. In addition, there were

Difficulties in application since the GDPR came into force. The conference of

independent data protection authorities of the federal and state governments (DSK).

against this background in March 2019 a guide for providers of

Telemedien (OH Telemedien 2019) published, which should help those who

implement legal requirements.

1 Where in this text or any appendices, designations such as "third parties" "third-party service providers" or "Third-party providers" are used, this is not to be understood in the sense of Art. 4 No. 10 DS-GVO, so that Processors and their services are included.

2 Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 on the

Processing of personal data and protection of privacy in the electronic

Communications (Privacy Policy for Electronic Communications).

3 If a provision of the ePrivacy Directive is mentioned below, the current one is always meant

as amended by Directive 2009/136/EC of the European Parliament and of

Council of 25 November 2009 amending Directive 2002/22/EC on universal service and

User rights in electronic communications networks and services, Directive 2002/58/EC on

the processing of personal data and protection of privacy in the electronic

communication and regulation

(EC) No. 2006/2004 on cooperation

in the

consumer protection.

With effect from December 1, 2021, Art. 5 Para. 3 ePrivacy-RL was replaced by § 25 des

new telecommunications telemedia data protection law (TTDSG)4 in German

Law implemented, to be observed in the future when using any technologies

is by means of which information is stored on or from terminal equipment

be read out. With a view to the new legal situation, the OH Telemedien 2019

completely revised and supplemented. The requirements outlined below

and ratings are not limited to running websites and apps, however

these are the most common applications

finishes

predominantly

examples

as an illustration

from these

areas of application.

The present guidance is subject to the express reservation of one

future - possibly deviating - understanding of the relevant

Regulations by the European Data Protection Board

(EDPB), by

relevant European jurisprudence and changes in European law

legal framework.

II.

New legal situation for telemedia from December 1, 2021

With the entry into force of the TTDSG on December 1, 2021, a new one came into effect at the same time

Telecommunications Act (TKG) and amendments to the TMG in force. In the TTDSG

the essential data protection rules for telecommunications and

Telemedia services bundled. Neither

in TKG yet

in the TMG are still

contain data protection regulations.5 The TTDSG has e.g. Impact on the very

practical use of cookies and similar technologies.

1. The Telecommunications Telemedia Data Protection Act

The TTDSG regulates, among other things, the protection of privacy when using

Terminal equipment, regardless of whether there is a personal reference or not.

In addition, the law contains special provisions

technical and

organizational precautions to be observed by telemedia providers

are, and the requirements for the provision of information on inventory and

usage data. The reason for the legislation was Directive 2018/1972/EU on the

European Code for Electronic Communications6, which amends the

TKG required. The legislature took the opportunity to

data protection regulations of the TKG and the

4 Act on the Regulation of Data Protection and Protection of Privacy in Telecommunications

and for telemedia from June 23, 2021 (Federal Law Gazette 2021 I 1982).

5 p. Bundestag printed paper 19/27441, p. 30: "The draft law is intended to create a closed and

of the Telemedia Act and the Telecommunications Act, separate legal regulation on

Data protection and privacy protection in telecommunications and telemedia created

become".

6 Directive 2018/1972/EU of the European Parliament and of the Council of December 11, 2018 on

the European Electronic Communications Code.

TMG also to be considered and merged in the new TTDSG.7 Goal

was to adapt both areas to the GDPR and the ePrivacy Directive and

in particular the requirements from Art. 5 Para. 3 ePrivacy Directive legally secure in national

Implement law.8 According to the original plans of the European Commission

Should a European regulation on privacy and

electronic communication (ePrivacy Regulation) come into force and the ePrivacy

Replace RL. Even at the end of 2021, however, it is still not foreseeable whether and when

there will be such an ePrivacy regulation. If it came to that, it would

TTDSG from the regulation as a higher-ranking right with direct effect in

be replaced by the Member States.

a) Addressees

addressees

of

TTDSG

are

next to

the

providers

from

Telecommunications services, especially providers of telemedia services

according to § 2 para. 2 no. 1 TTDSG. This includes any natural or legal person,

which provides its own or third-party telemedia, participates in the provision or

Provides access to use your own or third-party telemedia. This

definition gives way

in the wording something of the definition of

"Service provider" according to § 2 No. 1 TMG. After that, a service provider is any

natural or legal person who uses their own or third-party telemedia

provides or provides access for use. Since the TMG over the

December 1, 2021 - without the data protection regulations - remains in force,

the different wording harbors the risk of new legal uncertainties. The

No indications can be found in the justification for the law as to why in the TTDSG a

different definition of the providers of telemedia compared to the TMG

has been made. There is hardly any justification under European law in this case

possible, since European law allows the differentiation between telecommunications and

telemedia services.9 The consequence of the slightly different definition is a

further personal area of application of the TTDSG, since also only contributing

People are included in the target group.

b) Territorial scope

According to § 1 para. 3, all addressees are subject to the TTDSG who are within the scope of the

law have an establishment or provide services or work therein

participate or provide goods on the market. According to the explanatory memorandum, “applies

still the market place principle. Subsidiary in relation to the E-Privacy Directive

The applicable GDPR already contains the market location principle, which also applies to the

7 Law implementing Directive (EU) 2018/1972 of the European Parliament and of the Council of

11 December 2018 on the European Electronic Communications Code (recast)

and to modernize telecommunications law (Telekommunikationsmodernisierungsgesetz)

of June 23, 2021 (Federal Law Gazette 2021 I 1858). A remainder of the TMG was preserved, which became the TKG

re-enacted.

8 Bundestag printed paper 19/27441, Federal Government’s explanatory memorandum, page 30.

9 S. Jandt in: Spiecker gen. Döhmann/Bretthauer, Documentation on data protection, 2020, E 6.0 marginal number 20.

Processing of personal data by telecommunications providers applies.

With regard to the processing of personal data by providers of

The market location principle of the GDPR also applies directly to telemedia.”10

2. Delimitation of the areas of application of the TTDSG and the DS-GVO

According to Art. 2 Para. 1, the GDPR applies - with exceptions - to "the whole or part

automated

processing

personal data

as well as

for

the

non-automated processing of personal data

in one

file system are stored or are to be stored". The ePrivacy Directive - and

thus also the national implementation in the TTDSG - aims according to Art.

to an equivalent protection of the right to privacy and confidentiality

and aims to "detail and supplement" the provisions of the GDPR in

Reference to the processing of personal data in the field of electronic

Communication.

As part of the offer of telemedia, there are processes that only

Scope of one of the two regulatory matters

Use of technologies, for example, no personal data

processed, only the specifications of the TTDSG are applicable, but not those of the GDPR

12 However, processes such as

the use of cookies to track the behavior of users where

personal data is also processed and thus the

Areas of application of both the TTDSG and the GDPR are opened. For

In this case, Art. 95 GDPR contains a conflict rule. After that

no additional obligations are imposed on data processing bodies by the GDPR,

insofar as they are subject to special obligations specified in the ePrivacy Directive

pursue the same goal. This conflict of laws rule also applies to national ones

Implementation standards of the directive, such as the TTDSG.

Consequently, the specific provisions of § 25 TTDSG take precedence over the

Provisions of the DS-GVO, as far as the storage and reading of information

personal data are processed in terminal equipment. For the

subsequent processing of personal data, which was only carried out by the

This data can be read from the end device and not subject to any special regulation

are recorded, the general requirements of the GDPR must be observed.

10 Bundestag printed paper 19/27441, page 34.

11 More detailed explanations and examples can be found in EDPB Opinion 5/2019 on

Interaction between the ePrivacy Directive and the GDPR, particularly in relation to the

Competences, tasks and powers of data protection authorities of March 12, 2019, from paragraph 21

remove.

12 p. immediately under III.1.

III.

Protection of privacy in end devices according to § 25

TTDSG

The central standard of the TTDSG with reference to the technologies to be considered here

represents the regulation of § 25 TTDSG. § 25 TTDSG serves - unlike the regulations

the DS-GVO - the protection of privacy and confidentiality when using

Terminal equipment, as guaranteed by Art. 7 GRCh. end users

are therefore protected from unauthorized third parties accessing their terminal equipment

save or read information and thereby violate your privacy.

1. Subject and scope of § 25 TTDSG

The area of application and the control system of the

regulation shown. One focus of the explanations is the evaluation, in

in which cases consent is required in accordance with § 25 Para. 1 TTDSG and in

which cases the exemptions according to § 25 Abs. 2 TTDSG can apply.

a) Principle of the need for consent

§ 25 paragraph 1 sentence 1 TTDSG standardizes the principle that the storage of

Information in the end device of users or access to such

Information that is already stored in the terminal equipment, only with

consent of the end users are permitted.

b) terminal equipment

For the opening of the scope of the standard will not be sent directly to a

Telecommunications or telemedia service linked, but on the

Terminal equipment switched off - the title of the chapter reads accordingly,

to which § 25 TTDSG belongs, "terminal equipment".

Terminal equipment is legally defined in § 2 Para. 2 No. 6 TTDSG as "any direct or

indirectly to the interface of a public telecommunications network

connected device for sending, processing or receiving

News; for both direct and indirect connections, the

connection can be made by wire, optical fiber or electromagnetically;

with an indirect connection is between the terminal equipment and the interface

of the public network switched a device. "The explanatory memorandum is to

It can be seen that this broad scope of application was deliberately chosen in order not to

only allow communication via classic telephony and the Internet (Voice-over-IP).

capture, but also the variety of items that

in the meantime -

wired or via WLAN router – to the public communication network

connected.13 Beyond laptops, tablets or mobile phones, this applies

also the area of the Internet of Things (IoT), e.g. B. smart home

13 Bundestag printed paper 19/27441, page 38.

Applications such as kitchen appliances, radiator thermostats or alarm systems, as well

Smart TVs or networked vehicles, if and to the extent that they have the

appropriate communication functions. He finds his limit

Scope where technical facilities do not use the "Internet" as

public

telecommunications network

tied together

are

(e.g.

isolated

corporate networks).14

c) Information storage and access

According to § 25 Abs. 1 S. 1 TTDSG the storage of information in the

Terminal equipment or access to information already in the terminal equipment

are stored, the consent of the end users. The rule

is

formulated in a technology-neutral way in this regard, so that all technologies and processes are covered

can be used to store and read information.

Art. 5 para. 3 ePrivacy Directive in the version of July 12, 2002 pursued the goal, so

called "spyware", "web bugs", "hidden identifiers", "cookies" and similar

to regulate instruments by which, without the knowledge of the user in his

Terminal can be penetrated to gain access to information or

to trace user activity.15 In the new regulation of Art. 5 Para. 3

ePrivacy-RL in 2009 concrete examples were cookies, spyware or

Viruses are listed.16 In general and also in legal usage

Art. 5 Para. 3 ePrivacy-RL often abbreviated only referred to as cookie regulation,

since cookies are probably the most important storage option so far in practice

and for reading out information. A storage of information in

Within the meaning of the regulation, e.g. B. also through

Web storage objects (local and session storage objects).

Outside the website context, automatic update

Hardware or software functions for storage or reading

of information on the end devices, with the result that according to § 25 para. 1

TTDSG consent is required. For mobile devices are as special

practical cases of access to hardware device identifiers, advertising

Identification numbers, telephone numbers, SIM card serial numbers (IMSI),

Contacts, call logs, Bluetooth beacons or SMS communication.

For all devices, it is also possible to read out the unique identifiers of the network

Hardware (MAC addresses) must be taken into account.

So-called browser fingerprinting is now also frequently used

Mission. This denotes the process of server-side formation of a possible

unique and long-lived (hash) value or image as a result of a

mathematical calculation of browser information, such as

Screen resolutions, operating system versions or installed fonts.

14 Bundestag printed paper 19/27441, page 38.

15 S. Recital 24 f. of the ePrivacy Directive.

16 S. Recital 66 of the ePrivacy Directive.

Access is a targeted and not initiated by the end user

transmission

the

Browser Information

in advance. Become

exclusively

Information, such as browser or header information, which inevitably

or due to (browser) settings of the end device when calling up a

Telemedia service are transmitted, this is not considered "access to information,

already stored in the terminal equipment". Examples are:

 the public IP address of the terminal device,

 the address of the accessed website (URL),

 the user agent string with browser and operating system version and

 the set language.

In contrast, it is already available as access to information on terminals

Evaluate end users if active - for example using JavaScript code -

Properties of an end device are read out and for the creation of a fingerprint

be transmitted to a server.17

The processing of the transmitted browser information into a fingerprint and

its use for specific purposes is not straightforward in either case

permissible, but must, if there is a processing of personal data

come, meet the requirements of the GDPR.

d) No personal reference required

In contrast to the data protection regulations, § 25 paragraph 1 justifies

TTDSG requires consent for the storage and/or reading of

Information on or from a device regardless of a personal reference

of information. This is already clear from the wording of the provision

made that it goes beyond the scope of the GDPR.

In its “Planet49” decision of May 28, 2020, the BGH based on the

Delimitation of the regulatory area of Art. 5 Para. 3 ePrivacy Directive to the GDPR

performed the following:

"Art. 5 Para. 3 of Directive 2002/58/EC does not affect the subject of the regulation

VO (EU) 2016/679, according to Art. 1 Para. 1 DS-GVO the processing

personal data, but the storage of or access to

Information stored on the user's device. This

Difference in scope is due to the different

Protective purposes of the regulations concerned: During the VO (EU) 2016/679

according to its Art. 1 Para. 2 DS-GVO and its recitals 1 and 2

Fundamental rights and freedoms of natural persons and in particular

their right to the protection of personal data guaranteed in Art. 8 GRCh

protects data, Art. 5 Para. 3 of the RL 2002/58/EG, as can be seen from their

17 On the application of the ePrivacy Directive to browser fingerprinting, see Art. 29 Data Protection Working Party,

Application of Directive 2002/58/EC to the use of the virtual fingerprint (WP 224).

8th

Recitals 24 and 25 and recitals 65 and 66 of these

Directive changing RL 2009/136/EG results in Art. 8 Para. 1 EMRK

and (meanwhile) guaranteed by Art. 7 GRCh protection of privacy

user. Art. 5 Para. 3 of the Directive 2002/58/EG should warn the user before any intervention in

protect his privacy, regardless of whether it involves personal

Data or other data are affected […]. Consequently, the regulation of Art.

5 Para. 3 of Directive 2002/58/EC on the scope of application of the Regulation (EU)

2016/679.”18

Since § 25 TTDSG the requirements of Art. 5 Para. 3 ePrivacy-RL into German law

is to implement, the same considerations apply to the delimitation of the national ones

Regulation on the GDPR. For the use of cookies, this means, for example,

that the consent requirement according to § 25 TTDSG applies regardless of whether in

the cookie personal data, e.g. B.

in the form of a unique

identification number, are stored or are to be accessed.

e) Bundling of Consents

The consent to the storage and reading of information according to § 25

Para. 1 TTDSG is required, and the consent, which serves as the legal basis for a

planned further processing of the read data in accordance with Art. 6 Para. 1 lit.

GMOs may be required, considering the following

conditions are granted by the same action19.20 However, this presupposes that

that the providers of the telemedia service already inform the users of this

Inform body about all purposes of data processing that take place after the

Access to the terminal should take place. Here it is important to ensure that

it must be clearly recognizable from the query that a single action, e.g.

pressing a button,21 multiple consents are given. Become

users, e.g. B. by means of a banner, asked on a website, a

To give consent to the use of cookies without the wording of the

consent, the follow-up processing is also addressed, this is the case

not a bundled consent according to TTDSG and DS-GVO, but only

for consent according to the TTDSG.

2. Consent Requirements

In contrast to the previous regulations in § 94 TKG a. f

and § 13 para. 2 TMG a. F. Not telecom or telemedia specific

Requirements for Consent. § 25 para. 1 sentence 2 TTDSG refers both to the

18 BGH, judgment of May 28, 2020 - I ZR 7/16 para. 61 - Cookie consent II (Planet49).

19 EDPB, Guidelines 01/2020 on the processing of personal data in connection with connected vehicles and mobility-related applications, version 2.0, footnote 17.

20 For the delimitation of the processes, see above under I. and II.2.

21 In the context of this guide, button means any interactive possibility with which end users can make a statement, e.g. B. using a slider, selection field, box or button.

Information obligations towards the end users as well as the formal and content-related requirements for consent to the GDPR. is therefore decisive the definition according to Art. 4 No. 11 DS-GVO. The other requirements for a effective consent results from Art. 7 and Art. 8 DS-GVO.22 For the assessment the effectiveness of a consent according to § 25 Abs. 1 S. 1 TTDSG are accordingly to apply the same assessment standards as for consent in accordance with Art. 6 Paragraph 1 lit. a GDPR.

According to Art. 4 No. 11 DS-GVO, consent is always voluntary for the specific case, in given in an informed manner and unequivocally Expression of will in the form of a declaration or another clear one affirmative action by which the data subject indicates that they consent to the processing of your personal data is. Articles 7 and 8 GDPR also set further conditions, e.g. for the revocation and for children's consent.

The following essentially result from these legal requirements Test points for assessing the effectiveness of consent in the context of § 25 paragraph 1 TTDSG:

 Consent of the end users of the end device,

 time of consent,

informedness of the consent,

 unequivocal and unequivocally affirmative action,

 related to the specific case,

 voluntary declaration of will,

 Possibility to withdraw consent, which must be as simple as

the grant.

These characteristics of consent are explained in more detail below.

a) Consent of the end users of the end device

According to § 25 TTDSG, the consent of the end user of the end device is required

necessary. In the TTDSG there is no definition of "end user" or

"End User" included. The term comes from the telecommunications law and

will also, for example

used in § 6 TTDSG. become accordingly

End users in § 3 No. 13 TKG, which also applies in the TTDSG according to § 2 Para. 1 TTDSG,

legaldefined as users who are neither public telecommunications networks

operate nor provide publicly available telecommunications services. The

In telecommunications law, the term end user is primarily used for differentiation

to providers of telecommunications services, but not for specification

22 The application of these provisions of the GDPR is in line with the European requirements,

because Art. 2 S. 2 lit. f of the ePrivacy Directive refers to Art. 2 lit. h for the definition of consent

Privacy Policy. When considering this reference, it should be noted that the Data Protection Directive

was repealed by Art. 94 Para. 1 DS-GVO with effect from May 25, 2018. Since then apply

according to Art. 94 para. 2 DS-GVO references to the repealed directive as references to the DS-GVO.

or even limitation of the personal scope of § 25 TTDSG. In the

In contrast to data protection law, no subjective “affectedness” is required.

Rather, what is required is the consent of the person who objectively

terminal uses. ownership of the terminal

basically the same

irrelevant as the question of who contracted:in the

Telecommunications service is accessed by means of the terminal device

is taken.

b) time of consent

First of all, it must be ensured that a corresponding declaration of intent already exists

must be granted before access to the terminal device requires consent

he follows. Accordingly, it is not permitted if cookies requiring consent

already set when a website is called up for the first time and only then

consent is requested.

c) Informedness of the consent

Consent must be obtained in an informed manner. Which information specifically

are to be granted, results - in contrast to the enumeration of necessary

Information according to Art. 13 DS-GVO - not directly from the law. The

The characteristic of "being informed" requires at least that any storage and

Selection activities must be transparent and comprehensible. This means in

In the context of Section 25 (1) TTDSG, users e.g. get knowledge about it

need to know who accesses the respective end device, in what form and to

what purpose, how long the cookies have and whether third parties have access

on it.23 For this it is also necessary that already when accessing

on the terminal device is sufficiently informed as to whether and, if so, to what extent

Access to other data processing processes that meet the requirements of the DS
GDPR, with the specific purposes of the subsequent processing being precise
are to be described.24 To assess the implications of giving consent to
clarify, must finally also be informed about the fact that a
later revocation no longer refers to the
Lawfulness of the access that took place up to the point of revocation or that took place up to that point
storage affects.

In connection with websites and apps, there is often a deficit that
the banners with which consent is to be obtained are designed in a non-transparent manner
are, so u. the purposes of accessing an end device and the actors involved
are not sufficiently recognizable. A lack of transparency can also result from the fact that
it is unclear which button can be used to achieve which effect and how or

23 CJEU, judgment of October 1, 2019 – C-673/17 – Planet49, paragraph 75 et seq.

24 EDPB, Guidelines 01/2020 on the processing of personal data in connection with
connected vehicles and mobility-related applications, version 2.0, p. 16, from para. 49.

with what effort a rejection of processes requiring consent
is possible.

Transparency also requires that the information contained within a
Telemedia offerings are made available at various points,
are congruent. In practice, websites and apps are regularly noticed in which
Banners for the consent request contain different information than in the
Data protection declaration, in particular other legal bases, other third-party providers,
other purposes. Providers of telemedia who share their data protection information
update with a view to § 25 TTDSG, must also pay attention to the processes
to be clearly differentiated - if within the scope of the telemedia offer processes

take place, which fall under both the TTDSG and the GDPR, is about the

to inform each of the two legal bases separately.

d) Unmistakable and unequivocally affirmative action

Art. 4 No. 11 DS-GVO also requires an effective consent

“unmistakably given declaration of intent in the form of a declaration” or

another clear confirmatory action with which the user agrees

understand that they are engaged in accessing and retrieving information

expressly agree. Active action is therefore always required

end users. This can be done, for example, by clicking on a designated

button in a banner, by selecting technical settings or by

any other explanation or active behavior happened with the

End users clearly give their consent to the storage of or

express access to information in the terminal equipment.

Silence, already ticked boxes or inaction of the user

do not represent consent.25 Opt-out procedures are therefore always

unsuitable to justify an effective consent. The fact that the

End user browsers Cookies or web storage, e.g. B. Local Shared Objects

(LSO) allows, can accordingly also - regardless of other aspects such as

Awareness or specificity - do not constitute consent.

The mere further use of a website or app, e.g. B. by actions like that

Scrolling down, surfing through website content, clicking on content or

similar actions can also not be valid consent for access to

or represent the storage of information on a terminal device. This

Actions can under no circumstances prevent the use of cookies that require consent

or similar technologies - even if by means of a banner over

the processes are informed. Scrolling or continuing surfing are typical

Acts when using the Internet, which in principle no legal

explanatory content inherent. Art. 4 No. 11 DS-GVO expressly requires a

unequivocal affirmative action, so that an activity or interaction of the

25 S. Recital 32 of the GDPR.

users is required, which is a clear turning point in the further use of the

telemedia offer.26 Only then can the various

Actions clearly distinguished from each other and an unequivocal agreement

to be determined.

Whether there is an unequivocal declaration of intent when end users

Have given consent via a button also depends on whether this

could express their true will directly or unequivocally

could see how the true will can be expressed. In the

Evaluation is therefore included, as are the buttons for giving consent

and other options for action are labeled and designed and which ones

Additional information will be made available.

If consent banners are displayed in telemedia offers, which only

contain an "Okay" button, clicking the button does not provide any

unequivocal statement. The designations “Agree”, “I agree

a" or "accept" may not be sufficient in individual cases if from the

accompanying information text does not clearly indicate what specifically the

consent should be granted. Frequently, users must first have an im

Open consent banner integrated detail view to see which ones

Preferences are set to "Accept" in the event of a click and from this

deduce what the consent ultimately refers to. Such designs

also regularly stand in the way of effective consent.

In addition, end users may reasonably have the expectation that

they can simply remain silent if they do not wish to consent. In cases in

who are unable to remain idle because a consent banner den

Access to some or all of the content of the telemedia offering must be blocked

End users: inside their rejection at least without additional effort in clicks (compared to

of consent). This rating is also supported by recital

32 S. 6 of the GDPR, which specifies the requirements for consent. Therefore

the request must be clear and concise and without unnecessary interruption

of the service for which consent is given, if the data subject

person is requested to give their consent electronically.

Effective consent is also regularly not given if the user only

two courses of action are offered to choose from, which are not equally fast

lead to the goal of being able to use the telemedia service. Here you will

On the one hand an "Accept all" button is displayed, on the other hand

Button with labels such as "Settings", "More information" or

"Details". Using the first button, end users can directly and

submit a consenting declaration of intent without any further effort and that

Use the offer immediately. With the other button, users can neither

refuse to make any other declaration of intent, but only further

26 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, p. 22, example

16

Initiate action steps. It then requires further decisions or

Settings until the desired offer can be used. These two

Options for action therefore do not have the same communication effect. If

In this constellation, users select the only available button with which

immediately submit a declaration of intent that ends the decision-making process

can be, this action can also be inherent in the will to deal with the

simply no longer having to deal with the matter. This applies all the more

if not even clear based on the concrete labeling of the buttons

to realize how much overhead is required to get a rejection

to share.

In order to be able to prove that end users have an unequivocal and

have submitted an unequivocally confirmatory action, must therefore at least do so

such selection options are offered, their communication effect

is equivalent. Is a selection option precisely represented and generated immediately

one effect (e.g. an "accept all" button), while the other option

is kept nebulous and does not allow having the true opposite will

to express the same effort, there is an effect and information deficit. A

Such a deficit is likely to motivate end users to change their decision

not according to the clear will, but only to make which option the

Consent query ended significantly faster. Will the beneficiaries no

offers equivalent options for action in order to give consent

or to refuse them, these are the requirements for effective consent

regularly not before.27

e) Related to the specific case

In addition, consent must be obtained for the specific case. It

is therefore not possible, a general consent or blank consent for the

general use of certain techniques, e.g. B. Cookies, or for various potential

obtain follow-up processing. The requirement of certainty is closely related to that

Feature "in an informed manner" related and also overlaps with the

Criteria for whether consent was given voluntarily. Before consent

is queried must have a clear and legitimate purpose for the intended purpose

Processes are defined in order to then sufficiently inform the end users about this

to be able to inform. Already the Art. 29 data protection group as a predecessor of the

European Data Protection Board has pointed out that

Certainty requirement not through vague or general information such as

"Improvement

the

Experiences

of

user",

“promotional purposes”,

"IT

security purposes” or “future research”.28 At this

27 Some providers of telemedia give users a choice, as an alternative to granting a license

Consent to sign up for a paid subscription. This particular constellation is not

Subject of the preceding remarks and assessment.

28 Art. 29 Working Party Opinion 03/2013 on purpose limitation (WP 203), p. 16.

The requirement has not changed as a result of the GDPR either.29 Only if the

end users have sufficient information available for all purposes,

to which the terminal device is to be accessed, these can be used at all

understand for which cases they give their consent. Into the different

End users must then also give their consent separately for these purposes

can refuse. If the necessary granularity is missing, this also has more

Effects on the voluntariness and thus the effectiveness of the consent. Then

Recital 43 of the GDPR makes it clear that consent

regularly is not considered to be given voluntarily even if to different

Consent cannot be given separately for processes, although this is in the

relevant case would be appropriate.30

In principle, it is possible to design consent banners in several layers, i.e

to communicate more detailed information only on a second level of the banner

which users can access via a button or link. However, if already on the

first level of the banner there is a button with which consent is given

Various purposes may need to be granted at this first level as well

specific information must be included for each individual purpose. Too vague

would it be just generic, general or vague information about the

specify purposes such as B. “To provide you with a better user experience

we use cookies".

f) Voluntary consent

Finally, the consent is only effective if the expression of will is voluntary

he follows

is. It says about this

in the guidelines 05/2020 of the European

Data Protection Committee for consent:

"The element 'free' implies that the individuals concerned have a genuine choice

and be in control. In general, the GDPR requires that a

Consent is not valid if the data subject has no real choice

feels compelled to consent, or suffers adverse effects

must if she does not agree. […] Consent will not be given accordingly

considered voluntary if the data subject does not provide consent

refuse or withdraw without suffering any disadvantage. In the GDPR

also becomes the concept of "imbalance" between the responsible

and the data subject is taken into account.

In principle, consent is rendered inappropriate by any form

pressure or influence (which manifests itself in many different ways

can manifest) on the affected person who has this from the exercise

of their free will, ineffective."31

29 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, paragraph 55.

30 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, paragraph 43.

31 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, paragraphs 13 and 14.

According to recital 42 sentence 5 GDPR, it should be assumed that

the data subject has only given their consent voluntarily if they

has real and free choice and is therefore able to withhold consent

or withdraw without suffering any disadvantage. It should also be taken into account whether

among other things, the fulfillment of a contract is made dependent on the fact that in

data processing is consented to which is not necessary for the fulfillment of the contract

is required. According to Art. 7 Para. 4 DS-GVO, such a coupling leads regularly

to the fact that the consent cannot be considered voluntary and thus

is ineffective.32

When evaluating whether consent is given for access to end user devices

was granted voluntarily, it must first be clarified whether there is any compulsion for the

End users insisted on providing a statement, or whether they would have been idle

can stay. It can be assumed that such a compulsion exists if a

Banner or other graphic element for consent request access to

obscures the webpage in whole or in part, and the banner is not simple

can be closed without a decision.33

It is true that some in the literature assume that nobody is forced to

To visit a website whose content is basically also made by others on the market

is offered. However, this argument cannot prevail. As already the

European Data Protection Board (and its predecessor institution) clarified

consent cannot be considered freely given because

between a service to which the consent

into use

personal data for additional purposes, and a comparable one

Service offered by another controller, a

There is a choice.34 In such a case, the choice would be from

Behavior of other market participants and depends on whether an affected

Individual responsible for the services of the other really as

would consider equivalent. This would also mean that the

those responsible would have to follow market developments in order to

continued validity of consent

in the data processing activities

ensure that a competitor offers its services at a later date

time could change. Consent per se cannot therefore only be taken as

be qualified voluntarily if those affected theoretically consider alternative options

could have turned to that offered by a third party. This reasoning that too

data processing processes was taken,

is to access

Terminal equipment is transferrable, since the requirements of the GDPR are also met in this respect

are valid.

32 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, paragraph 14.

33 For the cookie walls to be distinguished from this, see EDPB, Guidelines 05/2020 on consent

according to Regulation 2016/679, version 1.1, paras. 39-41.

34 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, paragraph 38.

The characteristic of voluntariness is also noticeably influenced when the
Refusal of all access requiring consent involves a measurable additional effort
end users means. Such additional effort is z. B. generated by the
Rejection only on a second banner level, and thus only with a higher one
Number of clicks possible (compared to consent). The extra effort
usually does not just consist in the fact that the end user once more
have to click than when agreeing. Rather, you must also
the additional information and setting options that you can use on a
be confronted with the second level of consent dialogues, read, understand
and then select the appropriate one from the other selection options. The
The additional effort generated cannot be objectively justified (e.g.
with technical obstacles), but is artificially constructed. This is possible
not least conclude from this that end users now have access to a large number of
there is an equally simple opt-out option to choose from on websites
is provided.

If users ask for consent when calling up a telemedia offer
cannot simply ignore, because this covers the content of the offer, it is missing
thus regularly in the voluntariness of the consent if the granting of the
Rejection with a higher effort, e.g. B. in clicks and attention,
connected is. To ensure they demonstrate effective consent
can, providers of telemedia must therefore urgently pay attention to the
to make the options available for selection equivalent.

At this point, the principle of good faith is also included in the assessment
to include Art. 5 (1) lit. a GDPR. Can't have any real reason for that

be put forward why e.g. B. None associated with the same effort

Opt-out option is offered on the first level of a cookie banner

this represents an attempt to influence the end users in an unfaithful manner

take. In connection with telephone advertising, the Federal Court of Justice

decided that consent is ineffective in any case if the

Design is designed to prevent those affected from exercising their right to vote

to hold.35

g) Possibility to withdraw consent

From Art. 7 Para. 3 Sentence 4 DS-GVO it follows that the revocation of a consent

must be just as easy as granting it.

If the consent is given immediately when using a website, it must also be

their revocation may be possible in this way. Not conforming to specifications

exclusive revocation options via other communication channels such as e-

Mail, fax or even by letter. It is also inadmissible to use a

point out the contact form, since in this case the same communication channel is used

(i.e. via the website) is used, but the requirements are significantly higher

35 BGH, judgment of May 28, 2020 - I ZR 7/16 para. 37 - Cookie consent II (Planet49).

than when the consent was given (and data collected using the contact form

would not be necessary for the revocation). Was consent obtained by means of

Banners or similar queried, it is therefore also inadmissible if initially a

Called up the data protection declaration and then scrolled to the right place in it

must be made in order to obtain a possibility of revocation. Such a

Search process as an intermediate step would be a complication with the legal

specifications is not compatible. This detour is also not due to a technical one

Impossibility to trace back, since a large number of websites always have a visible one

Direct link or a

Show icon that goes directly to the

relevant

setting options. It only satisfies the legal requirements

Not right if you opt out at various points in the data protection declaration

Possibilities on different external websites are pointed out.

Note: Use of consent management platforms

To implement a comprehensive consent solution are increasing

Consent Management Platforms

(CMP)

used, the

from

numerous

companies are offered. These often advertise that with the use

their tool legally compliant consent would be obtained on the website. If

this is actually the case, however, depends largely on the specific use of the CMP

and the exact processes on the respective telemedia offer. The

Website operators have numerous configuration options, see above

that just by using the CMP is by no means automatically legally compliant

consents are obtained. Responsibility for the effectiveness of

The consent obtained remains with the

respective providers of the

telemedia offer.

3. Exceptions to the requirement for consent

There are two of the principle of the need for consent in Section 25 (2) TTDSG

exceptions provided. The first exception is primarily aimed at providers

of telecommunications services within the meaning of Section 3 No. 1 TKG nF The second exception

in contrast, addresses the providers of telemedia in accordance with Section 2 (2) No. 1

TTDSG.

a) Carrying out the transmission of a message

According to Section 25 (2) No. 1 TTDSG, consent is not required if the

sole purpose of storing information in the terminal equipment or the

sole purpose of accessing already in the end device of the user

information stored about the implementation of the transmission of a message

is a public telecommunications network.

18

b) Provision of a telemedia service

§ 25 para. 2 no. 2 TTDSG does not require consent if the storage of

Information in the terminal or access to already in the terminal

stored information is absolutely necessary so that providers: inside a

Telemedia service one expressly requested by the respective user

can provide telemedia service.

In the legislative process for the TTDSG and also in the European process

to the enactment of the ePrivacy Regulation, it was and is becoming clear that there are many

Efforts are significantly more exceptions to the consent requirement

permitted than is currently provided for in Art. 5 Para. 3 Sentence 2 ePrivacy Directive. Nonetheless

the German legislator has decided to very closely am

To be based on the wording of the European regulation and none over Art. 5 Para. 3 Sentence 2

exceptions that go beyond the ePrivacy Directive. The regulation contains

Essentially two elements of the offense that are fundamentally in need of interpretation

– these are “a telemedia service expressly requested by the user” and

"absolutely necessary". Both constituent elements are inseparable

Connection. The absolute necessity of storing and reading processes

is in relation to what is specifically desired by the end user

to check the telemedia service to determine whether the exemption applies.

When examining the requirements, it should be noted that § 25 TTDSG is a different one

systematic as Art. 6 Para. 1 DS-GVO. § 25 TTDSG sees only two

Possibilities of legitimacy. Either there is an effective consent of

End users before or there are the requirements of one of the two in paragraph 2

regulated exceptions are met. Art. 6 para. 1 DS-GVO, on the other hand, provides for several

Possibilities for the lawful processing of personal data before, by

where the consent according to Art. 6 Para. 1 lit. a DS-GVO is only one of several

equal variants.

The exceptions according to § 25 paragraph 2 TTDSG also differ significantly from

Art. 6 (1) lit. f GDPR, which expires on November 30, 2021

Supervisory authorities under narrow conditions as a possible legal basis

has been viewed. While the TTDSG specifies rigid criteria that must be met

must, the GDPR opens up a certain flexibility of consideration. No way is one

Weighing of interests, which was carried out in accordance with Art. 6 Para. 1 lit. f GDPR,

suitable, automatically the requirements of § 25 Abs. 2 Nr. 2 TTDSG

justify. In order to implement the new legal situation, it is therefore not sufficient

if only the designation of the legal bases in a data protection declaration

is exchanged.

ah. Telemedia service expressly requested by end users

The assessment of whether the use of a telemedia service is expressly

end user requires, as a result, an inner, personal

determine setting. This can only be based on objective criteria, such as in particular

derived from the actions of the users. In the context of websites and

Apps generally make use of a telemedia service by

they consciously invoke him. This is done regularly by entering the URL of the

Web page in a browser, by clicking on a link on a previously made one

Search in a search engine or install an app. That one act

does not, however, allow the conclusion that what is hidden behind the URL or app

or via the link to the entire website, possibly including various ones

subpages is expressly desired.

It is therefore crucial what understanding of the term "telemedia service" in the

connection with Section 25 (2) No. 2 TTDSG. This can be

on the one hand globally, e.g. B. a website as a whole, as well as granular, e.g. B. only one

interpret certain functions or certain contents of a website. The

A company's website can B. Information about the company, a

Online shop, contact options via contact form, an integrated chat,

contain a route planner to the company as well as own and third-party advertising.

Generally to an entire range of telemedia, possibly including various subpages,

to be turned off, in particular with regard to highly complex websites and

Apps regularly not the right benchmark. Article 5 implemented by § 25 TTDSG

Para. 3 ePrivacy-RL refers to “a participant or user expressly

Desired Information Society Service”. With many offers will not

"one" service, but a bundle of services with different functions

offered, which when visited by the individual users is hardly always all

be used. These services are intended specifically for the addressees of the

websites or apps and not as an end in itself. track at the same time

Providers of the websites or apps or integrated third-party service providers

personal interests beyond that. The differentiated view of a

Website or app corresponds to the purpose of the standard, only those interference with the

To allow users' end devices that are absolutely necessary in the specific case

are, because without them the service specifically desired by the individual user would not be possible

can be provided. If you were to focus on a website or app as a whole,

providers of telemedia would have it in their hands, through comprehensive embedding

various not used in practice, but with some very invasive ones

Data processing of related functions the scope of the telemedia service

to be determined arbitrarily. The user's wish would remain global

interpretation ignored. Accordingly, Art. 29-

Data protection group on the ePrivacy Directive for such a granular view of the

pronounced service. According to this, a service is the sum of different ones

functions and can therefore depend on the users

called functions have a different scope.36

36 Cf. Art. 29 Working Party on Data Protection, Opinion 4/2012 on the exception of cookies from the

Obligation to consent (WP 194), p. 4.

It is therefore first to be determined which user request results from calling up the

Website or the app can be closed.37 Every telemedia service has

initially a basic service that is inseparable for the entire offer of

meaning is. The basic services can be regularly selected from the category of

Derive telemedia service. Examples of categories are web shops,

Search engines,

information pages

from companies

or

public

Institutions, government portals, online banking, blogs, social networks,

called translation services. The basic service of a web shop is the sale of

products. Basic service of a search engine is that when entering a search term

matching websites found on the internet and via hyperlinks as search results

be listed. The basic service is often flanked by components so that this

can be made available securely, quickly and stably. Such systems for

user-oriented fraud prevention and

IT security basically serve

equally the users and the operator of the website and can dem

be charged for basic service. For certain categories of telemedia services

there are other user-oriented additional functions through which the basic service

is supported, such as the shopping basket function in online shops. The

Additional features are built into the basic service, but are coming for some

Users not at all or not over the entire period of use of the

offer to wear. In addition to these basic services, users are becoming frequent

Additional services and features provided that are fundamentally independent

are of the category of the telemedia service, e.g. B. language settings,

Chat boxes, contact forms, push messages, map services, weather services,

Videos and audios, log-in areas including authentication, advertising, management of

Consent by means of consent management tools, watch lists or favorites lists.

At least there is

in the context of private law, basically one

Freedom of design for providers of telemedia services. With which

Functionalities providers, e.g. B. an online shop, a news site

Equip a rating portal or a social network therefore suits them

basically free. However, § 25 Paragraph 2 No. 2 TTDSG due to the wording

"Telemedia service expressly desired by the user" explicitly on the

perspective of the users, which is therefore to be significantly included.

The basic service

is basically the one desired by users

view telemedia services as soon as they consciously call up a service. Out of

However, this action does not automatically lead to the conclusion that

the user wants all the additional functions of the basic service. Which

range of functions is desired is average in individual cases from the perspective

to be judged by knowledgeable users. The basic service of web shops has e.g. B.

a shopping cart function and integrated payment functions. However, these are only

then desired by users when a product is actually in the shopping cart

37 How the user request is then implemented must be assessed in a further step, see below

under bb. Absolutely necessary.

placed or a number function is selected. Additional services and functions that

can be used independently of the basic service, such as

e.g. B. a contact form, a chat or a map service, are also not

automatically when the user calls up the website or app for the first time

desired. Users often have none before calling up the offer

further knowledge of the exact scope of services and functions

the website or app. Users “wish” the ones mentioned as examples

Additional services and functions only if you explicitly use them, e.g. B.

click on a chatbot, create a watch list or fill out a form. The

express request of the user in relation to these additional services and -

functions must therefore be expressed in further actions. This means in

website context that users do not have any access to their end device,

in particular, have to accept the setting of cookies just because a website

or an app was actively called up. Users must first be aware

(can) find out that there are additional services and functions to which

Providing access to the terminal equipment is required, and a

Use additional function consciously.

Finally, additional general functions can be added to websites or apps

be integrated, such as the measurement and/or analysis of visitor numbers

or A/B testing. These are not per se attributable to the basic service. The

However, users are regularly unable to consciously perceive them and

therefore do not select actively. Here it is important for the evaluation whether the

concrete, very differentiated purposes of the functions

be user-oriented.

bb Absolutely necessary

The feature "absolutely necessary" is neither in the TTDSG nor in the ePrivacy Directive

defined in more detail. In the explanatory memorandum to the TTDSG, however, one

technical necessity, which suggests a strict understanding.38

This means that also for services expressly requested by end users

only those accesses to the terminal device are covered by the exception that

are technically necessary to provide the requested service.39

Because the criterion of necessity within the meaning of the provision refers

solely on the functionality of the telemedia service as such. One

An exception to the need for consent can therefore not be justified by this

that the storage of or access to information in the end device

is economically necessary for the business model in which the telemedia service

is involved.

38 BT-Drs. 19/27441 p. 38.

39 See also Recital 66 of the ePrivacy Directive: “Exceptions to the information obligation and the granting of the right of refusal should be limited to those situations where the technical storage or access are essential to the use of a participant or to enable the user to provide the service that he or she has expressly requested”.

In addition to the question of "whether", the criterion of absolute necessity still has temporal, content and personnel dimensions. are always to be taken into account the time of storage (when?) and the duration of the cookie (how long?), the Content of the cookie (What?) and the setting domain of a cookie, the above decides who can read the information (for whom?). Access to the Terminal equipment and access to the information are within the meaning of the standard to reduce all dimensions to the required minimum.

Cookies for any additional functions, e.g. B. for storing products in the Shopping cart or making a payment, may be in terms of time Dimension regularly only considered as absolutely necessary if a corresponding user interaction has taken place, i.e. actually an article placed in the shopping cart or the payment process was initiated. For a mere Use of the offer, e.g. B. browsing in a web shop, it is not required that the shopping cart and payment functions are already activated. Also In the case of individualized cookies, the validity is often only for one session to be required. According to Section 19 (1) TTDSG, it can be generally assumed that that under the use of a telemedia service a single usage process understand, i.e. a session.40 Regular use of the telemedia service by certain end users, it can generally only be assumed that if it is a subscription-based service.

Based on the purpose of § 25 TTDSG, the privacy of end devices

protect, in terms of content, processes are to be questioned in particular

which unique identifiers (cookie UIDs) are assigned,

because these in particular result in invasions of privacy. For such

Storage is only absolutely necessary in a few cases, since

many functions by means of storing information on and the

Reading of these from end devices of the users should be implemented without

Individualization can be done. For example, it is not considered necessary to

consider that for storing consent or for load balancing

Cookie with a unique ID is stored in the long term and can be retrieved

can. The same applies to saving settings for the language or background

Color. This is not a unique identifier such as a unique

User ID required, but storing one is not enough

identifying information such as B. "background-color: black" or "language: de".

Also the question of who can access the information is in view of that

Strictly check the necessity criterion.

In connection with the storage of consents given by users

a website, requires the fulfillment of the obligation to provide evidence

§ 25 paragraph 1 sentence 2 TTDSG i. In conjunction with Art. 7 (1) and Art. 5 (2) GDPR none

persistent UID cookies. As a rule, it is sufficient to be able to prove that and

40 In the context of websites, a usage process is usually ended when the user

Actively close the website or browser.

which processes have been implemented to obtain consent and that

Result in a cookie with no UID or other excess information

to take off

Finally, it should be noted that while it is possible to use a

To store information in a terminal to access it, that is z. B.

use a cookie for different purposes. But such a one can

Multi-purpose cookies can only be exempted from the consent requirement if

if for each individual purpose for which the cookie is used, the

Prerequisites for the exception according to § 25 Para. 2 No. 2 TTDSG are met.41

c) Application examples and test criteria

Numerous processes and third-party services are used on websites and apps

fall within the scope of § 25 TTDSG and with those very much

different purposes are pursued. Meanwhile, some have

Designations and formulations developed, which are used regularly around

these services

to

categorize as

e.g.

B.

range measurement,

Website optimization, fraud protection and personalized services. From the point of view of

It would be desirable for those responsible if the supervisory authorities issued a statement

to determine whether, for example, a range measurement according to § 25 para. 2

No. 2 TTDSG in principle without the consent of the end users of a website

may be used. For many reasons

find each other

in this

Guidance no such statements. This is shown below using the example of

Range measurement clarified.

First, the terms commonly used are too vague. The

Reach measurement originally comes from the area of analogue media. At
Press media and television broadcasts only the number is recorded, how many
Readers, viewers and listeners the respective media offer
has reached. In the case of press media and books, the first step is sales figures
determined. On the air and in terms of the number of actual readers
there is no direct technical possibility, at least in the analogue world, to
determine which viewers or listeners of which radio program
switched on and which readers have read which print medium, so that in
some representative households surveys as a basis for the calculation of
ratings were made. Transferred to the web page context
ratings correspond to a pure count of how often a website is viewed
is called up (page impression). It is sufficient for this every time a page is called up
increase the counter for this page by one, based on log files without
personal data to determine the number of page views or
Simple tracking pixel (of the directly accessed telemedia offer) on the website
to implement, through which no further user data is collected. Offers
41 S. Art. 29 Data Protection Working Party, Opinion 04/2012 on the exception of cookies from the
Obligation to consent (WP 194), p. 6.

from third-party service providers for range measurement on websites or in apps
however, regularly process (sometimes very extensive) information about
users and
make based on this
information much more
Evaluation results available. The evaluations can be rough
A distinction is made between information about visitors, e.g. e.g. devices, software,

times, user IDs and user-defined variables, and information about that

Behavior of users on the website or in the app, e.g. B. Entry and

Exit pages, page titles, internal searches, downloads and submissions. This

Information is used to obtain further insights, such as

for example to analyze and evaluate the average length of stay,

Number of visitors who dropped out, actions per visit, page views,

internal searches, downloads or how users use the website

have called.42

In the website and app context, the original range measurement has therefore changed

using numerous, often individualized pieces of information about a

Reach analysis developed with an indefinite scope that can be expanded to any

criteria can be added.

Even if there is a common understanding of the term reach measurement

or the range analysis, there would be the second problem that with it completely

different purposes can be pursued. Basically, the goal

follows, with insights from the past to make decisions for the future

meet the interests of both the providers of the telemedia offer, the

be used by users or by third parties. Reach analysis of websites

become e.g. B. used to develop business models, the sales value of

to determine advertising space, to better place frequently accessed content,

malfunctions

to

realize the scope

from those regulated by law

to record ancillary copyrights of the authors of published contributions and

much more. The purpose for which reach measurement is used is

however, decisive for answering the question of whether a

the user: in the desired telemedia service is to be accepted. Even the

simple measurement of visitor numbers is therefore not per se part of the

classified as a basic service, but depends on the specific purpose pursued in each case.

Additional problems arise from the fact that the providers of the telemedia

Several purposes are often pursued with the use of individual cookies and

Integrated third-party service providers in turn have other purposes of their own

track information from the cookies.

Thirdly, when integrating third-party services, there is the problem that the process

of storing information on the end device of the user and reading it out

This information is often not just a service with a clearly identifiable

Function is assigned, but represents the basis for several services. As an an example

42 E.g. via a search engine, a social network, another website or from the internal one

Seek.

The providers of consent management platforms are ideal here. Whose

In many cases, the product range also includes marketing services, for example. At the

Using a CMP, a cookie is often set that has a unique

Has user identification, although this is for the purpose of storing the

consent status is not required. In this case the assumption is urgent

that the same cookie can also be used for the marketing service. If

if this is the case, users of the website cannot directly

to be determined.

From the point of view of the supervisory authorities, the relevant test criteria are set out below

summarized, by providers of telemedia in the evaluation

should be considered whether an exception according to § 25 Abs. 2 Nr. 2 TTDSG

present.

Relevant criteria for determining the end user's explicit

Desired telemedia service:

 Granular determination of which function of the telemedia service

specific storage and reading process of information on the end device

he follows.

 Determining whose primary interests this function serves: their own

Interests of the providers, the interests of the users of the website, the

Interests of the integrated third-party service provider or the interests of

third party.

Relevant criteria for determining the absolute necessity:

 Time of storage – when is the readout and storage process allowed

take place?

The storage and reading process of information on the end device is allowed

only begin when the specific function of the telemedia service is

is actually used by the user.

Content of the information – What information is stored and

read?

The stored and read information must be related to the

granularly defined function of the telemedia service is absolutely necessary

be. In particular, when using cookies, there is no general indication

prevent a cookie from being set or read, but the im

Cookie stored information is authoritative.

 Duration of retention of information – How long will information be retained

stored on the end devices and for what period of time

be read out?

The period of storage may only be selected as long as for the

Implementation of the granular function of the telemedia service required. In

26

With regard to the use of cookies, this period is due to their term

to be determined in advance. Basically, session cookies are more likely

required as persistent cookies.

 Readability of the information – for whom is the information from the end device

readable and usable?

Become

Information on the end device of the user at the

saved using a telemedium

technically

it must be ensured that these are subsequently only used by the

operators of the respective website can be read out. At Third-

This is not the case with party cookies, so it must be ensured

that third-party service providers read out

information in principle

exclusively for the website accessed by the user.

IV. Lawfulness of processing according to GDPR

If personal data (e.g. under

collected using cookies and similar technologies).

be used, for example to track the individual behavior of users,

the general requirements of the GDPR must be observed for this. For simplification

Used for processing to track user behavior

hereinafter the term "tracking" is used.43

The processing of personal data is lawful only if

at least one of the conditions of Art. 6 Para. 1 DS-GVO is fulfilled. All of the

The legal bases mentioned in this standard have the same priority and are of equal value

side by side. For the processing of personal data by non-

public responsible in the provision of telemedia services it comes

basically considering relying on a consent according to Art. 6 Para. 1 lit. a) DS-

GVO, to contractual obligations according to Art. 6 Para. 1 lit. b) GDPR or to

overriding legitimate interests in accordance with Article 6 (1) (f) GDPR.

It should be noted that with the integration of third-party content on websites,

a disclosure of personal data to operators of the respective

third party server is connected. According to Art. 6 Para. 1 DS-

GMO requires a legal basis. Typical examples of such third party content are

Ads, fonts, scripts, maps, videos, photos or content from

social media services.

43 This understanding of the term is also used by the European supervisory authorities,

See EDPB, Guidelines 05/2020 on consent in accordance with Regulation 2016/679, version 1.1, paragraph 4.

Note: Accountability

As part of their accountability pursuant to Art. 5 Para. 2, those responsible must

GDPR can prove that the processing of personal data

done lawfully. This means that responsible persons check in advance and

must document the legal basis for the processing

support. According to Art. 13 f. GDPR, the persons concerned must have the

Legal basis for all processing of your personal data

be informed.

1. Article 6(1)(a) GDPR – Consent

The formal and content-related requirements for effective consent result

for both the telemedia-specific and the data protection law

relevant processes from Art. 4 Para. 1 No. 11 i. In conjunction with Articles 7 and 8 GDPR.44 Accordingly

Consent is any voluntary for the specific case, in an informed manner and

unequivocally given declaration of intent in the form of a declaration or a

other clear affirmative action by which the data subject agrees

understand there that

them with the processing of data concerning them

agrees to personal data.

For the assessment of the effectiveness of a consent are therefore fundamental

to apply the standards already mentioned above under III.2. were presented – with

the proviso that the consent must be given by the data subject and

the

to the

Disposal

asked

information

itself

clearly

on

Data processing processes (and not just the technical use of cookies

or similar).45

Finally, Art. 25 Para. 2 DS-GVO must be observed, which is governed by data protection law

Responsible requires appropriate technical and organizational measures

take to ensure that through privacy-friendly defaults only

personal data are processed that are specific to the respective

Processing purposes are required. In addition, by the data protection law

Controllers technically ensure that procedures for tracking

User activities that require consent under data protection law only then

be used if the person concerned has the information about the planned

Data processing recorded content and a decision in the form of an explicit

has made an act of will about it.

44 For the delimitation of the processes, see above under I. and II.2.

45 For the bundling of consents in accordance with Section 25 (1) TTDSG and Article 6 (1) (a) GDPR see

III.1.e).

Note: consent banner

In practice, consent is regularly requested by

first call-up of a website or an app, a banner or similar graphic

Element with buttons appears. About the use of cookies and

However, similar technologies are usually used with such consent banners

consent for subsequent data processing processes is also requested.

Not every use of cookies or the subsequent tracking is per se

requires consent, so appropriate consent banners should only

be used if consent is actually required. Otherwise

creates the misleading impression that the people concerned have a choice

have, although this does not exist.

If operators of websites or apps display such consent banners for the

If you use a query for consent, the following requirements in particular apply

observe:

- This appears when opening a website or app for the first time

Consent banner, for example, as a separate HTML element. Usually

This element consists of an overview of all those requiring consent

Processing operations, naming the actors involved and their

function are sufficiently explained and activated via a selection menu

can. Activate means

in this context that the

Choices must not be “enabled” by default.

- While the consent banner is displayed, none are initially displayed

advanced scripts of a website or app that potentially access the

access the end devices of the users (TTDSG) or their personal data

process (GDPR) and in particular no content from external servers

loaded, as far as the related disclosure of personal data

requires consent. Access to imprint and privacy policy

must not be obstructed by the consent banner.

- Only when users give their consent(s) through an active action, such as

For example, ticking the consent banner or clicking on one

button may have submitted information on the end devices

saved

or

out of

this

read

become,

as well as

the

data processing that requires consent actually takes place.

- The user must be given a consent in the consent banner

be given an equivalent opportunity to refuse consent. If

There is a button for a on the first level of the consent banner

If there is consent in certain processes, there must also be a corresponding one there

button shown to reject these processes.

29

- The submission of consent is stored by the person responsible so that

a further visit to the website, the banner does not appear again and the

Consent secured for verification purposes

is. To the

fulfillment of

It is the obligation to provide evidence of Art. 7 Para. 1 DS-GVO according to Art. 11 Para. 1 DS-GVO

it is not necessary for the users to be identified directly. an indirect one

Identification (see recital 26 of the GDPR) is sufficient. In cases in

which users do not give their consent, this circumstance should be done without

using a user ID or similar are stored on the respective end devices,

to prevent a renewed request to submit a

declaration of intent is displayed.

- Since consent is revocable, there must be a corresponding possibility for

revocation to be implemented. The revocation must be as simple as possible

the granting of consent, Art. 7 para. 3 sentence 4 DS-GVO.

2. Article 6(1)(b) GDPR - Contract

The processing of personal data of the contractual partner on a contractual basis

Basis according to Art. 6 Para. 1 lit. b) GDPR is only possible if the

Data processing to fulfill a contract or in the context of pre-contractual

Measures are required, which are carried out at the request of the data subject. With the

Processing of personal data in accordance with Art. 6 Para. 1 lit. b DS-GVO im

connection with the provision of online services has already

European Data Protection Board busy. The statements in the

Guidelines 2/2019 can therefore be used by providers of telemedia as

standard of audit.46

3. Article 6(1)(f) GDPR – overriding legitimate interests

When processing personal data on the basis of Art. 6 Para. 1

lit. f) GDPR, it must be taken into account that the provision is not a catch-all event

represents. It can therefore be considered equivalent to the other permissions

be used.

The processing is lawful according to Art. 6 Para. 1 lit. f) GDPR if this

Protecting the legitimate interests of the controller or a third party

is necessary, unless the interests or fundamental rights and freedoms of the

46 EDPB Guidelines 02/2019 on the processing of personal data pursuant to Article 6(1).

Letter b GDPR in connection with the provision of online services for data subjects

persons, version 2.0, paragraph 48 et seq.

data subject prevail. Whether the requirements of Art. 6 Para. 1 lit. f) DS-

GMOs are met can be determined using a three-stage test:

1st stage: Existence of a legitimate interest of the person responsible or a

third party

2nd level: Necessity of data processing to protect this interest

3rd stage: Weighing against the interests, fundamental rights and fundamental freedoms of the

data subject in a specific individual case

In the context of tracking, in practice there are only a few constellations

Requirements of Art. 6 Para. 1 lit. f) GDPR fulfilled.

The balancing of interests within the scope of Art. 6 Para. 1 lit. f GDPR requires a

substantial discussion of the

interests, fundamental rights and

fundamental freedoms of those involved and must be related to the specific individual case.

Although general statements that data processing according to Art. 6 Para. 1

lit. f DSGVO is permissible, do not meet these legal requirements, these are

often to be found in the data protection declarations of telemedia providers.

In addition, in cases where third-party service providers are used for tracking as

Processors are involved to ensure that these service providers

Process the data of the data subjects for our own purposes (e.g. to

to improve our own services or to create interest profiles). In this case -

and even if the third-party service provider only reserves the right to do so in the abstract - the

exceeded within the scope of order processing according to Art. 28 DS-GVO. For the

Transmission of personal data - even if only the IP address - to them

Article 6 (1) lit. f GDPR then generally cannot provide a third-party service provider

form the legal basis.

Since this legal basis is regularly only used in individual cases and only with one

can be used according to meaningful consideration, the

Examination of the prerequisites in this guide is not further detailed. The

However, statements in the OH Telemedien 2019 can still be used as

standard of audit.47

4. Transfers of personal data to third countries

Finally, it should be noted that the aforementioned legality check

only to the processing of the data within the European Economic Area

relates. It must therefore always be checked in addition whether the respective

Data processing for the transfer of personal data to third countries

comes. This is particularly the case with the integration of third-party content created by large

providers are provided, often the case. This is particularly problematic when

for these countries, such as B. the USA, no adequacy decision of the European

47 p. there the explanations under III. 2. c), available at https://www.datenschutzkonferenz-

online.de/media/oh/20190405_oh_tmg.pdf.

31

commission exists. With its judgment of July 16, the European Court of Justice

2020 in the case "Schrems II" (C-311/18) the decision of the European

Privacy Shield Commission invalidated and the high hurdles for the

data protection-compliant transfer of personal data

to third countries

clarified.

A transfer of personal data to the USA and other third countries

without a level of data protection recognized by the EU Commission is therefore only allowed

subject to appropriate warranties such as B. standard data protection clauses, or at

Existence of an exception for certain cases according to Art. 49 DS-GVO

take place. It should be noted that the mere conclusion of standard data protection clauses

such as the standard contractual clauses adopted by the EU Commission

enough. In addition, it must be checked in each individual case whether this is the law or practice

of the third country the protection guaranteed by the standard contractual clauses

affect and whether additional measures to comply with this may be necessary

protection levels are to be met. A detailed guide on how to proceed with the

The European Data Protection Board has published the necessary examination.48

Especially in connection with the integration of third-party content and use

However, tracking services are often not sufficient

additional measures may be possible. In this case, the affected services may

not used, so also not

be integrated into the website.49

Personal data that

in connection with the

regular

Tracking of user behavior on websites or in apps are processed,

can generally not be based on consent in accordance with Article 49 (1) lit

DS-GVO are transmitted to a third country. extent and regularity of such

Transfers regularly contradict the character of Art. 49 DS-GVO as

Exception provision and the requirements of Art. 44 S. 2 DS-GVO.50

48 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance

with the EU level of protection of personal data, Version 2.0.

49 Cf. use cases 6 and 7 of Appendix 2 of Recommendations 01/2020 on measures that

Supplement transfer tools to ensure compliance with the EU level of protection of personal data, version ion

2.0

50 EDPB, Guidelines 2/2018 on the exceptions under Article 49 of Regulation 2016/679, p. 4.