

Draft Bill

of the Federal Government

Ordinance on Consent Management Services under the Telecommunications Telemedia Data Protection Act¹⁾

(Consent Management Ordinance – EinwV)

A. Problem and objective

Section 26 Paragraph 1 of the Telecommunications Telemedia Data Protection Act of 23 June 2021 (Federal Law Gazette I, p. 1982; 2022 I p. 1045) (TTDSG) provides that an independent body may recognise services that provide, inter alia, user-friendly and competitive procedures to manage the consent of end-users required by Section 25(1) of the TTDSG. Many providers of telemedia access the terminal equipment of end-users (Section 2(2)(6) TTDSG) in order to store information here or retrieve already stored information. This is often done through the use of cookies or tracking technologies that act in a similar way. Based on the information stored in the cookies or by similar tracking technologies, the web server can, among other things, recognise the end user, restore user-specific settings, perform range measurements, track activities (so-called tracking) or display individual advertising. Under Paragraph 25(1) of the TTDSG, telemedia providers may store information in the terminal equipment of the end-user or access information already stored there only if the end-user has consented to the processing of personal data and on the free movement of such data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, L 314 of 22.11.2016, p. 72, L 127 of 23.5.2018, p. 2, L 74 of 4.3.2021, p. 35). An exception to the requirement for consent to the use of cookies or similar tracking technologies exists pursuant to Section 25(2) TTDSG only if the sole purpose for this is the transmission of a message over a public telecommunications network or when the use is strictly necessary so that the provider of a telemedia service can provide a telemedia service expressly requested by the end user. The requirement for consent pursuant to Section 25(1) TTDSG does not depend on the personal data being processed. The possibilities provided for in Article 6(1)(b) to (f) of Regulation (EU) 2016/679 to process data without consent do not apply here. Therefore, telemedia providers must ask end-users for consent to the use of the different types of cookies or similar tracking technologies each time they use their service. In practice, this is done by means of so-called consent banners. Consent banners also enable telemedia providers to obtain consent to the further processing of personal data in accordance with Article 6(1)(a) of Regulation (EU) 2016/679, so end-users are often confronted with a large number of consent banners on the internet.

Recognised consent management services are intended to provide a user-friendly alternative for end-users to the multitude of individual decisions that need to be taken. They manage the decision taken by the end-user as to whether or not to give consent to a telemedia provider and transmit that decision to the telemedia provider when the latter requests it. If the providers of telemedia receive the consent or the refusal to give consent in this way, they are no longer dependent on making their own request from the end user pursuant to

¹)Notified in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17 September 2015, p. 1).

Section 25(1) sentence 1 TTDSG. The burden on end-users is relieved by reducing consent requests.

Section 26 Paragraph 2 of the TTDSG authorises the Federal Government to regulate the following by means of a statutory ordinance with the consent of the Bundestag and the Bundesrat:

- the requirements for user-friendly and competitive procedures that a consent management service must offer in order to be recognised;
- the process for recognition and
- the technical and organisational measures such that software for the retrieval and display of information from the internet and providers of telemedia can take into account the settings of end users managed via an integrated recognised consent management service with regard to consent pursuant to Section 25(1) of the TTDSG.

The purpose of this regulation is to implement this authorisation.

B. Solution

The integration of a recognised consent management service is intended to provide end-users with a transparent tool by which they can give or refuse their consent and understand and review their decisions at any time. Recognition by an independent body is to provide an incentive for end-users and telemedia providers to use such consent management services and strengthen confidence in a legally secure procedure. For telemedia providers, this procedure provides an opportunity to obtain end-users' consents in a user-friendly manner in accordance with Section 25(1) TTDSG, without having to disrupt the end user's use of their service by displaying their consent banner. In addition to the management of consents granted and refused pursuant to Section 25(1) of the TTDSG, which relate to the storage and reading of information on end-user terminal equipment, the recognised consent management services may also provide further services for end-users, insofar as is compatible with the requirements of Section 26 TTDSG and this Ordinance. This includes, for example, the assertion of data protection rights or the management of consents to the processing of personal data. The latter may be particularly advantageous for end users and telemedia providers if the use of a cookie or similar tracking technology results in the processing of personal data requiring consent.

C. Alternatives

Section 26 Paragraph 2 of the TTDSG requires that the requirements referred to therein be determined by ordinance of the Federal Government with the consent of the Bundestag and the Bundesrat. There are no alternatives to carry out the legal authorisation. Without the Ordinance, Section 26(1) TTDSG has no specific meaning in legal practice. The Federal Government could refrain from issuing a statutory ordinance pursuant to Section 26(2) of the TTDSG. In this case, the practice of requesting consent would continue to be determined by the use of consent banners. Recognised services are intended to regulate an alternative consent management process that gives end-users more control over their given and refused consents vis-à-vis the different telemedia providers. The Federal Government therefore considers it useful to adopt a corresponding ordinance so that recognised services for the administration of consent can develop. Experience can be gained with alternative consent management procedures and it can be examined whether such procedures become accepted and whether they are suitable for other areas where the consent of end-users is required.

The statutory ordinance is within the limits of the authorisation basis laid down in Section 26(2) TTDSG. It does not provide for any further rules with obligations on economic operators.

D. Budgetary expenditure exclusive of compliance costs

There are one-off material costs, the amount of which is estimated at EUR 7 000.

E. Compliance costs

E.1 Compliance costs for citizens

None.

E.2 Compliance costs for businesses

There is no mandatory compliance burden for business. The burden on business results from the requirements of Regulation (EU) 2016/679 for effective consent, which are not affected by the Ordinance. There are no mandatory implementation requirements. The Ordinance provides a framework for effective, user-friendly and competitive consent management through the integration of recognised consent management services. Where telemedia providers choose voluntarily to integrate the consent management services recognised by the independent body, this may replace the costs of the existing consent management when obtaining consent.

Administrative costs under this heading arising from information obligations

None.

E.3 Compliance costs for the authorities

The estimated one-off compliance cost of the administration is EUR 187 200. In addition, there is an annual compliance expense, the amount of which is estimated at EUR 78 920.

F. Further costs

Providers of consent management services that wish to be recognised in accordance with this Ordinance will incur costs in implementing the requirements of the Ordinance. The calculation of further costs in the form of fees is subject to uncertainties as there are no figures for the number of potential applicants. In order to quantify the further costs at least approximately, it is assumed as a simplification that the further costs of the economy through fees correspond approximately to the amount of the annual compliance costs of the Federal Commissioner for Data Protection and Freedom of Information of around EUR 79 000.

Further costs, in particular other economic costs and social security costs, as well as effects on individual prices and price levels, in particular on consumer price levels, are not to be expected.

Draft Bill of the Federal Government

Regulation on Consent Management Services under the Telecommunications Telemedia Data Protection Act

(Consent Management Ordinance – EinwV)

Dated ...

On the basis of Section 26(2) of the Telecommunications Telemedia Data Protection Act of 23 June 2021 (BGBl. (Federal Law Gazette) I p. 1982; 2022 I p. 1045) the Federal Government decrees, while respecting the rights of the Bundestag:

Part 1

General provisions

§ 1

Scope of application

(1) This Ordinance regulates:

1. the scope and definitions (Part 1);
2. the requirements that a consent management service must meet in order to be recognised (Part 2);
3. the procedure for the recognition of consent management services by an independent body (Part 3); and
4. the technical and organisational measures to be taken by telemedia providers, as well as manufacturers and providers of software, to retrieve and display information from the internet in order to comply with the settings of end-users and to take into account the integration of recognised consent management services (Part 4).

(2) The provider of telemedia remains responsible for the fulfilment of the information obligations and for compliance with the requirements for the effectiveness of consent under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119 of 4.5.2016, p. 1, L 314 of 22.11.2016, p. 72, L 127 of 23.5.2018, p. 2, L 74 of 4.3.2021, p. 35), as amended.

§ 2

Definitions

- (3) For the purposes of this Ordinance,

1. 'consent management service' means an information technology application or telemedia service that enables end-users to manage end-users' settings; management includes storage, transmission and revocation of end-user settings;
2. 'recognised consent management service' means a consent management service recognised by the competent body;
3. 'retrieval and display software' means software used to retrieve and display information from the internet; this includes all programs and applications through which content is accessed and displayed from the internet and which are not telemedia services within the meaning of Section 1(1) sentence 1 of the Telemedia Act,
4. 'end-user settings' means the decision of the end-user to grant or refuse consent pursuant to Section 25(1) of the Telecommunications Data Protection Act vis-à-vis providers of telemedia or third parties who wish to store information in their terminal equipment or access information already stored there.

(4) In addition, the definitions of Section 2 of the Telecommunications Telemedia Data Protection Act apply.

Part 2

Requirements for recognised consent management services

§ 3

General requirements

(5) The recognised consent management service stores end-user settings made by the end user when using a telemedia service for the first time. The same applies if the provider of telemedia requests consent pursuant to Section 25(1) of the Telecommunications Telemedia Data Protection Act which has not yet been managed by the recognised consent management service. It transmits these settings of end-users to the respective provider of telemedia during each further use of the telemedia service.

(6) The recognised consent management service only manages such consents where the telemedia provider has at least informed the end-user before consent is given about:

1. the provider(s) of telemedia or third parties who can store information in the end-user's terminal equipment or access information already stored there;
2. the specific information, to be stored in the end-user's terminal equipment and which are already stored in the terminal equipment of the end-user and which is to be accessed;
3. the purposes for which the information is to be stored in the terminal equipment of the end-user and for which information already stored in the end-user's terminal equipment is to be accessed;
4. the periods during which the information is to be stored in the terminal equipment of the end-user and in which information already stored in the end-user's terminal equipment is to be accessed;

5. the possibility of revocation of the consent at any time as well as the fact that the legality of the accesses and storages carried out on the basis of the consent until the revocation within the meaning of Section 25 paragraph 1 of the Telecommunications Telemedia Data Protection Act is not affected by the revocation.

Further information obligations of the providers of telemedia remain unaffected.

(7) If the end user gives the consent required by Section 25(1) of the Telecommunications Telemedia Data Protection Act, the information underlying the declaration of consent must be documented with the declaration of consent in a manner easily accessible to the end user.

Section 4

Requirements for a user-friendly procedure

(8) A consent management procedure is user-friendly if:

1. the user interface of the consent management service is transparent and comprehensible enough that the end-user can make a free and informed decision, and
2. the end-user's settings, including the date and time the settings were made, with the information provided at that time, can be viewed by the end user at any time and the end-user's settings can be changed and, where appropriate, revoked by the end-user at any time.

(9) A request to review the settings of the end-users by the recognised consent management service may be made after one year at the earliest unless the end-user has provided for a different setting.

(10) The consent management service shall allow the end-user to export the settings of end-users stored in accordance with paragraph 1(2), with the information provided at that time, into common file formats.

Section 5

Switch to another recognised consent management service

(11) The end user has the right, at any time, to easily

1. switch to another recognised consent management service and
2. transfer the settings of the end-users made by them to the other recognised consent management service.

(12) For this purpose, the recognised consent management service shall keep the end-user's settings in a common and machine-readable format and make them available for retrieval by another recognised consent management service free of charge if the end-user requests a transfer to the other recognised consent management service.

Section 6

Requirements for a competition-compliant procedure

A consent management procedure is competition-compliant if:

1. the provider of telemedia which integrates the recognised consent management service may obtain the necessary consents from the end user under the same conditions in accordance with Section 25(1) of the Telecommunications Telemedia Data Protection Act on the recognised consent management service in real time;
2. no telemedia provider who integrates the recognised consent management service, refuses to transmit the settings of end-users made for this purpose, and
3. in the default settings of the user interface of the recognised consent management service,
 - a) the providers of telemedia are presented uniformly in a list, either in alphabetical order according to the names held by the provider of telemedia pursuant to Section 5(1)(1) of the Telemedia Act or chronologically ordered according to the order of the settings stored by the recognised consent management service regarding the requests of telemedia providers, and
 - b) the settings of the end-users and the information necessary for the settings are presented in a uniform manner.

Section 7

Requirements for technologies and configurations for interaction with telemedia providers and with retrieval and display software

The recognised consent management service uses technologies and configurations that enable:

4. providers of telemedia and retrieval and display software to recognise that the end-user is using the consent management service and that it is recognised in accordance with Part 3;
5. providers of telemedia can use it to send their requests for consent pursuant to Section 25(1) of the Telecommunications Telemedia Data Protection Act; and
6. providers of telemedia who have requested consent under Section 25(1) of the Telecommunications Telemedia Data Protection Act can check whether end-user settings are managed.

Part 3

Recognition of consent management services

Section 8

Body making the decision

The Federal Commissioner for Data Protection and Freedom of Information is the independent body responsible for the recognition of consent management services.

Section 9

Exchange of information with competent supervisory authorities of the Länder

(13) The competent authority shall inform the competent supervisory authorities of the Länder in accordance with Section 40(1) of the Federal Data Protection Act electronically about the recognition of a consent management service.

(14) If, within the scope of its jurisdiction, the competent supervisory authority of a Land finds that a provider of telemedia cannot prove the existence of effective consent pursuant to Section 25(1) of the Telecommunications Telemedia Data Protection Act due to deficiencies in the integrated recognised consent management service, it shall inform the competent authority electronically. To this end, the supervisory authority of the Land and the competent authority shall exchange all relevant information.

Section 10

Recognition requirements

(15) A consent management service shall be recognised if it:

1. fulfils the requirements of Part 2, and
2. has submitted a security concept in accordance with Section 12.

Section 11

Application

(16) The application for recognition of a consent management service shall be submitted electronically to the competent authority.

(17) The application shall include a documented description of the consent management service, enabling the competent body to verify the compliance of the requirements set out in Part 2.

(18) The application must include the following information about the provider of the consent management service:

1. its name,

2. its legal status, in the case of legal persons additionally the legal form and the authorised representative, as well as information on the register, if the applicant is registered in the commercial register or in a register comparable to the commercial register, and the corresponding registration number;
3. its address or the address of its establishment or principal establishment within the European Union as referred to in Article 4(16) of Regulation (EU) 2016/679;
4. Information on the electronic availability of information about it and its activities;
5. its telephone number and email address or other online means of communication provided by it, if these ensure that the end-user can store his correspondence with it on a durable medium, including the date and time of the correspondence;
6. Information on its economic and organisational structure, including information on its financing and information indicating that:
 - a) has no economic self-interest in the consent of end-users and in the data managed and
 - b) is legally and organisationally independent of companies that may have such an interest.

Where the provider of a consent management service uses processors in accordance with Article 28 of Regulation (EU) 2016/679, the application shall contain the information referred to in subparagraphs 1 to 6 of paragraph 3 accordingly for those processors.

(19) The application must be accompanied by:

1. the declaration by the provider of the consent management service that it will not process personal data of the end-users using the service and the settings of the end-users for any purpose other than consent management;
2. a security concept in accordance with Section 12; and
3. Information on completed or ongoing participations, opinions and decisions of the competent data protection supervisory authorities, as far as this takes place.

(20) The competent body may draw up a template for the submission of the application. It shall publish the template or make it available to all providers of consent management services in any other appropriate manner.

Section 12

Security concept

The security concept required by Section 26(1)(4) of the Telecommunications Telemedia Data Protection Act must contain information:

1. on the security of the personal data and the settings of end-users managed by the consent management service;
2. on the storage location of the personal data and the settings of end-users,
3. on the technical and organisational measures to ensure that personal data and end-user settings are processed exclusively for the functions of the consent management service;

4. on the necessary technical and organisational measures to be taken;
 - a) to protect personal data from unauthorised access; and
 - b) to ensure the availability and access of personal data; and
5. on the technical and organisational measures to identify and minimise risks to the integrity, confidentiality and availability of the service offered.

Section 13

Register of the recognised consent management services

The competent body shall maintain a public register of the recognised consent management services.

Section 14

Display of changes

(21) The provider of a recognised consent management service shall verify on an annual basis whether the requirements set out in Part 2 continue to be met and whether facts underlying the information on which the application was submitted have changed. The competent body may request that the provider carries out additional checks. It may set deadlines within which the additional tests must be carried out in each case.

(22) Amendments relating to the requirements set out in Part 2 shall be notified electronically without delay to the competent body. Updates and changes to facts underlying the submission of the application shall also be notified electronically without delay to the competent body.

Section 15

Notification of complaints

(23) Third parties may electronically report to the competent body notices and complaints about possible violations by the recognised consent management service against the requirements set out in Part 2.

(24) The competent body may set up a body to receive the notifications.

Section 16

Withdrawal of recognition

The competent authority shall withdraw the recognition of a consent management service if it becomes aware of facts indicating that the conditions for recognition are no longer met. Before deciding on the revocation, the provider of the recognised consent management service must be consulted.

Part 4

Technical and organisational measures by providers of telemedia and manufacturers and providers of retrieval and display software

Section 17

Measures by manufacturers and providers of retrieval and display software

Within the scope of the technical possibilities, manufacturers and providers of retrieval and display software shall ensure, by means of technical and organisational measures, that:

1. the retrieval and display software takes into account the integration of recognised consent management services by end users, and
2. a signal stored through the recognised consent management service or through the provider of telemedia and the settings of the end-users are not suppressed, delayed or decrypted or otherwise changed.

Section 18

Measures by telemedia providers to integrate recognised consent management services

(25) The integration of recognised consent management services by telemedia providers is voluntary.

(26) Providers of telemedia that integrate a recognised consent management service and request the end-users' settings for their consents pursuant to Section 25(1) of the Telecommunications Telemedia Data Protection Act shall ensure, by means of technical and organisational measures in accordance with the state of the art, that:

1. the involvement of a recognised consent management service by the end-user is taken into account when invoking their telemedia service; and
2. it is checked whether end-users' settings for the requested consent of the telemedia provider are managed by the recognised consent management service.

(27) Telemedia providers that integrate a recognised consent management service shall:

1. enable the consents requested by them in accordance with Section 25(1) of the Telecommunications Telemedia Data Protection Act and the settings made by end users for this purpose to be stored by the integrated recognised consent management service;
2. point out to end-users, in a visible and appropriate place, that the offered telemedia service integrates recognised consent management services and takes into account the settings of end-users managed therein;
3. cooperate with the recognised consent management service to implement the requirements of Section 7; and

4. provide the recognised consent management service with the information required by Articles 7 and 12 to 14 of Regulation (EU) 2016/679 in a machine-readable format.

Section 19

Measures by telemedia providers to take into account the settings of end-users

(28) Telemedia providers that integrate a recognised consent management service shall take into account the settings of end-users. When requesting to consent from end-users from whom they have not obtained consent to the integration of the recognised consent management service and the settings of end-users, they shall point out the end-user's settings in the recognised consent management service at the same time.

(29) Telemedia providers may transfer consents of the end-user they already have to a recognised end-user consent management service used by the end-user. At the same time, the information referred to in Section 3(3) with the date and time of the consent of the end users shall be transmitted.

Section 20

Neutrality measures

Telemedia providers, manufacturers and providers of on-demand and display software that integrate a recognised consent management service shall not, without objective reason, seek to ensure that end-users use or exclude certain recognised consent management services.

Part 5

Final provisions

Section 21

Entry into force

This Ordinance shall enter into force on xx.xx.xxxx.

Approved by the Federal Council.

Berlin/Bonn, [\[date of official copy\]](#)

The Federal Chancellor

[\[...\]](#)

The Federal Minister [\[...\]](#)

[\[...\]](#)

[\[any other Federal Ministers\]](#)

Explanatory notes

A. General part

I. Objective of and need for the provisions

The proposed Ordinance utilises the power to issue ordinances contained in Section 26(2) TTDSG. The regulation is necessary because a user-friendly and legally secure alternative to the current practice of consent banners can only be developed by means of legal requirements for the recognition procedure and through corresponding technical and organisational requirements for recognised consent management services.

II. Main content of the draft

The Ordinance regulates the requirements that a consent management service must meet in order to be recognised, the procedure for recognition by the Federal Commissioner for Data Protection and Freedom of Information, as well as technical and organisational measures required for providers of telemedia and software to retrieve and display information from the internet. This creates a procedure for consent with the help of recognised consent management services.

III. Alternatives

None. Section 26 Paragraph 2 TTDSG requires the regulation of certain issues of recognised services for the administration of consent by means of a statutory ordinance with the consent of the Bundesrat and the Bundestag. Without the Ordinance, Section 26(1) TTDSG has no specific meaning in legal practice.

IV. Regulatory Power

The Federal Government's competence to issue the Ordinance derives from Section 26(2) of the TTDSG.

V. Compatibility with European Union law and international treaties

The provisions of the draft ordinance are compatible with European Union law and international procedures. In particular, there is no conflict with Regulation (EU) 2016/679 and Article 5(2) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1-66). A notification procedure required by Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and rules on information society services (OJ L 241, 17.9.2015, p. 1-15) has been carried out.

VI. Consequences of the Ordinance

The draft has the effect of providing end-users with an alternative procedure for granting consent requested by telemedia providers in future, in accordance with Section 25 TTDSG. No unintended consequences can be recognised.

1. Legislative and administrative simplification

Legal and administrative simplifications are not foreseen.

2. Sustainability aspects

Regulations and indicators of the sustainability strategy are unaffected.

3. Budgetary expenditures exclusive of compliance costs

For the Federal Commissioner for Data Protection and Freedom of Information, one-off material costs will be incurred for the technical implementation of an online application form, the amount of which is estimated at EUR 7 000. The implementation is to be carried out by an external service provider and based on existing systems.

4. Compliance costs

Compliance costs for businesses

There is no additional compliance cost for businesses. The burden on business results from the requirements of Regulation (EU) 2016/679 for effective consent, which are not affected by the Ordinance. The Ordinance provides framework conditions that enable effective, user-friendly and competitive consent management. The effort to be made by economic operators, in particular with regard to the voluntary involvement of recognised services, serves their own interest in obtaining effective consents and cannot be regarded as a compliance burden. However, this effort can replace the previous effort of consent management. Providers who are currently configuring consent management for telemedia service providers will be able to open up a new commercial activity as recognised services within the meaning of the Consent Management Ordinance.

Administrative compliance costs

The new tasks of the Federal Commissioner for Data Protection and Freedom of Information, which he or she is required to perform as the body responsible for recognition, will result in an estimated one-off implementation cost of EUR 187 200. In addition, there is an estimated annual compliance cost of EUR 78 920.

The costs for the one-off implementation effort, including material costs, include in particular the preparation and design of the process for the application procedure (Sections 11, 12) as well as the establishment of the corresponding IT infrastructure. In order to be able to process incoming applications, internal work processes need to be established, such as the development of a checklist which allows applications to be examined uniformly for compliance with all legal and technical requirements. In addition, an application form is to be drawn up (Section 11(4)). In addition, an audit concept for the safety concept must be drawn up (Section 12). For communication with the applicant (Sections 11, 14) and the establishment of a body for receiving notices and complaints (Section 15(2)), technical infrastructure must be provided, whereby in this case, in particular, use should be made of existing technical systems for contacting the applicant. In addition, there are costs for setting up a public register (Section 13). The implementation of these measures requires an estimated 1 600 working hours in the higher grade of the Civil Service and 1 600 working hours in the upper grade. According to the current personnel cost rates, this corresponds to EUR 112 800 (1 600 x 70.50) for the higher grade of the Civil Service and EUR 74 400 (1 600 x 46.50) for the upper grade.

Einwilligungsverordnung nach § 26 TTDSG/Aufwandsschätzung
Einmaliger Aufwand

Spalte1	Stunden jährlich	Spalte2	Kosten	Spalte3
Aufgaben / Tätigkeiten im Einzelnen	hD	gD	hD (70,50 Euro / Std)	gD (46,50 Euro / Std)
Vorbereitung und Ausgestaltung des Prozesses für das Antragsverfahren (§§ 11, 12)	300	300	21.150,00	13.950,00
Erarbeitung einer Checkliste, durch die Anträge einheitlich auf die Einhaltung aller juristischer und technischer Anforderungen geprüft werden können, §§ 11, 12	500	190	35.250,00	8.835,00
Erarbeitung eines Antragsformulars, § 11 Absatz 4	170	170	11.985,00	7.905,00
Erstellung eines Prüfkonzpts für das Sicherheitskonzept, § 12	230	70	16.215,00	3.255,00
Errichtung entsprechender IT-Infrastruktur für die Kommunikation mit dem Antragssteller, §§ 11, 14	150	320	10.575,00	14.880,00
Errichtung einer Stelle zum Empfang von Hinweisen und Beschwerden, § 15 Absatz 2	150	320	10.575,00	14.880,00
Aufbau eines öffentlichen Registers, § 13	100	230	7.050,00	10.695,00
Gesamtsummen	1.600	1.600	112.800,00	74.400,00

Einwilligungsverordnung nach § 26 TTDSG/Aufwandsschätzung	Consent Ordinance pursuant to Section 26 TTDSG/Estimation of costs
Einmaliger Aufwand	One-time costs
Spalte1	Column 1
Stunden jährlich	Hours per year
Kosten	Costs
Aufgaben / Tätigkeiten im Einzelnen	Tasks/activities in detail
hD (70,50 Euro / Std)	Higher grade (70,50 EUR/hour
Vorbereitung und Ausgestaltung des Prozesses für das Antragsverfahren (§§11,12)	Preparation and design of the process for the application procedure (Sections 11, 12)
Erarbeitung einer Checkliste, durch die Anträge einheitlich auf die Einhaltung aller juristischer und technischer Anforderungen geprüft werden können, §§11,12	Development of a checklist allowing applications to be examined uniformly for compliance with all legal and technical requirements, Sections 11, 12
Erarbeitung eines Antragsformulars, § 11 Absatz 4	Preparation of an application form, Section 11(4)
Erstellung eines Prüfkonzpts für das Sicherheitskonzept, § 12	Preparation of an audit concept for the safety concept, Section 12
Errichtung entsprechender IT-Infrastruktur für die Kommunikation mit dem Antragssteller, §§11,14	Establishment of appropriate IT infrastructure for communication with the applicant, Sections 11, 14
Errichtung einer Stelle zum Empfang von Hinweisen und Beschwerden, § 15 Absatz 2	Establishment of a body to receive notices and complaints, Section 15(2)
Aufbau eines öffentlichen Registers, § 13	Establishment of a public register, Section 13
Gesamtsummen	Total amounts

The annual compliance effort is due to the maintenance and optimisation of the existing processes and the technical infrastructure, in particular the register (Section 13). In addition, it includes the implementation of the application procedures (Section 11), the examination of amendments (Section 14), the processing of notices and notifications (Section 15) and the implementation of any necessary revocation procedures (Section 16). There are currently no figures for the number of potential applicants. Consent management services that manage consent for end-users within the meaning of the Ordinance are not yet available. On the basis of the aim of the Ordinance to promote the emergence of these services and to develop corresponding business models, a moderate number of applications is expected at first. The development of services and the number of applications is the subject of the evaluation and a robust estimate of the annual compliance costs can therefore only be made after evaluation (at the latest after two years). Currently, the ongoing annual compliance effort is therefore forecast at 0.25 FTE of the higher service, 0.5 force FTE of the upper grade and 0.25 FTE of the middle grade. This corresponds to personnel costs of 400 working hours x 70.50 = EUR 28 200 for the higher grade, 800 working hours x 40,50 = EUR 37 200 for the upper grade and 400 working hours x 28.30 = EUR 13 520

5. Additional costs

There are costs for providers of consent management services if they wish to have their service recognised in accordance with this Ordinance and set up the service in accordance with the requirements of the Ordinance. In addition, fees are to be paid for recogni-

tion. The calculation of further costs in the form of fees is subject to uncertainties as there are no figures for the number of potential applicants. In order to quantify the further costs, at least approximately, it is assumed that the further costs for business through fees correspond approximately to the amount of compliance costs of the Federal Commissioner for Data Protection and Freedom of Information. Assuming that the Federal Commissioner for Data Protection and Freedom of Information fully covers the additional expenditure through fees, business would therefore have to face additional costs of around EUR 79 000. Further costs to business, costs of social security systems and impacts on individual prices and price levels, in particular on consumer price levels, are not expected

6. Further consequences of the legislation

The draft regulation has no gender equality or demographic impact.

VII. Time limit; Evaluation

Pursuant to Section 26(3) of the TTDSG, within two years of the entry into force of the Ordinance, the Federal Government shall assess the effectiveness of the measures taken with regard to the development and enforcement of user-friendly and competitive consent procedures and the effects on software for retrieving and displaying information from the internet and on providers of telemedia. The Federal Government submits a report for this purpose to the Bundestag and the Bundesrat. In particular, the aim is to determine whether and how many recognised consent management services emerged during the evaluation period. As a criterion for the evaluation, the number of applications for recognition under the Ordinance may be considered. The report is also intended to identify any existing difficulties in the implementation of the recognition procedure, so that it can be considered whether the arrangements set out in Part 3 of the Ordinance are sufficient to ensure a functioning recognition procedure. The Federal Government's report is also intended to show how many telemedia providers voluntarily integrate recognised consent management services and take into account the managed decisions of end-users accordingly. In particular, the provision in Section 19(1) is to be examined in order to determine whether it is suitable to promote the development of user-friendly and at the same time legally secure consent management procedures. It will also examine whether and to what extent software for retrieving and displaying content from the internet takes into account the integration of recognised consent management services by end users. Findings of the report are to be obtained, in particular, through the survey of professional circles and associations. If no recognised consent management services have developed after the expiry of two years after the entry into force of the Ordinance, the circumstances for this should be examined.

B. Specific part

Re Part 1 (General provisions)

Part 1 regulates the scope of the Ordinance and individual definitions.

Re Section 1 (Scope)

Section 1 defines the content and scope of the Ordinance.

Re paragraph 1

According to paragraph 1, in addition to the general rules on scope and definitions (Part 1), the Ordinance regulates the requirements that a consent management service must meet in order to be recognised (Part 2), the procedure for the recognition of consent man-

agement services by the competent body (Part 3) and the technical and organisational measures by telemedia providers and manufacturers and providers of software to retrieve and display information from the internet when they voluntarily integrate recognised consent management services (Part 4).

Re paragraph 2

Paragraph 2 declares that the provider of telemedia remains responsible for the requirements for the effectiveness of consent. It must provide the information required by Regulation (EU) 2016/679 for effective consent to the processing of personal data to the end-user (Articles 13 and 14 of Regulation (EU) 2016/679). The Ordinance does not affect the requirements for the effectiveness of consent pursuant to Regulation (EU) 2016/679 or other legal requirements for the design for obtaining consent pursuant to Section 25(1) of the TTDSG by providers of telemedia. For example, telemedia providers must comply with and demonstrate compliance with the requirements of Article 4(11) and Article 7 of Regulation (EU) 2016/679. In addition, certain providers of telemedia may have special requirements for the design for obtaining consent, which also remain unaffected. This applies, for example, to requirements arising from Section 19a(2) sentence 1 subparagraph 4a of the Restrictive Practices Act (GWB) and to European regulations such as Article 5(2) of Regulation (EU) 2022/1925.

Re Section 2 (Definitions)

Re paragraph 1

Paragraph 1 lays down the definitions.

Re subparagraph 1

Subparagraph 1 defines the concept of a consent management service. This is, in principle, any telemedia service or other information technology application on the end-user's terminal equipment that enables the end-user to manage consent to cookies or comparable accesses to its terminal equipment. Consent management is the storage and transmission of the end user's decision on consent pursuant to Section 25(1) TTDSG. Similarly, the decision on the withdrawal of consent must be able to be stored and also transmitted. Section 26 Paragraph 1 TTDSG expressly refers to consents pursuant to Section 25(1) TTDSG. Section 25 Paragraph 1 of the TTDSG provides that, in principle, any storage of information in the end-user's terminal equipment or access to information already stored in the terminal equipment is permitted only with informed consent, in accordance with Regulation (EU) 2016/679. The admissibility of the further processing of the personal data stored in the cookie or through similar tracking technologies is only permitted with consent in accordance with Regulation (EU) 2016/679, unless there is another legal authorisation under Article 6(1)(b-f) of Regulation (EU) 2016/679. Therefore, a large number of existing consent banners currently also ask for consent to the further processing and use of the personal data obtained through the use of cookies or similar tracking technologies. Examples of this include, among other things, consent to the disclosure of information about the use of the telemedia service to advertising partners or the evaluation of the information to optimise the offer. In addition to managing decisions to grant or refuse consent pursuant to Section 25(1) TTDSG, recognised consent management services may also be used for the management of decisions to grant or refuse consent to the processing of personal data. This may be particularly advantageous for end-users and telemedia providers if the use of a cookie or similar tracking technology results in the processing of personal data requiring consent.

For the purposes of technology neutrality, the definition does not contain any specifications for technical implementation. A consent management service can be both a retrievable telemedia service (e.g. offering consent management on a central platform) as well

as a technical application on the end-user's terminal equipment, as well as any other design that enables consent management within the meaning of the definition.

Re subparagraph 2

Subparagraph 2 defines the concept of the recognised consent management service. This is a consent management service that is recognised by the competent authority in accordance with Section 8.

Re subparagraph 3

Subparagraph 3 defines the concept of retrieval and display software within the meaning of the Ordinance. This is software for retrieving and displaying information from the internet. This includes all applications through which content from the internet is displayed and which are not a telemedia service within the meaning of Section 1 paragraph 1 sentence 1 Telemedia Act. This includes in particular browser software that enables navigation on the World Wide Web. The term software does not cover apps that offer information and communication services via the internet as telemedia.

Re subparagraph 4

Subparagraph 4 defines the settings of end-users as the decision to grant and refuse consent pursuant to Section 25(1) TTDSG. These decisions are managed by the recognised consent management service.

Re paragraph 2

Paragraph 2 refers to the existing definitions of the TTDSG. This is based on the explanatory memorandum to the Act regulating data protection and the protection of privacy and telecommunications and in the case of telemedia (BT Drs. 19/27441, p. 34).

Re Part 2 (Requirements for recognised consent management services)

Part 2 regulates the requirements that consent management services must meet in order to be recognised. This concerns the general requirements for the management of end-user consent, the requirements for a user-friendly procedure, the switch to another recognised consent management service and the requirements for competition-compliant procedures, as well as the technologies and configurations for interacting with telemedia providers and with software to retrieve and display information from the internet.

Re Section 3 (General requirements)

Section 3 defines the requirements for the administration of consents by a recognised consent management service.

Re paragraph 1

Paragraph 1 regulates how the settings of end-users are stored in the recognised consent management service. The recognised consent management service shall store the requests made by the provider of telemedia and the settings made by the end user when using the telemedia service for the first time and make them available for access by the end user and the telemedia providers. This also applies if the provider of telemedia requests the end user for specific consent under Section 25(1) TTDSG for the first time if the telemedia service is used again. This may be, for example, in the event of (significant) changes in the circumstances of access to the end-user's terminal equipment or if a previously granted consent is no longer effective. The recognised consent management service then transmits the stored settings directly to the provider of telemedia when the telemedia are used in the future, so that a direct request to the end user by the provider of

telemedia becomes unnecessary. General defaults to possible requests for consent from the provider of telemedia, which are made by the end user without reference to the specific use of a telemedia offer, do not meet the requirements for the administration of consents.

Re paragraph 2

Paragraph 2 provides that the recognised consent management service shall only manage consents where the end-user is aware of access to the terminal equipment, the purpose of access and the period of access, and the revocation of consent. This regulation does not transfer responsibility to the recognised consent management service. The provider of telemedia remains responsible for the effectiveness of consent and therefore for the lawfulness of storage or access to information in terminal equipment. However, at least some minimal verification of certain information relevant to end-users should be carried out by the recognised consent management service. It should be ensured that consents are not managed that from the outset cannot meet the requirements for informed consent. The second sentence is intended to clarify: To the extent that there are information obligations for the providers of telemedia that go beyond the elements contained in subparagraphs 1 to 5, these shall continue to be fulfilled.

Re paragraph 3

Paragraph 3 regulates a documentation obligation by the recognised consent management service in order to make the deposited decisions of end-users transparent and comprehensible.

Re Section 4 (Requirements for a user-friendly procedure)

Section 4 specifies the requirements for a user-friendly procedure.

Re paragraph 1

Paragraph 1 lays down the conditions for a user-friendly procedure. These relate to the design of the user interface for the recognised consent management service as well as the setting options and information that must be available to end users when administering their consents pursuant to Section 25(1) TTDSG.

Re subparagraph 1

Subparagraph 1 stipulates that the configuration and design of the user interface of a recognised consent management service must be sufficiently transparent. The consent of end-users must not be controlled by the use of behaviour-influencing design elements. This includes the use of manipulative designs or processes designed to persuade end-users to take action. This includes measures capable of exploiting typical behaviour, such as the impatience of end-users, or leading them to a decision that they would not otherwise have taken. To the extent that the recognised consent management service provides its own text content, it must be written in simple, clear and easy-to-understand language. The design is based on the principles of digital accessibility, i.e. visibility, usability and comprehensibility are guaranteed. This includes, in particular, sufficient colour contrast and keyboard operability. Existing legal obligations arising from the disability equality laws of the federal and state governments as well as from the Barrier-Free Act also apply to recognised services for consent management.

Re subparagraph 2

Subparagraph 2 ensures that end-users are able to manage and verify their settings. End-users must be able to view their settings for the respective telemedia providers regardless of the specific access situation. The end-user should be able to view and understand the

consents stored by the recognised consent management service with as few intermediate steps as possible. This includes, among other things, digital accessibility, a logical structure and design as well as self-explanatory navigation on the end devices. Changing the setting must be as simple as the original decision and possible to carry out through the same user interface.

The storage of the date and time that the setting was made serves to trace the decision for the end user. It also serves the provider of telemedia with regard to proof of the information basis on which the end user has given consent.

Re paragraph 2

Paragraph 2 lays down rules on a reminder function of the consent management service of the decisions already taken and stored by end users regarding the consent requests pursuant to Section 25(1) of the TTDSG. Regulation (EU) 2016/679 does not provide a time limit for declared consent. It thus retains its validity until revocation, unless otherwise stated in the context or expectations of the parties. The recognised consent management service may remind the end user of his/her attitudes to the consent requests at the earliest after one year. This ensures that end-users do not feel harassed or urged to change their decision by regular reminders. This does not apply if the end user expressly sets a reminder by the recognised consent management service at shorter intervals.

Re paragraph 3

Paragraph 3 allows the end-user to export his/her settings to the specific consent requests of telemedia providers in order to assert his or her rights from the recognised consent management service.

Re Section 5 (Change to another recognised consent management service)

Section 5 is intended to strengthen interoperability in order to prevent “lock-in” effects and enable the end-user to switch between several recognised consent management services. The scheme is limited to the possibility of data export.

Re Section 6 (Requirements for a competitive procedure)

Section 6 imposes requirements on the competition conformity of the recognised consent management service.

Re subparagraph 1

Subparagraph 1 stipulates that the consent management service must enable providers of telemedia that integrate it to ask for consent pursuant to Section 25(1) of the TTDSG and that the declarations made by end-users are communicated to them if necessary.

Re subparagraph 2

Subparagraph 2 provides that a recognised consent management service may not refuse to transmit the end-user decisions taken in this regard to any telemedia provider that integrates it.

Re subparagraph 3

Subparagraph 3 imposes requirements for the equal representation of the telemedia providers on the user interface of the recognised consent management service. The recognised consent management service may not, without legitimate reason, represent the different providers of telemedia by sequencing, size of display or other measures in such a way that individual providers of telemedia may be preferred or disadvantaged

when deciding on the consent to be made or when changing settings. In order to ensure this, an alphabetically ordered list of the providers of telemedia in accordance with Section 5 paragraph 1 subparagraph 1 Telemedia Act or a chronological order as determined by the consents given shall be made in the default settings.

Re Section 7 (Requirements for technologies and configurations for interaction with telemedia providers and with retrieval and display software)

Section 7 lays down the technical and organisational requirements for a recognised consent management service so that the information about its integration and, where applicable, the settings of the end-users made during a previous use of the telemedia can be transmitted to providers of telemedia and transported via software for retrieving and displaying information from the internet.

Re subparagraph 1

Subparagraph 1 stipulates that the recognised consent management service uses such technologies and configurations for data transmission that providers of telemedia and software for retrieving and displaying information from the internet can recognise and read in accordance with the state of the art. This means the use of a commonly used programming language and/or a commonly used communication protocol, such as the use of the internet protocols HTTP and HTTPS for the World Wide Web. Another conceivable technology would include the addition of the headers to the HTTP/HTTPS request by a signal indicating the integration of the recognised consent management service (see Stiemerling/Weiß/Wendehorst, research opinion on consent management pursuant to Section 26 TTDSG, 2021, paras 23, 208). Where legally and technically appropriate and available, existing industry and market standards should be used to enable the communication of stakeholders involved in the exchange of information.

The recognised consent management service shall also indicate that it has been recognised by the competent authority pursuant to Section 8. As proof, it may refer, for example, to the register of the competent body, which is to be held in accordance with Section 13.

Re subparagraph 2

In addition to subparagraph 1, subparagraph 2 provides that the provider of telemedia may request his consent under Section 25(1) of the TTDSG via the technology or configurations used by the provider of a consent management service. The aim is to ensure that communication between the provider of a consent management service and the provider of telemedia can be carried out on both sides, i.e. information can be sent and retrieved.

Re subparagraph 3

Subparagraph 3 provides that the recognised consent management service allows telemedia providers to recognise via the technologies and configurations used for data transmission whether the end-user has already made a setting for the specific consent request of the telemedia providers during previous use of the telemedia. The provider of a recognised consent management service shall allow telemedia providers to access the settings made by the end-user for their service. Access to settings made for another provider of telemedia must be excluded. The aim shall be that the consent requests of the telemedia providers can be compared with the settings of the end-users made during a previous use and that a renewed demand by the providers of telemedia from the end user is unnecessary. This comparison always refers only to the specific consent request. Providers of telemedia and recognised consent management services do not have their own scope for interpretation with regard to the settings of end-users.

Re Part 3 (Recognition of consent management services)

Part 3 regulates the competence of the Federal Commissioner for Data Protection and Freedom of Information, the exchange with the supervisory authorities of the Länder, the recognition requirements for consent management services, the application and the security concept, the procedure for recognition and the withdrawal of recognition.

Re Section 8 (Competent body)

Section 8 defines the Federal Commissioner for Data Protection and Freedom of Information as the competent authority. The Federal Commissioner shall carry out this task in similarly complete independence as his/her other tasks.

Re Section 9 (Exchange of information with competent supervisory authorities of the Länder)

Section 9 lays down the procedure for the exchange of information between the competent authority and the supervisory authorities of the Länder in the process of the recognition procedure and in the case of decisions relating to the integration of recognised consent management services. The reciprocal exchange of information between the competent body and the supervisory authorities of the Länder is intended to provide legal certainty and increase confidence in the use of recognised consent management services as a whole.

Re paragraph 1

In accordance with paragraph 1, the competent authority shall inform the competent supervisory authorities of the Länder in accordance with Section 40 of the Federal Data Protection Act (BDSG) before recognition of a consent management service. This information serves to be able to identify and resolve divergent views between the supervisory authorities at an early stage when assessing a recognised service.

Re paragraph 2

Paragraph 2 stipulates that the competent supervisory authority of the Länder pursuant to Section 40 BDSG shall inform the competent body if decisions by the competent supervisory authorities of the Länder arise in connection with the integration of a recognised consent management service. The provider of telemedia remains responsible for the lawful use of cookies or similar tracking technologies even if a recognised consent management service is integrated. The supervisory authorities of the Länder are usually responsible for monitoring compliance with data protection regulations. If, within the scope of their supervisory activities, they conclude that a permitted use of cookies or permitted data processing cannot be proven by the provider of telemedia due to defects in an integrated and recognised consent management service, they must inform the competent authority thereof in accordance with Section 8.

Re Section 10 (Requirements for recognition)

Section 10 lays down the conditions for a consent management service to be recognised. The provider of a consent management service must meet the requirements of Part 2, submit an application and submit a security concept in accordance with Section 12.

Re Section 11 (Application)

Section 11 regulates the application.

Re paragraph 1

The first sentence of paragraph 1 stipulates that the application must be submitted electronically to the competent authority. No special formal requirements are required.

Re paragraph 2

In accordance with paragraph 2, the application shall include a documented description of the consent service. This is intended to enable the competent authority to verify the presence of the conditions set out in Part 2.

Re paragraph 3

Paragraph 3 sets out in the first sentence the information that the application must receive. Sentence 2 refers to the information on the involvement of a processor pursuant to Article 28 of Regulation (EU) 2016/679.

Re subparagraphs 1 to 5

Subparagraphs 1 to 5 define the information to be made available to the provider of the consent management service. This includes information about the provider itself and its accessibility. The formal requirements for recognition are primarily intended to identify for the competent body at least one responsible and available contact person who is the addressee of the recognition and the communication required for it. However, they also provide transparency for the subsequent procedure and serve to facilitate the identification of the service by the end-user.

Re subparagraph 6

Subparagraph 6 requires the provider of a consent management service to provide information on the business and organisational structure which shows that it has no economic self-interest in the consent of end-users and in the data managed and is legally and organisationally independent of undertakings that may have such an interest. Independence presupposes that the operation of the consent management service is not entirely financially dependent on financing by third parties who themselves have a direct or indirect interest in the granting of consent. In particular, this means that no influence is exercised on the personnel and/or organisational arrangement of the consent management service. Economic independence does not mean that recognised consent management services must be offered free of charge or that there is no overall commercial interest in the offering of the consent management service. The consent management service may be provided for a fee both for the end user and for telemedia providers who require the end-user's consent pursuant to Section 25(1) TTDSG.

Re paragraph 4

Paragraph 4 specifies the declarations and documents to be attached to the application.

Re subparagraph 1

According to subparagraph 1, the application must be accompanied by a self-declaration that the purpose limitation within the meaning of Section 26(1)(3) TTDSG is complied with. In the self-declaration, the provider of the service undertakes to administer consent itself to comply with the purpose limitation principle and confirms that its information is correct and that recognition given will be void in the case of false information. The body responsible for recognition may provide templates/forms to be signed with legal force by the provider of the consent management service. To the extent that the processing of personal data and the information on consent decisions are for the sole purpose of evaluating and improving the consent management service, it fulfils the purposes of consent man-

agement. Section 26 Paragraph 1(3) TTDSG and the Ordinance do not impose requirements on the purpose limitation principle that go beyond Article 5(1)(b) of Regulation (EU) 2016/679. Non-personal data is not covered by the purpose limitation principle.

Re subparagraph 2

Subparagraph 2 provides that a complete application presupposes the submission of a security concept. The requirements for the security concept are set out in Section 12.

Re subparagraph 3

Subparagraph 3 stipulates that existing opinions or other contributions by competent data protection authorities in relation to the activity as a consent management service must be attached to the application. These also relate to the activity of the consent management service before an application for recognition was made.

Re paragraph 5

In accordance with paragraph 5, the recognition body may provide appropriate templates/forms for the application, to simplify and standardise the procedure. It must point this out accordingly.

Re Section 12 (Security concept)

Section 12 lays down the requirements for the security concept to be attached to the application. The requirements for the security concept are mainly based on the types of data being processed for the recognised consent management service. The benchmark is the requirements of Regulation (EU) 2016/679. Where required by Article 35 of Regulation (EU) 2016/679, a data protection impact assessment shall be carried out.

Re subparagraph 1

Subparagraph 1 provides that the security concept must include information on the security of personal data and the consent decisions processed by the recognised consent management service. If no personal data are processed by the consent management service, the related requirements in the security concept are omitted.

Re subparagraph 2

Subparagraph 2 regulates the location and duration of the storage of personal data and the declared or rejected consents. This also concerns the personal data and information about the consent decision that is stored by a processor.

Re subparagraph 3

Subparagraph 3 regulates the measures taken to ensure the processing purpose of the personal data and the information on the consent decisions. To the extent that the processing of personal data and the information on consent decisions are for the sole purpose of evaluating and improving the consent management service, this fulfils the purposes of consent management. Section 26 Paragraph 1(3) TTDSG and the Ordinance do not impose requirements on the purpose limitation principle beyond Article 5(1)(b) of Regulation (EU) 2016/679. Non-personal data is not covered by the narrow purpose limitation principle.

Re subparagraph 4

According to subparagraph 4, the security measures must be described that are necessary to protect personal data against unauthorised access and to ensure the availability of personal data and the access to the data.

Re subparagraph 5

Subparagraph 5 regulates the core integrity of a security concept, regardless of whether personal data is processed. This is about the security of a consent management service as a whole. In this respect, documentation is required that in the development and operation of the recognised consent management service, the relevant warranty objectives of integrity, confidentiality and availability are taken into account and that corresponding risks are minimised as much as possible.

Re Section 13 (Register of recognised consent management services)

Section 13 regulates the public register of the recognised consent management services to be managed by the competent body. This is intended to create transparency and security vis-à-vis end-users, software for retrieving and displaying information from the internet and providers of telemedia.

Re Section 14 (Display of changes)

Section 14 regulates the notification of changes by the consent management service to the competent body. The competent body has no independent auditing and monitoring obligations that go beyond the recognition procedure.

Re paragraph 1

Paragraph 1 provides for an annual verification obligation by the recognised consent management service.

Re paragraph 2

Paragraph 2 lays down the obligation to notify changes concerning circumstances which were the subject of the application procedure by the recognised consent management service. This allows the competent authority to verify whether the conditions for recognition are still met. If it concludes that the conditions for recognition are no longer met, it shall give the applicant the possibility of rectification before withdrawing recognition in accordance with paragraph 16.

Re Section 15 (Reporting of complaints)

Section 15 regulates the reporting of complaints by third parties.

Re paragraph 1

Paragraph 1 regulates the case where third parties point out to the competent authority pursuant to Section 8 that the recognised consent management service does not comply with the requirements laid down in Part 2 and Part 3. Third parties include end-users and providers of telemedia and software for retrieving and displaying information from the internet.

Re paragraph 2

Paragraph 2 provides that, in order to receive the notifications referred to in paragraph 1, the competent authority may set up a separate body receiving those messages.

Re Section 16 (Revocation of recognition)

Section 16 regulates the withdrawal of recognition if the independent competent authority pursuant to Section 8 acquires knowledge of facts according to which the conditions for recognition no longer exist.

Re Part 4 (Technical and organisational measures by providers of telemedia and manufacturers and providers of retrieval and display software)

Part 4, in implementation of Section 26(2)(3) TTDSG, regulates the technical and organisational measures by manufacturers and providers of software for the retrieval and display of information from the internet and providers of telemedia.

Re Section 17 (Measures by manufacturers and providers of retrieval and display software)

Section 17 regulates the measures by providers and manufacturers of software for retrieving and displaying information from the internet

Re subparagraph 1

Subparagraph 1 stipulates that software for retrieving and displaying information from the internet should in principle be provided in such a way that it takes into account the integration of recognised consent management services. This may include access to local storage, network communication and its user interface. The purpose of this regulation is to enable recognised consent management services to transmit the information on the end-user's settings to the telemedia providers requesting consent. This applies in particular to providers of browsers if the recognised consent management service wishes to deposit the information on its integration and on decisions already made by end users regarding the consent settings by means of a signal in the header of the HTTP/HTTPS request (see Stiemerling/Weiß/Wendehorst, research opinion on consent management pursuant to Section 26 TTDSG, 2021, paragraph 208 et seq.).

Re subparagraph 2

Subparagraph 2 is intended to prevent software for retrieving and displaying information from the internet being made available in such a way that it affects the signal stored through the recognised consent management service or via the provider of telemedia or on the settings of the end-users.

Re Section 18 (Measures by telemedia providers to integrate recognised consent management services)

Section 18 regulates voluntary measures by telemedia providers to integrate recognised consent management services.

Re paragraph 1

Paragraph 1 clarifies that the integration of recognised consent management services is voluntary for telemedia providers. The regulation aims to create an incentive for the development of recognised consent management services. It is assumed that telemedia providers will integrate voluntarily recognised consent management services where such services have been recognised by an independent body and can thereby be used to request and obtain effective consent in a legally secure manner. In addition, in the event of a corresponding demand from end-users to make preferential use of recognised consent management services when offered, it must be assumed that there is an interest of telemedia providers to integrate recognised consent management services. This is especially true in the segment of newly-established digital offerings.

Re paragraph 2

Paragraph 2 describes the technical and organisational measures to be taken by telemedia providers in order to obtain consent through a recognised consent management service.

Re subparagraph 1

According to subparagraph 1, providers of telemedia services integrating consent management through a recognised consent management service shall take technical and organisational measures in accordance with the state of the art so as to enable them to recognise that the end-user is using a consent management service and that it is possible to exchange information with the recognised consent management service.

Re subparagraph 2

According to subparagraph 2, the request for consent using integration with a recognised content management service is to be carried out by the provider of telemedia by means of an automated comparison of the requested consents pursuant to Section 25(1) of the TTDSG with the stored settings of the end-users in the recognised consent management service. The provider of telemedia may request the consents to the access to terminal equipment that it requires, for example via the so-called 'http response' from the consent management service and, if appropriate settings are stored, transfer them.

Re paragraph 3

Paragraph 3 lays down the technical organisational requirements to be taken into account by telemedia providers when they voluntarily integrate a recognised consent management service.

Re subparagraph 1

According to subparagraph 1, the provider of telemedia is to enable the recognised service to store the settings of end-users for their consent requests. This provision is intended to implement the requirement laid down in Section 3(1).

Re subparagraph 2

Subparagraph 2 provides that end-users are informed in a visible and appropriate manner that a recognised consent management service is involved and the decisions of the end-users deposited therein are taken into account. This can be done, for example, within the framework of a (visual) interface, for example when the provider of telemedia requests end-users to give their consent via its own form (consent banner). At this point, it should be made possible for the end-user to choose between consent management directly vis-à-vis the provider of telemedia or use of the integration of a recognised consent management service.

Re subparagraph 3

Subparagraph 3 regulates the participation of telemedia providers and with regard to the technologies and configurations to be fulfilled by the recognised consent management service pursuant to Section 7. The basic approach is that the concept laid down in Section 26(1) of the TTDSG on user-friendly and competitive procedures and technical applications for obtaining and managing consent can only be easily implemented if the parties involved work together. They can, among other things, establish a uniform technical standard that allows for the mutual exchange of data.

Re subparagraph 4

Subparagraph 4 concerns telemedia providers. These shall provide recognised consent management services with the information required by Articles 12 to 14 of Regulation (EU) 2016/679 in a machine-readable format. This requirement is necessary, inter alia, in order for recognised consent management services to implement the requirements set out in Section 3(2).

Re Section 19 (Measures by telemedia providers to take into account the settings of end-users)

Section 19 regulates how providers of telemedia who have voluntarily integrated a consent management service shall take into account decisions of the end-user regarding the consents requested by them pursuant to Section 25 TTDSG.

Re paragraph 1

The first sentence of paragraph 1 provides that telemedia providers should take into account the settings of end-users if they have voluntarily integrated a recognised consent management service. This consideration is based on good faith. End-users who use a recognised consent management service integrated by the telemedia provider to grant consent should be able to rely on their decisions being followed. The Ordinance also assumes that telemedia providers benefit in competition from the integration of a recognised service.

Sentence 2 regulates the case where the recognised consent management service does not manage the end-user's consent to the specific consent request. This may be the case, for example, because no end-user settings have yet been made for the specific request for consent, for example because advertising partners of the providers of telemedia, purposes of processing personal data or technologies used have changed. It is important that the providers of telemedia inform the end-user accordingly and strive to ensure that this specific demand will also be managed by the recognised consent management service in future, so that a comparison with the settings of the end-users can also take place here. The Ordinance therefore assumes that such cases will decrease over time. The Ordinance does not prohibit telemedia providers from asking for consent if they have not obtained consent through the settings of end-users deposited with the recognised consent management service. The effectiveness of consent depends solely on Section 7 of Regulation (EU) 2016/679.

Re paragraph 2

Paragraph 2 lays down that telemedia providers may also deposit with the recognised consent management service declarations of consent from end-users previously declared to them. This enables end-users to view their declared and managed consents in a clear location. At the same time, telemedia providers may transfer the consents that they manage to the recognised consent management service and have them verifiably documented.

Re Section 20 (Measures for neutrality)

Section 20 lays down a requirement of neutrality. It is intended to prevent, in particular, powerful market providers of software for retrieving and displaying content from the internet, and in particular powerful telemedia market providers, specifically favouring or hindering individual recognised consent management services. A factual reason to cooperate only with certain recognised consent management services exists in particular if the integration of the other recognised consent management services is only feasible with a disproportionate organisational, technical or economic effort. A disproportionate organisa-

tional, technical or economic effort cannot be justified solely by the fact that several recognised consent management services exist and would need to be integrated.

Re Part 5 (Concluding provisions)

Re Section 21 (Entry into force)

Section 21 regulates the entry into force of this Ordinance.