Conference of the independent federal and state data protection authorities

# Guide to video conferencing systems

As of 10/23/2020

Unofficial translation provided by Zoom

# Contents

# 1 Introduction

In situations such as the corona crisis, video conference services can play a central role in our communication. These services can be used to enable group communication in addition to video calls. This guide explains data protection requirements for the use of video conferencing by companies, public authorities, and other organizations.

Personal data of the participants is processed within the framework of video conferences. Due to the already high, and still growing, functional diversity of today's video conferencing solutions and the multitude of other IT services connected to the video conference systems as peripheral systems, there is a wide range of personal data to be taken into account.

This concerns statements of content and the transmission of sounds and images of the participants and, if applicable, their surroundings, such as their home, workplace or other place of residence (content data). Images and sounds of the participants also contain enough information to be able to identify them by their voice or facial features. However, depending on the type of service, it is also possible to send messages in the form of graphic or text chat messages or to display one's own screen for individual or all participants; the allocation of these messages or display processes to the participants who have expressed, presented or received them must be regarded as personal.

Furthermore, metadata on the conduct of communication, data on professional contacts, working hours and work performance can be processed on the basis of data from one or more video conferences (framework data).

In addition, personal data may be contained in textual contributions by participants and in documents discussed and made visible during video conferences. This data may relate to the conference participants themselves, but also to non-participants inside and outside the institutions.

Personal data of those from the environment of the participants, whose images or sounds may also be processed by the conference system, may also be affected. Example: a person from the household of the conference participant walks through the image or speaks in the background.

The controller organizing the video conference is obliged to check the extent to which it is authorized to process the data. In doing so, it must in particular observe the principle of data economy. It must therefore examine the extent to which the data processing associated with the specific use of the conference system can be limited to what is necessary to achieve the

purpose through the selection of the systems used and through technical and organizational measures. If it uses tools from a provider, it must clarify the data protection relationship with that provider. It must also ensure that the technical and organizational measures required to protect the relevant data are taken. It must also provide information on data processing in the required form. This handbook is intended to help controllers.

# 2 Operating models

In principle, the controller has three options when operating a video conference system: Either it uses an online service (software as a service), operates the system itself, or has the system operated by an external IT service provider.

## 2.1 Self-operated service

An institution (company, authority, etc.) that wants to operate a video conference service itself can use free (open source) or other software for this purpose and is therefore in control of which software is used and what data processing is involved.

Self-operated software has the advantage that any questions regarding the necessity of concluding an order processing contract (Art. 28 GDPR) [1] or an agreement on joint responsibility (Art. 26 GDPR)[2]do not arise, nor do those regarding possible joint liability.

At the same time this ensures that data is processed exactly as desired. The operation of video conference systems on a self-operated infrastructure has the advantage that only the controller can analyze and control the content and framework data of the systems, as it is the only one who can access the data required for this.

Controllers must then of course have sufficient technical and personnel capacities for operation and maintenance and take suitable technical and organizational measures to protect the data. This is to be expected from large and efficient institutions, but can pose a personnel and technical challenge for smaller controllers.

It is therefore also possible to commission service providers.

## 2.2 Operation by an external IT service provider

Anyone who prefers a particular software but cannot operate it themselves can commission a service provider for this purpose. If data processing by the service provider is limited to the

1 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf
2 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf

fulfilment of this order, this is considered to be order processing. An order processing contract must be concluded pursuant to Article 28(3) GDPR for this purpose.

In particular, data protection authorities recommend that public administrations operate such systems themselves or provide one or more video conference services on a centralized (national or regional) basis. Through the relevant service providers engaged by the national government and federal states, systems can, if necessary, be adapted to the needs of the relevant sectors and purposes, in particular the school system.

It should be noted that the software used or offered to participants must be examined for data outflow to the manufacturer and third parties. This includes diagnostic and telemetry data or other data outflows.

Corresponding data outflows must be prevented, unless there is a legal basis for this.

## 2.3 Online service

Instead of self-operating the video conference system or having it operated by a service provider according to personal perceptions, there is also the option to use existing online services.

The first argument in favor of an online service is the ease with which the video conference system on offer can be made available, in which case the controller concludes a contract with the provider. Depending on the concrete design of the online service, central configuration options (e.g. data outflow, access rights) must then be checked and adjusted if necessary. Then, if required, the authorized persons register a video conference with the provider and invite the participants. The controller must conclude at least one order processing contract (see Section 3.5.2).

The controller must ensure compliance with data protection principles by selecting a suitable provider (see the requirements of Art. 28(1) GDPR) as well as giving appropriate instructions to the service provider and making its own arrangements.

To this end, the controller must examine the order processing contracts, terms of use and security certificates submitted by the processor as well as its privacy statement.

As a matter of principle, when selecting a provider, care must be taken to ensure that the provider takes appropriate technical and organizational measures, that the processing is carried out in accordance with GDPR requirements and that the provider offers sufficient guarantees for this. However, the largest and best-known providers of video conferencing products are based in the United States and process the data there. Data transfers to the United

States or other third countries must comply with the requirements of Chapter V GDPR (see the following paragraph and Section 3.5.6). The use of standard contractual clauses as a means of justifying the data export must take account, among other things, of the need for the controller to analyze the legal situation in the third country with regard to administrative access and legal remedies for data subjects before the transfer begins. Additional measures are required in the event of deficits; data export may have to be omitted.

The ruling of the ECJ in the Schrems II case of July 16, 2020 (C-311/18) invalidated the adequacy decision on the EU-U.S. Privacy Shield. The Privacy Shield is therefore no longer available as a tool to ensure adequate protection of data transferred to the United States. When using standard contractual clauses and other contractual guarantees as a basis for transfers of personal data to the United States, the ECJ has ruled that additional measures must be taken to ensure that this data enjoys a level of protection during and after transfers substantially equivalent to that in the EU. Further analysis is needed in order to make more concrete statements, in light of these requirements clarified by the ECJ, on whether and under which additional safeguards personal data can be transferred to the United States or to US providers. For this reason, DSK currently recommends that the use of video conferencing products from US providers be carefully examined. This also applies if the contracting partner is a European subsidiary. The same applies to European providers if they transfer their personal data to the United States.

# 3 Legal requirements

Before operating or using a video conference service, the roles and responsibilities of the parties involved must be clearly assigned and clearly defined in order to ensure compliance with GDPR provisions (see also Section 4.4). Pursuant to Article 4(7) GDPR, the controller is the body which, alone or jointly with others, determines the purposes and means of the processing. Controllership is not the same as the existence of an authority to process data. The concept of controllership only clarifies that the body which, in accordance with Article 4(7) GDPR, determines the purposes and means of processing personal data must fulfil the data protection obligations of the controller resulting from the GDPR.

## 3.1 Self-operated service

If, for example, an employer or school operates a video conference system, the employer or school as the organizer of the video conference is a controller within the meaning of the GDPR, as it determines the purposes and means of processing in the context of the use of this system. This applies in particular to data exchanged directly within the framework of using

the video conference system (content data, e.g. chats stored centrally on the server, shared documents, recordings of the conference), but also to framework data, particularly metadata, necessary to maintain the system.

## 3.2 Operation by an external IT service provider

The operator of the video conferencing system may process personal data as a processor on behalf of the controller. If, for example, the controller uses a service provider who provides the technical infrastructure and has no personal interest in the personal data, an effective order processing contract must be concluded with this provider pursuant to Article 28 GDPR (see Section 3.5.2). When selecting the processor, care must be taken to ensure that the processor provides sufficient guarantees regarding the necessary technical and organizational measures. Since, in practice, the corresponding contracts are often based on the service providers' model contracts, particular attention should be paid to ensure that the processor's obligation to follow instructions is comprehensively regulated and that the controller is given sufficient powers of control.

## 3.3 Online service

If the provider of the service used also processes the participants' personal data for its own purposes or the purposes of third parties (e.g. processing of data on user behavior, use of analysis tools, tracking for advertising purposes), it should be noted that the organizer requires a legal basis for any disclosure of personal data to the provider just as the provider requires a legal basis for any processing of personal data in its own – possibly joint – controllership. This is often the case for online services.

However, a legal basis for the disclosure of personal data to the provider of the service is regularly difficult to justify (see Section 3.4.6).

If the provider processes personal data arising from the use of the video conference service for its own purposes or the purposes of third parties, joint controllership must be examined pursuant to Article 26 GDPR. In particular, where there is joint controllership, an agreement must be concluded. This agreement does not replace the legal basis required by each of the joint controllers, but constitutes an additional requirement.

At all times, it must be made transparent to the data subjects who is processing what personal data and in which role. The organizer must be clearly identified as the controller for the data processing, stating the contact details and, if applicable, the data protection officer and their

contact details. This also applies to the provider of the service, who may have joint controllership, in such a way that it must also be clearly stated what data is processed under joint controllership. If, on the other hand, the provider is a processor, it only has to be named among the recipients of the data, but not as controller.

## 3.4 Legal basis for the controller and purpose limitation

For the lawful processing of the personal data of persons participating in the conference, the controller requires a legal basis in accordance with Article 6 GDPR.

### 3.4.1 Structure of the legal bases

Depending on the context of the processing situation, a standard of authority may result from Article 6(1)(a), (b), (e), (f) GDPR, possibly also in conjunction with national law. Data processing can thus be based on effective, i.e. voluntary and informed, consent. In addition, Article 6(1)(b) GDPR (performance of a contract) could be considered as a legal basis. If, in the course of performing the contract, there are alternatives to video conferencing as a matter of principle, or if employees of other companies and other persons take part in a video conference, legitimate interests pursuant to Article 6(1)(f) GDPR can also legitimize data processing, in which it should be noted that, in this case, the controller must indicate the right to object in accordance with Article 21(4) GDPR.

However, public authorities cannot refer to Article 6(1)(f) GDPR in the performance of their tasks (Article 6(1)(2) GDPR). In the case of public authorities, however, Article 6(1)(e) GDPR in conjunction with the relevant standard in German law, such as school legislation, may be considered as the legal basis.

### 3.4.2 Consent

If the consent of the data subject is to be used as the legal basis for the processing of personal data, the following should be noted:

Consent is only effective if given in an informed and voluntary manner (see Article 4(11) GDPR). Voluntariness can only be assumed if there is a real choice regarding participation in the video conference.

Voluntariness is often questionable, particularly in a professional or school context, especially when information, which is essential for the performance of the professional activity or for school teaching, is communicated exclusively via video conference. The voluntariness of participation in the video conference will then regularly not be given, so that the consent of

the data subjects is no longer a legal basis. In such cases, effective consent can only be considered if the voluntariness of the consent is ensured by additional measures, such as providing those who do not wish to participate in video conferences with the relevant knowledge in an equivalent form by other means, or by offering other means of communication (e.g. participation in the conference by telephone).

Unless voluntariness can be ensured by such measures, the use of video conferencing cannot be based on consent as a legal basis, so the controller must consider whether it can base its use on another legal basis (see Section 3.4.1).

### 3.4.3 Employers as controllers

If the data controller is also an employer which induces its employees to use the video conferencing system for the purpose of performing their contractual tasks, the legal basis for data processing is Section 26(1)(1) of the German Federal Data Protection Act (BDSG) or the corresponding provision of state law in the public sector. However, the necessity of transmitting image data must always be checked.

In the employment context, it is possible to regulate the processing of employee data more specifically through collective agreements. Company and service agreements can be used in particular to specify the general legal provisions in specific use cases, i.e. whether and how video conferencing is used. However, the level of protection must not fall below that of the GDPR.

### 3.4.4 Processing of special categories of personal data

If special categories of personal data, such as health data, are addressed in the video conference, this data processing must also be permitted pursuant to Article 9(2) GDPR, possibly in conjunction with a national law. The same applies if the occasion of the video conference already relates to data within the meaning of Article 9 GDPR, for example in religious education or theological studies.

If special categories of personal data are processed during the video conference, explicit separate consent may be required pursuant to Article 9(2)(a) GDPR. However, such consent is only effective if it is an explicit, informed, voluntary, prior, active consent for the individual concrete case and separately declared as well as reasonably revocable at any time.

### 3.4.5 Participation from private residences

If employees participate from their home office, the problem arises that other participants are not allowed to gain insight into their private sphere through images or sounds without the employees' consent. The employer must therefore use technical and organizational measures (Art. 25(1) GDPR) to ensure that such insights are not possible, e.g. by aligning the camera or providing a screen or – if offered by the provider of the video conference system – by inserting a virtual background. As an alternative to such technical and organizational measures, the consent of the employees (Section 26(2) BDSG) is conceivable, in which the voluntariness of the consent must be ensured in particular.

Controllers should inform their employees and other participants in video conferences who (may) participate from private homes about the risks involved. Unfavorable camera orientation, taking the equipment into unsuitable rooms or rooms occupied by third parties, the unprepared visual and/or acoustic appearance of third parties in the video conference and similar "mishaps" must be avoided.

### 3.4.6 Processing by providers for their own purposes

If a provider processes personal data for its own purposes, it cannot refer to the legal basis on which the organizer bases the processing, but requires a legal basis itself – as the controller within the meaning of data privacy laws (Art. 4(7) GDPR). For example, Section 26 BDSG only regulates the processing of personal data by employers, but not data processing by the provider for its own purposes. The same applies to the provisions of state school legislation. The disclosure of personal data to the provider of the service for its own purposes is associated with a change in the purpose of the processing. Such a change of purpose is only permissible within the narrow limits of Article 5(1)(b), Article 6(4) GDPR. As a rule, there will be no compatibility of purposes within the meaning of these requirements. It must also be possible to place disclosure to the provider on a legal basis.

In relation to a processor, the order processing contract must ensure that the processor processes the personal data of participants only on the instructions of the controller and not for its own purposes.

### 3.4.7 Processing of third-party data

Whenever personal data of third parties not participating in the video conference is discussed and thus also processed within the context of the conference, the general legal bases must be applied.

### 3.4.8 Transparency, recordings of video conferences

Furthermore, the nature and purpose of the processing of personal data must be clearly defined in order to comply with transparency requirements. In principle, the processing must be limited to the purpose of the video conference, as further processing and evaluation of the conference data is generally not necessary. This applies in particular to recordings for which the legal basis must be examined separately. Exceptions are conceivable for open events or public seminars and public lectures, where a recording of the speaker may be necessary in individual cases. If there is no special documentation requirement, consent to the recording and further processing (possibly further consent to be granted independently of the consent to the data processing associated with participation in the video conference) is therefore regularly required. The recording option must be mentioned when fulfilling the obligations to provide information (see also Section 4.6).

The audio and video data as well as the framework data of the conference may only be processed for as long and as far as it is necessary for the transmission of messages by a service provider or as part of necessary documentation. Storage beyond the conference is regularly neither necessary nor compatible with the purpose of collection, Article 5(1)(b), Article 6(4) GDPR. This means that any existing recording function must be disabled by default.

Users should be informed that the recording (especially secretly) of video and/or audio data, the storage and distribution of such recordings may be punishable by law.

## 3.5 Obligations of the controller

When operating or using a video conference service, the controller as the organizer must, among other things, fulfil the following obligations in accordance with the GDPR.

### 3.5.1 Obligations to provide information and rights of data subjects

Controllers must provide clear and unambiguous information to conference participants on the data processing associated with the use of the service in accordance with Articles 13 and 14 GDPR. In order to ensure transparency of processing, the information must be presented in such a way that it can be understood by the average user of the service without excessive effort (Art. 12 and Art. 5(1)(a) GDPR). Excessively complex wording and technical or legal terms should be avoided. Where the use of technical terms appears unavoidable, they must be explained in a comprehensible manner. In the case of extensive data protection declarations in particular, care must also be taken to ensure that clarity is maintained by means of a

comprehensible structure and meaningful headings, so that it is possible for the data subjects to select specific information (e.g. for recording the conferences or transmitting data to third parties).

The obligations to provide information pursuant to Article 13, 14 GDPR include, in particular, information on the purposes for which and on what legal basis what personal data is processed, whether the provider of the video conference service or software can obtain knowledge of such data, whether and, if so, for how long personal data is stored after the end of a conference session and whether personal data is to be transferred to a third country. In view of the controller's transparency obligations (Art. 5(1)(a) GDPR), it should also inform the participants whether and if so what type of encryption[3] is used when operating the system. This information is of particular importance for those participating in a video conference on the basis of consent.

In addition, the controller must also inform the participants about the legal basis of the individual processing operations and – insofar as the controller invokes Article 6(1)(f) GDPR – about the legitimate interests pursued. In addition, in this case the participant must be informed of his/her right to object in accordance with Article 21(4) GDPR. Where different standards of authority apply, it should in particular be made clear whether and, if so, which processing operations are based on the consent of the participant. This is because only if the participants are aware of their authority to dispose of their own data can they exercise this authority (e.g. if an employee does not know that the use of the video function in the context of official meetings is voluntary, this voluntariness has no protective effect on him/her). From the point of view of the controller, in the case of consent-based processing operations, there is also a risk that inadequate provision of information to the participants could lead to the unlawfulness of the data processing, since only informed consent can justify the processing of data (see Art. 4(11) GDPR).

If the provider of the service processes data for its own purposes – insofar as this is at all permitted (see Section 3.4.6) – the obligations to provide information generally (also) apply to the provider itself. The organizer of the video conference must in principle also inform the participants about such processing operations itself in accordance with Article 13(3) GDPR and cannot merely refer to the data protection provisions of the service used. In addition, the organizer should inform the participants about the possibilities for them to work toward the

[3] It is not necessary to specify the cryptographic procedure, but to what extent the encryption is suitable for keeping the encrypted data secret from third parties and from the operator of the service, and to what data it applies.

protection of their personal data within the privacy settings of the service itself (e.g. by using a pseudonym, setting an artificial background). In particular, the participants should also be informed whether a recording of the conference by the organizer is possible and, if the recording function is activated, the participant should be informed about the ongoing recording.

In addition, the rights of the data subjects under Articles 15 to 21 GDPR must be guaranteed. Insofar as the organizer of the conference is also responsible for data collected by the service, possibly even without the organizer being able to access it itself, it should consider, when selecting the service, to what extent it allows both content data and framework data to be erased specifically or in general. The erasure of the content and framework data of the ended conference must also be carried out regularly and immediately after the end of the video conference, irrespective of a request by the data subjects pursuant to Article 17 GDPR, since the purpose of the processing of the personal data has then been achieved and further storage of the data is not necessary on the basis of a legal obligation to which the controller is subject under Union law or the law of its Member State.

### 3.5.2 Order processing contract

GDPR offers a high level of data protection. This must not be jeopardized by the involvement of service providers. If the video conference system is operated by the provider or if the provider has the option to access personal data, an order processing contract must be concluded with it. Depending on the solution used, such an access option can also exist for systems operated by the controller itself. Please refer to Short Paper No. 13 of the Data Protection Conference (Order processing)[4]. Pursuant to Article 5(2) GDPR, the controller must be able to prove at any time that it complies with the data protection principles. The order processing contract must therefore undoubtedly cover all the requirements of Article 28 GDPR. Ambiguities in the order processing contract are therefore regularly a criterion for exclusion for the use of the relevant provider.

### 3.5.3 Processing directory

The organization of the video conference(s) must be included in the directory of processing activities in accordance with Article 30 GDPR. Please refer to Short Paper No. 1 of the Data Protection Conference (Directory of processing activities)[5].

4 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf
5 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf

### 3.5.4 Reporting obligation for data breaches

In the event of a violation of the protection of personal data in connection with the video conference, the controller must comply with the obligations arising from Articles 33 and 34 GDPR.

### 3.5.5 Data protection impact assessment

The controller must check whether a data protection impact assessment has to be carried out in accordance with Article 35 GDPR. This may be the case in particular if special categories of personal data of the participants or other persons are extensively processed in the video conference pursuant to Article 9 GDPR. Please refer to Short Paper No. 5 of the Data Protection Conference (Data protection impact assessment)[6].

### 3.5.6 Specifics for transfers to third countries

GDPR offers a high level of data protection. The regulation also applies to providers of video conference systems established outside the EU, under the conditions laid down in Article 3(2) GDPR. Providers from non-EU states are generally also subject to the legal provisions of their home state and thus, under certain circumstances, the access rights of authorities of third countries, which may make compliance with the GDPR data protection requirements more difficult or conflict with the latter in individual cases.

If video conference systems are selected that lead to data transfers to third countries, i.e. countries outside the EU or the European Economic Area, the transfer must comply with special conditions (Chapter V, Art. 44 ff. GDPR, see also Short Paper No. 4 of the Data Protection Conference[7]). Such transfers may occur in particular in the case of providers who are themselves established in the third country or use subcontractors from third countries. A transfer of data to third countries also occurs when the provider or a subcontractor from the third country accesses data processed in the EU (e.g. for maintenance or support purposes).

For some third countries, the EU Commission has decided that there is an adequate level of data protection, in which case no further conditions must be met for the data export to be permissible (Art. 45 GDPR).

6 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf
7 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf

Given that ECJ ruling C-311/18 (Schrems II) invalidated the EU Commission's decision on the EU-U.S. Privacy Shield, it is no longer available as a means of ensuring an adequate level of protection in the United States, as explained under 2.3.

The conditions set out in Chapter V GDPR can otherwise be complied with, e.g. through the standard contractual clauses of the EU Commission which the controller concludes with the provider as the processor.

However, the ECJ ruling on Schrems II, as already mentioned under 2.3, also has an impact on the possible use, in conformity with data protection law, of the other instruments for transfer in international data traffic pursuant to Article 46 GDPR, such as standard contractual clauses and binding corporate rules (BCRs). These effects arise not only with regard to data transfers to the United States, but also to other third countries. Here, also, controllers must verify that the transfer instruments chosen ensure that the personal data to be transferred to the third country enjoy substantially the same level of protection during the transfer and in the third country itself as in the EU and, if necessary, take additional measures to achieve this protection. If the inadequate level of protection stems from access by public authorities, it is difficult to envisage sufficient additional measures in the field of video conference services, since certain basic conference data must, at least, be accessible to the provider for technical reasons. Pursuant to Article 5(2) GDPR, controllers using video conference services must be able to prove that they have carried out this check and that the data is sufficiently protected in the third country in accordance with these standards. On July 23, 2020, the European Data Protection Board (EDPB) adopted FAQs on the effects of the ruling in general and the consequences for individual transfer instruments.[8]

# 4 Technical and organizational requirements

In accordance with Articles 24, 25 GDPR, the video conference system must be set up by selecting and implementing suitable technical and organizational measures in such a way that it meets the GDPR requirements for the processing of personal data. Guidance on the implementation of these requirements can be found in the following sections.

[8] https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/frequently-asked-questions-judgment-court-justice-european-union_en

## 4.1 Transmission security

Video conference systems must implement state-of-the-art encryption. The Federal Office for Information Security (BSI) provides recommendations on suitable cryptographic procedures[9].

The transmission of video conference data requires at least transport encryption in accordance with the relevant BSI technical guidelines[10]. Transport encryption must guarantee the confidentiality, integrity and authenticity of all transmitted data: both content data and framework data[11].

In particular, if the processing of data within the framework of a video conference can lead to a high risk for data subjects, the controller and, if applicable, the processor must take appropriate technical and organizational measures, to ensure in particular the confidentiality of the transmitted content data on central servers and the IT components otherwise involved. This can be ensured by end-to-end encryption and the encryption of stored data, for example. Effective end-to-end encryption requires that participant devices authenticate each other in a verifiable manner and that new transient encryption keys for each conference are generated, negotiated or distributed under control of the conference participants in such a way that the operator cannot gain knowledge of the keys. At the time of producing this paper, end-to-end encryption solutions, which meet these requirements and enable video conferences for a higher number of participants, even if the participants only have limited or varying bandwidth and computing power available to them on the endpoints they use, were not yet commercially available. In the circumstances described, transport encryption may therefore be sufficient to fulfil the legal obligations, provided compensatory measures ensure a level of protection appropriate to the risk. The compensatory measures must extend to the security of the operator's services and systems – i.e. the service provider or the contractor used to host the service (additional hardening) and must also include organizational measures taken by the operator that make it difficult for employees of the operator to gain knowledge of the processed data.

In the event of suspected unauthorized outflow of personal data in the course of video conferences, the benefits of using certain functionalities of the service (in particular private chats, screen sharing and making documents available in a workspace open to all participants) should be weighed against the risks involved and, where appropriate, the functionalities

9 https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/tr02102/tr02102_node.html
10 ibid.
11 see Section 1 for the definition

should be disabled. It is helpful if the organizer can reliably and technically disable corresponding functionalities centrally for all participating devices. A suitable measure for the detection of such outflows may also be a logging of the use of the above-mentioned functionalities. The transparency of such logging for the participants must be maintained.

Use of the individual functionalities of a video conference system in use should be considered separately and in context. For example, a controller may have a document management system (DMS) in use. It should be considered whether this system is preferable to the document exchange functionality of the video conference system. The examination must take particular account of the risks to the rights and freedoms of data subjects.

If the controller (or a contractor used for hosting the service) operates server software for the operation, or if the controller makes (mobile) applications available to the participants for which it has acquired rights of use from a third party, it is also obliged to ensure that the manufacturer and other third parties do not gain access to the processed data, including individual parts such as usage data.

## 4.2 User authentication

Only authorized persons should be able to access a video conference session and its data. For this purpose, participants must authenticate themselves to the video conference service.

The minimum level of authentication required depends on the severity of the risks to the rights and freedoms of the data subjects that may arise in the event of a breach of the confidentiality or integrity of the content data.

### 4.2.1 Normal risks

For normal risks, authentication with user name and suitable password is sufficient. The authentication protocol should be designed in such a way that passwords are neither transmitted nor stored by the service provider. State-of-the-art authentication procedures prevent data, derived from the password and transmitted in the course of one authentication process, from being reused for a second authentication process. They also prevent the verification data, stored by the controller or by the processor carrying out the authentication, from being used for a login in order to minimize the consequences of compromising this data.

### 4.2.2 High risks

If the breach of confidentiality of the information on natural persons likely to be contained in the content data of the conference entails high risks for the rights and freedoms of those persons, at least one state-of-the-art two-factor authentication must be carried out. Depending on the level of risk, software or hardware tokens are particularly suitable for this purpose.

### 4.2.3 Authentication service

In order to ensure consistent management of user authorizations, it is strongly recommended that controllers base user authentication on procedures already used for other procedures. When deciding on a possible connection, the specific context of use and the risks associated with the connection must be taken into account. If the video conference service is connected to a directory service via LDAP, the user passwords are usually processed in plain text. Therefore, this method is primarily suitable for self-operated video conference systems. For non-hosted video conference systems, OpenID Connect can be used instead. The identity provider must ensure the integrity of the authentication process and the non-interlinking of different usage processes.

For the authentication of persons outside the controller's institution, authentication by an identity service provider may be used if the controller is convinced of the relevant aspects of the identity of the participant(s) in the run-up to or during the first video conference.

For use cases which require prior identification of users and are likely to lead to the transmission of particularly sensitive personal data via third parties, appropriate procedures must be implemented to enable the authenticity of users to be verified retrospectively.

### 4.2.4 Guest participation

Under the following conditions, video conference systems may offer guest access that does not require prior identification of the user:

- Guest access must be required for the specific use case.
- The risks for data subjects arising from unauthorized participation are negligible.
- It is guaranteed that only persons who are known to each other participate.
- Unauthorized persons are detected and can be actively excluded even before they can actively participate in the video conference.

Guest access can be made possible in the usual systems, e.g. via an invitation link which is communicated to the guests in the run-up to the video conference session and where the guests only have to assign a pseudonym to themselves before the video conference begins. The recipients of this link must be made aware of the consequences of any unauthorized distribution of the link. The transfer of the link must maintain confidentiality at an appropriate level.

## 4.3 Installation and software update

Technical weaknesses and other security gaps in video conference systems may, once they become known, lead to an unacceptable processing risk and thus to a halt in use. They must be remedied within a reasonable period of time, and immediately in the case of high risks. This must be done by the software manufacturer or the provider of the service; controllers must ensure this. Functional additions should, if the use case permits, be made by means of update methods specific to the operating system (package management). If the video conference systems operate in an administered environment, the associated software should be updated centrally.

All components installed on a client in order to participate in a video conference must be able to be uninstalled just as easily and completely.

Even if a participant only uses a native client once, it must be ensured that no unmaintained software remains on the system and poses a potential security risk.

If web-based video conference systems are used, an up-to-date web browser version must always be used for secure operation. The same applies to any necessary browser extensions.

## 4.4 Separation of roles

Video conference systems for large numbers of participants should permit the establishment of at least the following roles:

1. administering persons:

   This role typically has the authority to define parameters of the conferences to be held (e.g. permission or prohibition of recordings and chats which parallel the video conference) and the assignment of the moderation role.

2. moderating persons:

   This role typically has the authority to schedule video conferences, invite or exclude participants, open or close access to a conference, assign participants to groups where separate exchanges take place, and assign the presentation role to individual participants.

3. presenting persons:

   This role typically has the authority to provide audiovisual media and documents for the attention of participants and to control their requests to speak.

4. participants:

   This role typically only has the authority to control one's own recording and playback devices.

The roles may be tailored differently if necessary, provided the responsibility for controlling the implicit processing of personal data remains clearly assigned.

Each participant must be able to disable his/her microphone and camera at any time. It must not be possible to activate the participant's microphone and camera without his/her consent.

For high-risk applications, a user management system which ensures the authorization of the participants to assume one of the above-mentioned roles is mandatory (see also Section 4.2).

## 4.5 Data economy

Video conference services should only process the technical information and other information strictly necessary for the provision of the service. In particular, protocol data should only be processed for the purpose of the conference. Analyses of usage behavior and the processing of personal diagnostic and telemetry data by the provider of the service, used for its own purposes, contradict the principle of data economy (see Section 3), unless they are necessary for the provision of the service and have their own legal basis. An example of critical data processing would be the chaining of uses of a user account that participates in conferences of different conference organizers.

Video conference systems must comply with the principles of data protection through technology design and privacy-friendly default settings (Art. 25 GDPR). In order to save data, the camera, microphone and screen sharing of participants must be switched off by default before entering the conference. To enable participants to decide when to switch on these

devices and functions, it must be transparent to them who or what types of participants can see and hear them.

## 4.6 Transparency

To supplement the legally required references in the data protection regulations issued by the operators of the video conference systems (see Section 3.5.1), the manufacturers of the systems should also make statements on the technical implementations, the standards used, software libraries and licenses.

It must be easy for the participants to understand and it must be recognizable in a prominent location whether and, if so, which data processing operations are carried out beyond the actual purpose of the video conference. In particular, functions such as video and/or sound recordings as well as attention analyses, if they are at all permitted, must be demonstrably announced to the participants before processing begins and may only be activated after this function has been enabled. In addition, the legal requirements must be observed.

Open source systems can promote transparency, as technical experts can perform more in-depth analyses of individual function calls here than in proprietary software. Technical papers such as white papers can systematically disclose the technical structure and key components of video conference systems. Security audit reports should be made publicly available, if necessary, after a reasonable period of time to resolve any security problems found.

## 4.7 Recordings

If recordings of the video conference are not permitted (see Section 3.4.8), the recording options for participants must be technically prevented if the controller has influence over this (i.e. within the scope of its own organization). If this is done by a configuration setting, only an administrator may cancel it. The participants in the video conference must be informed that recording is not permitted.

Where recordings are permitted by way of exception, they may only be activated by particularly privileged users, such as moderators. Participants in a video conference must be notified when a video conference is being recorded in whole or in part, either by an explicit notice, to be confirmed by the participants, or by marking it in the user interface.

Recordings of video conferences should be saved encrypted. Where there is a high risk, this is mandatory.

## 4.8 Intervenability

Participants must have the technical ability to participate in conferences, at least temporarily, by receiving but not transmitting, i.e. by switching off the camera and microphone, with separate disabling options for audio and video transmission.