Information for those responsible in Berlin on providers of video conferencing services

The Berlin Commissioner for Data Protection and Freedom of Information as data protection supervisory against the background of the corona pandemic, the authority is being increasingly protection-compliant use of video conferencing solutions. For our supervision responsible persons responsible for checking the legality of the use of various To facilitate solutions, we publish the results of the conducted quick reviews of video conferencing services from various providers, where we found the Emphasis on assessing the legal compliance of those offered by providers have placed order processing contracts.

If the providers, after a short check, have legally compliant order processing contracts on horseback and have provided us with information or test access, we went through two more test steps. On the one hand, we searched cursorily for clues as to whether the providers export data to third countries. On the other hand, we checked some technical ones Characteristics of the Services relevant to compliance with data protection principles are. Of course, these technical properties are only relevant if the order processing contracts are legally compliant and we have not found any indications of this the have that the provider with regard to subcontractors involved or the location of the Data processing deviate from the provisions of the contracts. Only the products that this met the basic requirements, the technical review was then subjected to

The assessment is therefore made in two parts: on the one hand legal (Part 1), on the other hand - as far as we have legally reached the permissibility of the use by Berlin responsible persons - technical (part 2). There are separate tables for the overview of the two parts of the assessment.

Considered operating model

The present assessment extends exclusively to services that use video conferencing

offer as Software-as-a-Service (SaaS). From a technical point of view, however, this offer

with pre-configured settings, which in many cases cannot be changed.

NEN, the operation of a service by those responsible themselves (possibly on a

platform provided by the processor) is regularly preferable, since the persons responsible

You can then fully determine the circumstances of the processing yourself. In from-

Depending on the processing circumstances and the specific risks, this may

also be the only legally compliant solution available.

Version 2.0 of February 18, 2021

Part 1: Design and implementation of the

order processing relationship

The present notes lay the model contracts for the evaluation of the individual services

based on which the service providers ask their customers to fulfill the obligation pursuant to Art. 28

3 GDPR offer. General recommendations for auditing contract processing

We have contracts with providers of video conferencing services as of July 3rd, 2020

at the address https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientation-

fen/2020-BlnBDI-Recommendations_Examination_Order Processing Contracts_Videoconferencing-

Services.pdf published.

If there are legal deficiencies in the checked documents, the services may

only be used if different agreements have been made with the providers

the.

Data exports and access options from authorities in third countries

These notes take into account the requirements for data exports to third countries

Court of Justice of the European Union (ECJ) in its “Schrems II” judgment of July 16, 2020

(Case C-311/18). On the other hand, they do not take into account the possible legal

Consequences should there be a so-called "hard Brexit" in data protection issues

come, so the United Kingdom should be a third country from April 1 or June 2021

to be treated without special regulations, without an adequacy decision by the

EU Commission on the level of data protection in the UK is, or should be

the agreement, the United Kingdom is temporarily still under data protection law

to be treated as a member of the EU shall be rendered null and void. They also do not take into account

the question of what impact it has when the provider of a video conferencing service

Although the accruing personal data within the European Economic

room, but either itself or via a group company under foreign law

subject. This could be particularly true in the context of video conferencing services

US companies or their subsidiaries on data protection regulations

problems, if not through additional measures according to European

Legally inadmissible access by foreign authorities can be prevented (e.g. by means of

Circuit of a data trustee not subject to foreign law, through which access

of the provider himself is excluded for personal data). indications that

that access authorizations that are not permitted under European law could exist in this respect,

there is in the meantime. For example, a provider with a “green” rating is on the

legal level, in addition to inadmissible data exports, only counteracts the fact that the contract

illegal processing of personal data not only from the law of the

European Union or Member States. In this respect, the provider expressly informed us

happily that, as a US company, you are in a conflict between legal systems

conflicting requirements that cannot be solved by the company.

Those responsible in Berlin who want to use video conferencing services contact their providers directly

or indirectly subject to foreign law, must therefore be subject to appropriate examinations

do it yourself and keep a close eye on further developments.

Legal framework for OTT services

As of December 21, 2020, the EU member states would have the regulations of the EU Directive on

Transpose and apply the Telecommunications Code1 into national law. Thereby

would be so-called over-the-top services (OTT services) such as video conferencing services via the

Internet has been subjected to a new legal framework. Since a timely implementation in

Germany did not take place, the previous legal situation continues to apply.

1 Directive (EU) 2018/1972 of the European Parliament and of the Council of December 11, 2018 on the European

Electronic Communications Code.

Evaluation scheme part 1 (legal examination)

For the legal assessment of the contract documents and the actual

We used the following evaluation scheme for data processing.

overall grade

There are deficiencies that prevent legally compliant use of the service

and their elimination likely to require significant adjustments to business processes

requires about when

 According to the contract of the provider, the personal data processed in the order

may also process gene data for its own purposes,

 the contract only provides for data deletion with a delay or to a limited extent,

 the contractual requirements for the involvement of subcontractors

are currently not sufficiently designed and are likely to change

required in the contracts between providers and subcontractors

are,

 the contract provides for impermissible data exports that are part of the use

of the service cannot be avoided either.

We also rated services as "red" for which we are in the contract itself

have not found any defects, but according to the result of our technical

involve service providers who are not contractually subcontracted

contract processors are approved, and/or where data exports take place, the

are not permitted under the contract.

There are deficiencies that prevent a legally compliant use of the service

close, but their removal probably without major adjustments

of business processes is possible. This also includes services that are contractually

provide for permissible data exports, which, however, within the scope of the use of the service

tes can be avoided. (This rating was not used in this version

give.)

No defects were found in our quick check.

types of defects

We have identified deficiencies found during the legal assessment as follows:

(v)

(d)

(e)

(Contract) The checked contract documents have legal deficiencies.

(Service provider) In the provision of the video conference service,

service providers included in our data traffic checks, which are not

processors are approved. The check for activation not allowed

The service provider only takes place if the preliminary check of the contract documents

documents has not revealed any defects.

(Export) As part of our data traffic checks, we have not

envisaged data exports to third countries. The check for no

Permitted data exports only take place if the upstream verification of the

supporting documents has not revealed any defects.

A detailed description of the defects found can be found in the notes to

the individual providers at the end of this paper.

Version 2.0 of February 18, 2021

Place of data processing/waiver of data exports - column "EU"

□

Those services are marked with this symbol in the "EU" column

where according to the contract the place of processing of personal

Data refer to the European Union or the European Economic Area

is restricted. If this is not the case, is for the associated data exports

according to Art. 44 et seq. GDPR, an additional justification is required. in case of non-

filling the symbol □ is used.

Evaluation part 1

For the sake of clarity, we have listed the tested video conferencing services from a legal point of view

follows in summary (for the technical evaluation of the services rated green here

see assessment part 2).

EU

service

URL

version of the documents

□ A confi

https://alstermedia.de/

video conference

Appendix 1 AV / Version 14.12.2020 [German]

□

alphaview

https://alfaview.com

Contract for order processing according to Art. 28 DS-

GMO, status: December 2020 [German]

(v) □

Cisco Webex

meetings

https://www.webex.com/

en

Cisco Master Data Protection Agreement, version 1.0

– Germany, December 1, 2020 [English]; Digital River

Ireland Ltd. Terms and Conditions and

Consumer information Germany from 24.7.2017

[German]

(d),

(e)

□2 Cisco Webex

meetings about

telecom

https://conferences.

telekom.de/products-

and-prices/telephone-and-

web/cisco-webexr/

Appendix AVV to the contract

Telecommunication services with the annexes for

Cisco Webex - conferencing and collaboration

Conferencing solutions, version 3.0 from 12/14/2020

[German]

□3 Cloud1X Meet https://www.cloud1x.de/

meet/

Contract for order processing for "Cloud1X Meet

powered by Jitsi" – "Cloud1X Meet" for short, version 9

from 15.12.2020 [German]

4

freely available

Jitsi offers

https://apps.google.com/

meet/

Google Workspace Terms of Service, Last modified:

December 21, 2020; Data Processing Amendment to

Google Workspace and/or Complimentary Product

Agreement, Version 2.3 [English]

(v) □

Google Meet

(as part of

Google

Workspace under

Validity of

Google

workspace

(On-line)

agreement and

of the data

processing

Amendment to

Google

2 See note.

3 Basically limited to EU/EEA, data exports with prior consent of the person responsible for all

thing possible.

4 Usually "red" because there is usually no order processing contract. Case-by-case assessment required.

Version 2.0 of February 18, 2021

EU

service

URL

version of the documents

Workspace and/or

Complementary

product

agreement)

5

Google Meet

(for free)

https://apps.google.com/

meet/

Google Terms of Service effective May 31.

March 2020, Google Privacy Policy, effective

February 4, 2021 [German]

(v)

GoToMeeting https://www.gotomeeting

.com/de-de

Data Processing Addendum, Revised: December 15,

2020 [English]

 mailbox.org

https://mailbox.org/video AV contract for mailbox.org customers according to Article 28

Paragraph 3 DS-GVO, version V.39 from 15.12.2020

[German]

6 meetzi

https://meetzi.de

meetzi – order processing (AV) contract

Art. 28 GDPR, Version 3 (14.12.2020) [German]

https://www.microsoft.

com/de-de/microsoft-

365/microsoft

teams/group chat

software

https://www.microsoft.

com/de-de/microsoft-

365/microsoft

teams/group chat

software

Appendix to the Privacy Policy for

Microsoft Online Services January 2020 [German] –

File versions (according to metadata) from 01/03/2020 and

9.6.2020 (version is not in the document itself

apparent); Microsoft Online Services Addendum

Privacy Policy, Last updated: July 21, 2020

[German]; Additional Safeguards Addendum to

Standard Contractual Clauses (Reference Copy

as announced November 2020) [English];

Microsoft Online Services Data Protection Addendum,

Last updated December 9, 2020 [English]

Microsoft Services Agreement effective October 1, 2020,

Microsoft Privacy Policy Last

Update: January 2021 [German]

(v) □

Microsoft

teams (under

Validity of

on-line services

Terms, about as

Part of Microsoft

365 or in the

free

version at

Registration in

a work or

organizational

vicinity)

7 □

Microsoft

teams

(free

version without

applicability

the online service

terms, so no

when registering in

a work or

organizational

vicinity)

 NETWAYS

Web Services

Jitsi

https://nws.netways.de/

en/apps/jitsi/

AVV v1.7 [German]

 OSC

BigBlueButton

https://www.open-

source-company.de/

bigbluebutton-hosting/

Personal data processing contract

Data in order, version 1.6 (as of December 16, 2020)

[German]

safe-

video conferencing

z.de

https://secure-

videokonferenz.de

Contract for order processing

personal data according to EU data protection

Basic regulation status 06/2020 [German]

5 No data processing agreement.

6 Basically limited to EU/EEA, data exports with prior consent of the person responsible for all

thing possible.

7 No data processing agreement.

Version 2.0 of February 18, 2021

EU

service

URL

version of the documents

8 □

Skype (without

applicability

the online service

terms)

https://www.skype.com/

en/

Microsoft Services Agreement effective October 1, 2020,

Microsoft Privacy Statement November 2020

[German]

9

Skype for

Business

On-line

(expiring, under

Validity of

on-line services

terms)

(v)

TeamViewer

meeting

(formerly

blizzard)

https://www.teamviewer.

com/en/meeting/

Appendix to the Privacy Policy for

Microsoft Online Services January 2020 [German] –

File versions (according to metadata) from 01/03/2020 and

9.6.2020 (version is not in the document itself

apparent); Microsoft Online Services Addendum

Privacy Policy, Last updated: July 21, 2020

[German]; Additional Safeguards Addendum to

Standard Contractual Clauses (Reference Copy

as announced November 2020) [English];

Microsoft Online Services Data Protection Addendum,

Last updated December 9, 2020 [English]

TeamViewer order processing contract (AVV),

Version status: January 1, 2021; TeamViewer

End User License Agreement (EULA),

Version status: January 1, 2021; TeamViewer product

Privacy Policy” (without version number, retrieval

February 4, 2021) [German]

□

TixeoCloud

https://www.tixeo.com

Order processing contract version 20200608

[German]

□ Plant21

BigBlueButton

https://www.werk21.de/

products/co_working/

bigbluebutton/index.html

Order processing contract according to Art. 28 Para. 3 DS-

GVO, Version 1.2.1., 06/2020 [German]

□10 Wire Pro

https://wire.com/de/

Data Processing Addendum June 2020 [German]

(v) □

zoom

https://zoom.us

Global Data Processing Addendum December 2020

[English]; Zoom Privacy Statement (latest change

August 2020) [English]

8 No Data Processing Agreement.

9 See Notes on Microsoft Teams (subject to the Online Service Terms, e.g. as part of Microsoft 365

or in the free version when registering in a work or organizational environment).

10 Also Switzerland. For Switzerland, there is an adequacy decision by the EU Commission on the data

protection level.

Part 2: Technical and organizational measures

This section contains the results of our compliance audit

on data security and data protection through technology design and data protection-friendly

Default settings according to Art. 25 and 32 DS-GVO with regard to the services reproduced

have not already proven to be inadmissible in the legal examination.

use case and assumptions

For the short test, we made a few basic assumptions. This

relate on the one hand to the basic procedure when using the services

and on the other hand on several typical use cases, which are determined by the need for protection

differ in processing.

Assumptions about the use cases

We have taken four typical use cases as a basis, in which a conference through

a person is organized who has another person or group of people as a further part

participating and authorized by an invitation to participate in the conference.

The participants expect from such a conference that the communication

content is only shared between the authorized persons and is not saved afterwards

and used for other purposes, unless there is storage and retrieval

processing a legal basis and the participants will be informed in advance. of

They expect to be able to control the sound and image of their input devices themselves

an activation, for example by moderators or third parties from afar, without the

Participation by the participants themselves is excluded.

With regard to the information technology used, it is assumed for the assessment that

the service entirely by the processor without linking to internal

Services of those responsible and in connection with the conferences

no other processors independent of the service are used

become men. In particular, no authentication service is used that is

Responsible or third parties not involved in the provision of the video conferencing service

provided.

In relation to the content of the conference, it is assumed that a legal basis for

their transmission with the various functionalities of the service, so that a

Prevention of these functionalities is not necessary.

Use case 1: Minor risks

In this use case, the participants accrue from participating in the

Conference (including its statements) only risks of minor severity. Especially

will not lead to unauthorized disclosure or alteration of data about this participation

more than minor consequences.

No recordings of sound or images from the conference will be made by the person responsible

performed so that no risks can arise from this. Unauthorized

drawings by conference participants who are not affected by technical measures

can be ruled out remain unconsidered.

In addition, no content is discussed at all in the conference that

represent personal data, or among the contents are at most incidentally personal

contain related data with little significance, their unauthorized disclosure

entails only minor risks for the persons concerned.

Use case 2: Normally vulnerable content, guest participation with minor risks

In this use case, a normal protection requirement for the content data is used for the assessment.

provided. This implies that normal, but not minor confidentiality

risk is assumed.

The participants authenticate themselves to the video conference service with a

or several individual characteristics (typically with username and password) or

use a link and an additional conference-specific password as guests.

In the latter case, the conference moderator ensures that persons who participate without authorization

11 The risk associated with conference participation

Unauthorized by the moderation until their exclusion is minor. A

subsequent access by unauthorized persons with the risk that conference content will be acknowledged

is technically prevented.

A recording of the video conference is not required consistently for all video conferences.

compels.

Use case 3: Normal risks

This use case differs from the previous one in that the risks are also different

extend to the framework data about the participants and the circumstances of the conference and

the risk associated with the participation of unauthorized persons in the conference until they are excluded by the

deration is more than minor.

The consequence of this is that the group of conference participants is determined in advance

the must and the participants with one or more personal characteristics

paint (typically with a username and password).

Use case 4: High risks

Use cases where there are serious adverse consequences for the data subjects

can occur, require an individual risk assessment, so we are here in this regard

cannot make a general assessment of the services.

However, in this application, in addition to carrying out a two-factor

identification of the participants, the implementation of an end-to-end encryption of the internal

holding data between the conference participants is required, which is designed in such a way that the

Service provider cannot take note of the conference content, at least not without it

to manipulate the software used by the participants.

We therefore indicate in the summary of the result whether a service has an end-to-

End encryption offers and what quality it may have.

Here we distinguish between a strong and a weak variant. The under-

difference is that in the strong variant, the participating end devices

mutually verifiable authentication and new volatile encryption for each conference

Development keys are generated, negotiated or

be distributed so that the provider cannot take note of the key material.12

The weak variant of end-to-end encryption, on the other hand, protects users from

The service provider's employees casually take note of the conference content if they

through the systems of the service provider. It does not protect against interference

11 More precise requirements for guest participation can be found in No. 4.2.4 of the "Visual conferencing systems orientation guide"

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

Those responsible should also take care not to reuse the conference-specific passwords in order to avoid

Reduce the risk of unauthorized participants.

12 See Chapter 4.1 of the “Guidelines for Videoconferencing Systems” of the Conference of Independent Data Protection

Federal and state supervisory authorities (DSK).

of the service provider in the data processing of the systems operated by him, based on a

Discharge of the conference content is directed. A correctly deployed strong end-to-end

Encryption also protects against such intrusion.

test criteria

The requirements for technical and organizational

Measures in Chapter 4 of the "Visual conferencing systems orientation guide"13 (OH VK) of

Conference of the independent federal and state data protection supervisory authorities

(DSK) used. Only those measures were reviewed that proved to be

evaluation and testing of the client program used on the user side.

The test criteria were:

test criterion

At least transport

state-of-the-art encryption.

The video conferencing service offers the possibility of participating in a conference

limited to persons who identify with individual characteristics

have reported.14

reference

on OH VK

4.1

4.2

For use cases 1 and 2 as an alternative to the previous criterion:

4.2.4

The video conferencing service offers a service determined by the person responsible

person in the role of moderator has the option not to participate in the

Recognize conference authorized persons and actively exclude them in such a way

that re-entry into the conference is not possible.

The video conferencing system allows you to set up roles for administrative

moderating, moderating, presenting and participating people. Other

Roll cuts are possible, as far as the responsibility for controlling the

implicitly carried out processing of personal data

remains pointed.

Participants can use their microphone and camera at any time

deactivate. Without the consent of the participant, their

Microphone and its camera are not activated.

The client software does not transmit any data to the service provider that the

Evaluation of the use of the service by the service provider or third parties

serve (tracking).

Before entering the conference, camera and microphone functions and the

Screen sharing disabled and only required by the participating

person to be activated.

(System-side) recordings can be prevented.

4.4

4.4

4.5

4.5

4.7

13 https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf.

14 Whether the authentication procedure corresponds to the state of the art (cf. Chapter 4.2.1 of the

deoconferencing systems), we could not check all providers. For reasons of equal treatment, this

Therefore, this aspect is not part of the assessment. We summarize our statements in this regard

Providers therefore only for information in the comments.

test criterion

All participating persons are identified by an explicit and by the partial

information to be confirmed by the person or by marking inside

half of the user interface noted that the video conference

is recorded in whole or in part.

reference

on OH VK

4.7

The following aspects were not checked:

 Measures for data protection through technology design, in particular for data

economy and memory limitation in the processing of frame-15 and in-

holding data by the provider, including the immediate automated deletion

Analysis of personal framework and content data by the provider

end of the video conference or the existence of a possibility for the responsible

chen to bring about such a deletion,

 Extent and correctness of the information provided by the providers about their processing of personal

Business-related framework data (e.g. from the setup of the conference or the internal

use of functions of the service),

 the existence of a possibility to include information according to Art. 13

or 14 GDPR in the client software,

 the exclusion of the disclosure of personal data from the service

delivery by the providers of the service to third parties who are not involved in the provision of the service

service are involved, such as B. the manufacturers of the software used by the service providers

is used

 the suitability of the authorization concept prepared by the provider [if the

Providers Participating persons who are not the organizers of the conference

belong, no individual authentication is possible, but the existence

densein a function to exclude unwanted participants

checked by an authorized person (organizer, moderator)],

 the presence of known vulnerabilities in the software libraries of the

Client programs and in the web applications used to provide the services

fertilize.

We have included the results of the investigations at the end of this paper in the notes

summarized for the individual providers to make it easier for those responsible

ers to select a service suitable for their purposes and, if necessary, to supplement

to take appropriate technical and organizational measures.

Adaptation to the application context

Before use, those responsible must understand the application context and the specific

consider use cases in order to carry out an appropriate risk assessment and the

to be able to determine planned corrective measures to manage the risks. in particular

It is also possible that additional measures will be taken due to the risks

fen, which are not supported by the provider without us

noted this as a defect. In the latter case, those responsible must

check whether they can compensate for the defect through their own measures or

have to choose their provider.

These risk-related measures may include, in particular, verifying identity

of the participants of the conference and the security of the connection, if

15 Framework data is metadata about the implementation of the communication. You can e.g. B. Information about

professional contacts, working hours or work performance.

the selected service only provides mechanisms for this that, in view of the protection

If the communication content is not sufficient.

Further useful information on data protection-compliant configuration and use of video

conference services are in particular the already cited orientation guide video conference

systems of the DSK as well as our publications "Berlin data protection officer for

Carrying out video conferences during the contact restrictions"16 and "Check-

list for conducting video conferences during the contact restrictions”17

remove.

Evaluation scheme part 2 (technical test)

For the technical evaluation of the services we used the following evaluation scheme.

overall grade

There are serious deficiencies that prevent legally compliant use of the service

tes within the scope of the tested use case.

There are defects which, within the scope of the respective application, lead to a

compliance with the data protection requirements according to Art. 25 or 32 DS-GVO

being able to lead. The probability of occurrence of the use of the service

associated risks depends on the implementation of additional measures by the

those responsible, the severity of these risks depends on the respective use case.

If the residual risk is not within reasonable limits, the service

are not used in accordance with the law.

As part of our investigation in accordance with the test criteria presented, we

no indications of defects relevant to the respective application

found.

A service is defective if the person responsible is informed by using the

configuration options offered by the provider is not possible, a legally

to ensure proper data processing.

Types of defects found

Within the framework of the technical test criteria listed above, we were able to

services examined found only three deficiencies that prevent a positive assessment.

We have marked them with the letters (a), (r) and (k).

(a)

(r)

(k)

(Registration) The service does not allow participants to oblige themselves

with individual characteristics (typically username and password).

(No. 4.2 of the Video Conferencing Systems Orientation Guide, see explanation above under

test criteria).

(role concept) The service does not allow implementation of a role concept

No. 4.4 of the Video Conferencing Systems Orientation Guide (see explanation above under

test criteria).

(camera) With the service in question, it is not possible for the participants to

join a conference with the camera and microphone disabled

16 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientation aids/2020-BlnBDI-Empfehlungen_Vide-

okonferenzsystems.pdf.

17 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientation aids/2020-BlnBDI-Checkliste_Video-

conferences.pdf.

(No. 4.5 of the Video Conferencing Systems Orientation Guide, see explanation above and

ter test criteria).

When using the service in question, the circumstance designated by (k) is regularly

25 DS-GVO - this depends on the

circumstances of the individual case. For example, in video conferences between two people

25 DS-GVO cannot be assumed here as a rule.

A detailed description of the defects found can be found in the notes to

the individual providers at the end of this paper.

For an appropriate classification of the results, we would like to point out that by

insufficient technical and organizational measures in the backend of the services and

Vulnerabilities in the client software can still cause far more serious defects than

were detectable by our tests.

End-to-end encryption - column E2E

+

The services are marked with the plus symbol, one of which is explained above

offer weak end-to-end encryption.

++

Strong end-to-end encryption is marked with two plus symbols.

Evaluation part 2

We have the tested video conferencing services for clarity from a technical point of view

summarized as follows (for the legal assessment, see assessment part 1).

Use case 4 requires an individual assessment and cannot be represented as a traffic light.

use case18

AF1

AF 2

AF 3

E2E service

URL

(a)

+

A confi

https://alstermedia.de/videokonferenz

(a)

(a)

(a)

(a)

alphaview

https://alfaview.com

Cloud1X Meet

https://www.cloud1x.de/meet/

mailbox.org

https://mailbox.org/video

meetzi

https://meetzi.de

NETWAYS Web

Services Jitsi

https://nws.netways.de/de/apps/jitsi/

18 The use cases (AF) are numbered here as at the beginning of the chapter.

use case18

AF1

AF 2

AF 3

E2E service

URL

(r)

(a)

(r)

OSC BigBlueButton

https://www.open-source-company.de/

bigbluebutton-hosting/

safe-

videokonferenz.de

https://sichere-videokonferenz.de

(k)19

(k)

(k)

+

TixeoCloud

https://www.tixeo.com

work21

BigBlueButton

https://www.werk21.de/produkte/co_working/

bigbluebutton/index.html

++ Wire Pro

https://wire.com/de/

Only for the Wire Pro service in use case 3 with regard to the above

test criteria already in the standard configuration did not lead to any indications of defects and

no circumstances found requiring adjustment of the configuration or additional measures

make necessary.

19 providers have announced a new version 16.5 of the software for mid-February 2021, which will eliminate the defects

meant to be.

Part 3: Notes on the individual providers

Please note that beyond the issues addressed here, there are other

problems that we have not checked or are not aware of and the use of the

Services may then still be inadmissible despite the correction of the problems mentioned here

can.

In italics we have given the notes a concise summary of what has been found

legal deficiencies.

General notes on Jitsi Meet

Jitsi Meet is free and open source software. We have the example

Offers from some service providers who operate the software for those responsible

purport. The service providers have partially adapted the software. At the

A number of other operators of this software are active on the market. By naming the provider

no statement is connected to the effect that their service is that of others in the competition

advertising companies is preferable.

However, the provision of a Jitsi system also regularly leads to the adoption of

technical restrictions that affect data protection-compliant use

and have it systematically found again with the relevant providers. Some of these

Depending on how the system is used, restrictions can mean that

not all data protection requirements are met. To correct this,

Adjustments to the source code of the software may be necessary. A takeover in the public

Any community code base available would also allow other entities using the software

use, allow to benefit from the adjustments.

In particular, the role concept and the available methods are restricted

access control methods.

Except for use cases with minor risks, those responsible should be careful

ensure that the service you use offers a moderation role, which can only be

report with personal characteristics (typically with user name and passport

word) can be accepted. Many Jitsi instances assign the moderation role to the

first person to enter a conference room. This is for use cases with more than

not suitable for minor risks.

The services known to us that use Jitsi Meet do not allow participation in a

of a conference to people who deal with personal characteristics

(typically with a username and password). Depending on the

further measures taken by the person responsible and the risks in the specific case

In this case, this can lead to the impermissibility of the use.

The providers of jitsi-based services do not provide their own mobile applications

(Apps) ready to use their services. Instead, all such services can be

shared apps can be used. We warn against using the apps

from the Google Play Store and the Apple App Store, the respective software from tracking

Providers like Crashlytics and Firebase included. The variant of the Jitsi app from the F-

Droid-Store20, on the other hand, is free of such components. Those responsible must be in the

invitation to a conference to point out the deficits of the apps mentioned and to

recommend accessing the service via the F-Droid app or a web browser, where applicable

information is not yet known to the invitees.

As with any service where it is sufficient to attend a conference

renzlink and enter the conference password, those responsible must

special attention to the confidentiality of the transfer of the link to the conference and the

20 https://f-droid.org.

Set conference password. A security gain can be achieved by password

and invitation link to the participants on different communication channels

to be shared.

General notes on BigBlueButton

BigBlueButton is also free and open source software. We have at-

playfully considered the offers of some service providers who operate the software for

have responsible content. The service providers have partially installed the software

fits. A number of other operators of this software are active on the market. With the nomination

the provider is not linked to any statement that their service is the other

is preferable to competing companies.

The provision of a BigBlueButton system also regularly leads to the acquisition of

technical restrictions that affect data protection-compliant use

and can be systematically found with the relevant providers. Some of these

Depending on how the system is used, limitations may result in

not all data protection requirements are met. To correct this,

Adjustments to the source code of the software may be necessary. A takeover in the public

Any community code base available would also allow other entities using the software

use, allow to benefit from the adjustments.

One such technical limitation is the implementation of the recording function

for video conferencing. At the time of testing, the official version of the software provided that

always made a recording of the entire conference and this recording into one

trimmed later using crop marks. This can

lawfulness of the processing and in any case contradicts the principle of

Data minimization and regularly the expectations of the users. a sub

The service sought has therefore modified this function in such a way that, according to its own statement

now only saves recordings for those periods of time for which this is explicitly

was requested.

A-Confi – Jitsi

In the default configuration, conferences from this provider are not password-protected.

protects. Those responsible should therefore before the start date and before other participants

enter the conference, open the conference and set a password.

In order to permanently exclude a participant from the conference, it is the moderator

possible to set a new password and the function "eject" on the

person to apply.

In the course of the authentication of persons who take on the moderation role,

according to the state of the art, the transmission of your password to the provider

the.

A-Confi offers a weak variant of end-to-end encryption. That's what it's all about

is an experimental feature of Jitsi.

alphaview

The use of an app is required for the alfaview offer, but this can be used without administration

rights can be installed. The desktop app is available for Windows, macOS and Linux

available from the alfaview website and may not be downloaded from any other source.

the. It must also be considered whether an installation of software in the intended

ten environment is possible.

We did not find any shortcomings in the transport encryption. An end-to-end

alfaview does not offer encryption.

Version 2.0 of February 18, 2021

Cisco Webex Meetings

When ordering online, an order processing contract must be concluded separately.

Processing without instructions also permitted under third-country law. No sufficient-

the supplementary measures for data exports.

Cisco Webex Meetings can not only be held directly from Cisco or via Cisco partners (with

contract processing contract), but also online. By default, at

No order processing contract was concluded after the online booking, so this can be done later

must become.

Although the provider has made considerable efforts, the main processing

personal data in connection with the use of Cisco Webex Meetings

to increasingly relocate to the EU and to design the order processing contract free of defects

ten. An assessment of the order processing contract as free of defects is based on the legal

chen level, however, that the contract contrary to instructions processing

personal data not only from the law of the European Union or the

member states allows. Ultimately, there remains the problem of access rights for foreign authorities

hear that the provider cannot solve due to legal requirements: the

3.c.i, ii of the "Cisco Master Data Protection Agreement", Version 1.0 - Germany,

December 1st, 2020, does not meet the requirements of Art. 28 (3) lit

Processing outside of the instructions, also in the case of obligations on the part of the provider

from law other than that of the European Union or the Member States, that of the

bidder subject, allowed. Likewise, the obligation to provide information about

Processing does not meet the requirements of Article 28 (3) (a) GDPR. The standard

Standard contract clauses are not sufficient in themselves to transfer personal data

to the USA to justify, since there are no sufficient supplementary measures,

to prevent unauthorized access by US authorities under European law. for an-

Third countries without an adequacy decision by the EU Commission is not an evaluation

possible. Illegal data exports can only be partially avoided. Cisco has on-

announced that they would start up new data centers in the EU in mid-2021 and in any case

fix the lack of prohibited data exports as part of the telemetry functions.

As part of our cursory examination, we also had to determine that standard

Any number of other subcontractors who are not permitted in the contract may be involved. This should

according to Cisco, however, can be deactivated.

Due to the legal deficiencies, no technical assessment was carried out.

Cisco Webex Meetings via Telekom

In the "Appendix AVV to the contract for telecommunications services" with the annexes for Cisco

Webex - Conferencing and Collaboration Conference Solutions (Version 3.0 from December 14th, 2020).

we have not found any defects. However, according to the contract, certain, very

limited sets of personal data transferred to the United States for billing purposes,

Namely first name, surname and e-mail address of the host of the video

conference and technical information about the video conference (URL, start and end time of the video

deoconference). In the case of 24/7 support, personal data may also be included in the

be transmitted to the USA.

There is no legal basis for such transfers of personal data to the USA.

basis. However, it is possible to specify other than real data as "hosts", specifically

a kind of group account, via which the video

conferences are organized. If this excludes a personal reference, there is no

Transfer of personal data to the USA, a legal basis for this is therefore

not mandatory. It should be noted that use of the central access data by different

different people (instead of a central body) is only considered if within the framework

of administrative access no access to personal framework or content data

other video conferences is possible.

Should it be possible to negotiate standard contractual clauses with the sub-processor Cisco

close, it would also be conceivable to use undetectable personal pseudonyms to name the
to use host. In this case, however, it should be noted that the pseudonyms also
not by other information that may be subject to access by US authorities
may be discoverable. If the invitation links are sent by the hosts via e-
Mail sent to participants who use US service providers, this solution does not apply
tracht because US authorities put the information together and uncover the pseudonym
could. A solution with pseudonyms therefore appears essentially only for the internal one
Communication can be realized in larger organizations. In individual cases, the unit
obtaining effective consent. On the high demands of an effective
We expressly point out consent, especially in the context of employment or school.
In particular, the data subjects must be able to choose freely between consent and
refusal to have consent, i.e. they are allowed to do so in the event of refusal of consent
no disadvantages arise. In addition, the special requirements from Art. 49
Paragraph 1 lit. a GDPR must be observed.
24/7 support may involve data exports to unsafe third countries. Should this
are used, a justification for this must therefore be found, which is extremely time-consuming
and in some constellations may be impossible (see the “Recommendations
01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of
protection of personal data" of the European Data Protection Board, available at
https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-
best practices_en). In special exceptional cases, consent may also be conceivable,
whereby the additional requirements of Article 49 (1) (a) GDPR must be observed.
With regard to 24/7 support, however, it can be agreed with Telekom that personal
Customer-related data is only transferred to the USA with the express consent of the customer
be transmitted. In this case, customers can give their consent in advance
of the persons concerned - the high requirements described above

effective consent must also be observed here - or, if this is not (effectively) possible

refrain from pursuing the case with 24/7 support.

However, as part of our technical examination, we had to establish that unlawful

Frequent data exports took place that are not covered by the contract. The are immediately apparent

Data exports associated with the embedded in the various client programs

Telemetry function, with which data is exported to the USA, the information about the

Use of the service by the conference participants included. This function can be

according to Cisco also not deactivated by responsible persons. Cisco has a

Correction of this deficiency announced for mid-2021.

Further data exports to the USA and other third countries and inclusion in the contract

non-designated sub-processors that we identified as part of our cursory examination

had determined and / or are provided for in the contract, according to information from

Cisco and Telekom through appropriate configuration and additional instructions from the

prevent those responsible, or they can be prevented by technical, organizational and

possibly also avoid or through legal measures by those responsible

legalize. Since Cisco and Telekom provide us with a data protection-compliant configuration in the

could not provide the time frame of our audit, we provide the evaluation of this

regarding back.

Due to the legal deficiencies, no technical assessment was carried out.

Cloud1X Meet – powered by Jitsi

In the standard configuration, the conferences are not protected by a password. responsible

verbatim should therefore be given before the start date and before other participants leave the conference

enter, open the conference and set a password.

To permanently exclude a participant from the conference, it is

possible to set a new password and the function "eject"

apply to the person.

We did not find any shortcomings in the transport encryption. In the course of authentication

mation of persons who take on the moderation role will be carried out according to the status of the

Technology avoids the transmission of the password to the provider.

Google Meet (as part of Google Workspace under the terms of Google Workspace

(Online) Agreement and the Data Processing Amendment to Google Workspace and/or

Complimentary Product Agreement)

Deficiencies in the order processing contract. Impermissible restrictions of the

to the right. Prohibited data exports.

Section 6.1 of the "Data Processing Amendment to Google Workspace and/or Complimentary Pro-

duct Agreement, Version 2.3" (hereinafter: "DPA") restricts the right to issue instructions with regard to the

Data deletion and the obligation to notify contrary to Art. 28 Para. 3 lit. a DS-GVO,

by allowing Google a deletion period of 180 days and also the obligation to delete

permissible also due to member state law, which Google is not subject to.

lies. The obligation to delete after the order has been completed in accordance with Article 28 (3) lit. g GDPR is carried out by

Section 6.2 of the DPA is inadmissibly restricted in that Google has also set a deletion period of

granted 180 days.

Contrary to Art. 28 (3) lit. h GDPR, the DPA does not contain a comprehensive obligation for

Google, the person responsible with all necessary information to prove compliance

fulfillment of the obligations laid down in Art. 28 DS-GVO. Clause 7.5.1,

7.5.3.a and 7.5.3.b DPAs only review a limited right of inspection of certain

Reports commissioned by Google.

Section 7.5.3.c DPA provides for a fee obligation for any type of inspection by responsible

literal before. In any case, because no exceptions are required for breaches of contract

necessary checks are made, this will initially result in civil

che regulation largely devalues the right to review, so that Art. 28 Para. 3 lit. h DS-
GMO is violated.
The Procedure for Information on Current Subprocessors in Section 11.1 DPA
does not ensure that those responsible can prove (Art. 5 Para. 2 in conjunction with Art. 5 Para. 1 lit. a
DS-GVO) which sub-processors were approved with the conclusion of the contract.
Google's "affiliates" are generally allowed as sub-processors, whereby the term dy-
is defined namingly. Changes in company law can thus lead to the inclusion
hung other sub-processors, without the controller objecting to this
You have the right to object, as is mandatory under Art. 28 Para. 2 Sentence 1 GDPR.
Section 11.3.a.ii DPA does not ensure that - as required by Art. 28 Para. 4 Sentence 1 DS-GVO -
additional processors will be subject to the same data protection obligations as set out in the DPA
are set, but limits this to obligations in Art. 28 Para. 3 DS-GVO
are described.
The description of the information about new sub-processors in Section 11.4 DPA is
at least unclear in connection with Section 11.2 DPA, because they are also interpreted as such
can that the information is not proactive, but only through a website what after
Art. 28 para. 2 sentence 2 DS-GVO is not sufficient. In addition, those responsible cannot
Accountability (Article 5 (2) in conjunction with Article 5 (1) (a) GDPR).
Section 11.4(b) of the DPA grants the controller the only option to object to
the inclusion of new sub-processors the right to terminate the contract.
In practice, however, this right is massively restricted by Section 8.7 of the “Google
Workspace Terms of Service, Last modified: December 21, 2020" (hereinafter: "ToS") in the case
of termination provide that no reimbursement of fees will be made. This applies
also strongly for terminations based on the DPA.

Section 13 DPA impermissibly restricts the obligations arising from the standard contractual clauses, so that these cannot be used to justify the data export.

Specifically, liability is limited from Section 6.2 of the standard contractual clauses because under the concept of affiliates in Section 13.1 DPA can also apply to a natural person who is not itself is a contractual partner or responsible party. In addition, Clause 13.2 also refers to this Section 13 ToS, which in Sections 12.1 and 12.2 excludes any liability in connection with the use contract, and not limited to the parties. The severability

Clause 12.3 ToS includes - regardless of the question of whether severability clauses for Exclusions of liability are permissible at all - only those matters for which a Limitation of liability or exclusion of liability are excluded by law. the port 6.2 of the standard contractual clauses constitutes a contractual transfer of liability acceptance that goes beyond the statutory liability.

Clause 1.5(d) ToS allows Google to make unilateral changes to the DPA purely through publication information can be found on the relevant website. At least that's what makes it responsible impossible to meet their accountability (Art. 5 Para. 2 in conjunction with Art. 5 Para. 1 lit. a) men.

Note (not necessarily a defect): It must be checked in each individual case whether the Finally, technical and organizational measures defined the requirements of the Art. 32 GDPR are sufficient. In addition, the DPA contains clauses that require an evaluation.

Due to the legal deficiencies, no technical examination was carried out.

GoToMeeting

Deficiencies in the order processing contract. Impermissibly restricted scope. U.N-permitted data exports.

Clause 5.1 of the "Data Processing Addendum, Revised: December 15, 2020" looks forward Art. 28 para. 4 sentence 1 DS-GVO inspections at subcontractors and contractual

Agreements with these only exist if they are not group companies of

LogMeIn trades. In addition, contrary to Art. 28 Para. 4 Sentence 1 DS-GVO, the contractual

Data protection obligations only "essentially" also imposed on the subcontractors

be laid.

The procedure for information about current sub-processors in Section 5.2 of the

"Data processing addendum" does not ensure that controllers demonstrate (Art. 5

Paragraph 2 i. V. m. Art. 5 Para. 1 lit. a DS-GVO), which sub-processors with processing

were approved by the end of the contract. The procedure for informing about new subcontracting

5.2 requires active action by those responsible and is not sufficient

Art. 28 para. 2 sentence 2 GDPR. Those responsible who do not actively send the notifications themselves

subscribe, also cannot be accountable (Art. 5 Para. 2 in conjunction with Art. 5

Paragraph 1 lit. a GDPR).

Section 6.2 of the "Data processing addendum" does not meet the requirements of Art. 28

Para. 3 lit. h DS-GVO to proof obligations and control rights.

Section 10 of the "Data Processing Addendum" limits the applicability of certain

mandatory regulations mentioned in this section to an excerpt of the

Processing of personal data that is subject to the GDPR; Art. 3 GDPR is

much further.

Clause 10.3 i. V. m. Appendix 1 of the "Data Processing Addendum" provides for restrictions on the

Standard contractual clauses, which due to a priority regulation for the standard

12 should not apply under civil law, but nevertheless lead to an inadmissible

gene modification, so that these cannot justify the data export. the

Privacy Shield self-certification does not apply to HR data.

Due to the legal deficiencies, no technical examination was carried out.

Version 2.0 of February 18, 2021

mailbox.org – Jitsi

When setting up a new conference, two passwords (participation

password and moderation password), but each with its own password

a minimum length and complexity can be replaced.

In order to permanently exclude a participant from the conference, it is the moderator

possible to set a new password and the function "eject" on the

person to apply.

We did not find any shortcomings in the transport encryption. The authentication

procedure does not correspond to the state of the art and transmits the password within the

TLS session to the service.

meetzi—Jitsi

The offer meets the test criteria we apply. The authentication procedure

does not correspond to the state of the art and transmits the password within the TLS session

to the service.

Microsoft Teams (as part of Microsoft 365 under the validity of the Online Service Terms)

In principle, according to the regulations in the "Appendix to the data protection regulations

for Microsoft Online Services” (hereinafter: “DPA”), the version of the DPA that was valid when you

termination or renewal of online service subscription. Responsible, the

who have already subscribed to the service must therefore check which DPA version applies to them

is time.

Nevertheless, Microsoft has the DPA "German, January 2020" retrospectively without labeling

extensively changed. There is a document that, according to the metadata, is dated 01/03/2020

was created and a document that, according to the metadata, was created on June 9th, 2020

became. The designation of the documents is the same as that published by Microsoft on the Internet

light document was tacitly replaced. In the change history ("clarification

Gen and Summary of Changes") specifically states "None", although large

Parts of the contract have been changed. Microsoft points out in this respect that it is

the document is a translation of the English document, which itself is not

has been changed. Only corrections were made. the latter is

not correct, but not only adjustments were made to the English version

solution of the DPA, but partly new, originally non-existent deviations from the

German version from the English version.

We point out that we are given the subsequent and undocumented

Amendment of the published order processing contract by Microsoft during audits

also intend to comply with the form of the order processing contract

according to Art. 28 Para. 9 DS-GVO and the corresponding verifiability (Art. 5 Para. 2 DS-

GMO) to check.

Microsoft is of the opinion that the various versions of the DPA meet the

ben of the applicable data protection law, in particular Art. 28 DS-GVO.

We cannot take this view for the reasons detailed below

follow.

Due to the legal deficiencies, no technical examination was carried out.

a) DPA January 2020 (in the versions of January 3, 2020 and June 9, 2020)

Provider reserves the right to process order data for its own purposes. defects

in the order processing contract. Many ambiguities and contradictions in the order processing

employment contract. Prohibited data exports. Provider has published order processing

extensively subsequently changed without marking; version (according to meta

data) from January 3, 2020 contains impermissible restrictions on the right to issue instructions.

Most of the implied changes between the DPA January 2020 release

from January 3rd, 2020 - and the DPA January 2020 - version from June 9th, 2020 - are purely linguistic

of a kind. In particular, in the version of June 9th, 2020, the standard contractual
clauses that originally contained very extensive deviations from the wording of the approved
ten Standard Contractual Clauses, substantially aligned with the approved text.
However, there are also relevant substantive changes. Most changes are po-
to assess positively. Nevertheless, one of the most important fundamental problems of the treaty remains that
it is unclear and contradictory in many places.
Microsoft reserves the right in the DPA January 2020 under the item "Privacy Policy -
type of data processing; Ownership" the processing actually on behalf
processed personal data for their own purposes. A legal basis
for the associated disclosure of personal data by the person responsible
chen to Microsoft is not apparent. From the processing of the order data also to
Microsoft's purposes are followed by the problem of joint responsibility
according to Art. 26 GDPR. According to the case law of the ECJ, such a
if not ruled out based on the only rudimentary information in the DPA January 2020.
This is at least with regard to accountability (Art. 5 Para. 2 in conjunction with Art. 5
Paragraph 1 lit. a GDPR) is a problem. In the case of the actual existence, it is added that
no agreement according to Art. 26 DS-GVO exists.
The DPA January 2020 contains regulations in many places that exceed the legal minimum
contradict requirements. While there is in the “Privacy Policy –
processing of personal data; GDPR” one whose meaning is unclear
Reference to Annex 3 to the DPA January 2020, which in turn contains material content from the
Art. 28, 32 and 33 DS-GVO, but Annex 3 also leaves it unclear whether these
Rules now binding for Microsoft to the actual - clearly illegal - text of the
DPA January 2020 should proceed or not. The file version from 06/09/2020 deteriorated
even amends this clause in that it is now separated from "[the] personal data of the
GDPR” speaks. Such an unclear order processing contract makes it the responsible

literally impossible to account for according to Art. 5 Para. 2 i. in conjunction with Art. 5 Para. 1 lit. a GDPR.

But Annex 3 to the DPA January 2020 (in the file version of January 3, 2020) does not fully accept the relevant wording of Art. 28 GDPR. In any case, Section 2 lit. g of Annex 3 (in the file version of January 3rd, 2020) falls short of the legal minimum requirements of Article 28 (3) lit. g GDPR by deleting or returning Submission of the order data after the end of the order only at the request of the customer provided and not in every case. Item 2 lit. a of Appendix 3 (in the file version dated 3.1.2020) also impermissibly restricts the customer's right to issue instructions against Art. 28 (3) lit. a GDPR, because exceptions are not only due to the Union law or Member State law to which Microsoft is subject. In In the file version dated June 9th, 2020, these deficiencies have been tacitly corrected, as well as the wording of the annex further approximated the wording of the law became. However, the wording of the law from the version dated 01/03/2020 in the version of 06/09/2020 replaced by own terms. In addition, one new deviation from the minimum requirements of Article 28 (3) lit. adds by the obligation to notify the customer if Microsoft is obliged to data processing contrary to instructions, not only because of the work obligation relevant law, but on the basis of any law (wording "the legislation") is excluded. A further deviation at the expense of the customer or of the customer in the new version of June 9, 2020 of Item 7 of Annex 3 is that Microsoft the information required for reporting a so-called data breach only then must make available to customers if (instead of so far, i.e. now only even if the condition is met for all information and no longer as before partially if the condition for parts of the information is met) that information available to Microsoft in its reasonable discretion (rather than the objective formulation

"in an appropriate manner" is now limited to a judicially reviewable one

discouraging Microsoft's equity decision).

In the DPA January 2020 under the item "Data security - verification of compliance"

restrictions of the standard contractual clauses. These are called “Addition to

clause 5, paragraph f, and clause 12, paragraph 2 of the Standard Contractual Clauses” means and

it is claimed that the Standard Contractual Clauses are not modified thereby. That is

there is a general statement in the introduction to the January 2020 DPA that the standard

standard contractual clauses take precedence over the DPA January 2020, as do the standard contractual clauses

sels themselves contain a corresponding priority regulation with their prohibition on amendment.

It is already questionable - and problematic with regard to Art. 5 Para. 2 DS-GVO - whether the

common priority clause in the introduction of the DPA January 2020 is applicable at all,

if the specific limitation in question of the standard contractual clauses themselves

claims not to constitute a limitation, so that on this assumption the

Priority clause logically cannot be applied. However, this can often

stay away because any restriction of the rights and obligations from the standard contractual

clauses, regardless of their wording and even if they apply elsewhere

is declared subordinate and therefore not applicable, to an inadmissible modification of

standard contractual clauses. Because this is intended and the result is regular

also achieved that the standard contractual clauses are not fully applied

be able. Accordingly, recital 109 GDPR also emphasizes that other

contract clauses neither directly nor indirectly contradict the standard data

protective clauses may stand. Thus, the present restriction "additional"

Clause, despite its presumed invalidity under civil law, leads to an inadmissible

Conversion of the standard contractual clauses so that they do not justify the data export

be able. Microsoft has in addition a self-certification according to the Privacy

Shield, but the relevant adequacy decision of the EU Commission

sion was approved by the ECJ in a judgment dated July 16, 2020 (Case C-311/18 – “Schrems II”) for our

declared valid. Microsoft reserves the right to process the order data at any location

where Microsoft or its sub-processors operate (DPA January 2020,

Section "Privacy Policy - Data Transfers and Storage Location - Data

transmissions"), i.e. also in the USA. In addition, it is not evident that sufficient additional

additional measures would have been taken to, in accordance with the case law of

ECJ in the "Schrems II" judgment to compensate for the insufficient level of data protection in the USA

chen.

We recommend reviewing the January 2020 DPA with the Notes as well

to the DPA July 2020, which may contain references to

tail running problems.

b) DPA July 2020, Additional Safeguards Addendum to Standard Contractual Clauses No-

November 2020, DPA December 2020

Subject to overriding special regulations in the “rights of use”: Unclear

Scope of order processing. Provider reserves the right to process order data

for own purposes. Deficiencies in the order processing contract. Lots of ambiguity and

Contradictions in the order processing contract. Prohibited data exports. unacceptable

Restrictions on the right to issue instructions.

Also, the DPA "Last Updated: July 21, 2020" (referred to herein as "July 2020 DPA")

makes extensive language changes compared to the previous versions, but also

some relevant content changes. One of the most important basic problems of the treaty,

However, the fact that it is unclear and contradictory in many places remains in this one as well

version exist.

The regulations of the July 2020 DPA are subject to special regulations

may be included in “rights to use” that take precedence over the DPA. We could help

Our research does not identify any such overriding special regulations, but it is

cannot be ruled out that such overriding special regulations exist. Microsoft has

unfortunately did not respond to our request in this regard, so that those responsible

have to check it yourself comprehensively.

At the end of November 2020, Microsoft released "Additional Safeguards Addendum to Standard Con-

contractual Clauses” announced. We have addressed their content at a relevant point.

The "Microsoft Online Services Data Protection Addendum, Last updated December 9,

2020” (referred to herein as “DPA December 2020”) essentially only assumes the

succeeded in the "Additional Safeguards Addendum to Standard Contractual Clauses" in the

DPA. So far it is only available in English. As far as the translation into German

only those changes are made that are also in the English language version

ment have been made, DPA July 2020 and DPA December 2020 are therefore - as far as relevant here

vant – to be evaluated immediately.

Since the DPA July 2020 has a very complicated structure and is reflected in various places

contains contradictory regulations, the description of the defects and hindrances found

in the following essentially based on the wording of the law.

scope of application

It remains unclear to what extent exactly after the DPA July 2020 an order processing

should be available and to what extent Microsoft should act as the responsible party.

The introduction to the section "Privacy Policy - Processing of personal

ner data; GDPR" provides for the applicability of the section and Annex 3 (objectively)

depends on whether "Microsoft is a processor or sub-processor of personal

personal data within the meaning of the GDPR”. In the following paragraph, however, "agreed

ren" Microsoft and the customers, under which conditions Microsoft (company

ter-) processor is - it should be noted that this question is not the dis-

position authority of the parties is subject, but from the facts and the legal

chen definitions in Art. 4 No. 7 and 8 DS-GVO follows. The rule follows that (only

then,) "when Microsoft is acting as a processor or sub-processor,"

Microsoft acts in accordance with instructions, which is precisely the essential element of

tracing processing represents. In this respect, it follows indirectly that the contractual regulation in

DPA, according to which Microsoft defines itself as a processor, due to the

Definition as processor subject to contractually limited instructions

results in Microsoft acting as a processor within the scope of the contractual definition

is actually a processor within the meaning of the law. In any case, this applies

while ignoring further restrictions of the instruction binding in the DPA. It turns out

In this respect, however, the dogmatic problem arises that according to the regulation in the introductory

to the section “Privacy Policy – Processing of Personal Data”

th GDPR” the regulations governing the applicability or non-applicability of the

Rules for role determination decide, depending on the result of the role determination

gene.

The problem that is more relevant in practice arises from the fact that the regulations for determining roles

as a (non-) processor in the section "Privacy Policy - Processing

processing of personal data; GDPR – Processor and Controller – Role

rights and responsibilities” to the “specific conditions of the respective online

service or in this DPA”, which may state otherwise. in the

In the case of the July 2020 DPA, this clearly affects the processing of personal data

“to legitimate business activities of Microsoft” for which Microsoft has no

subject to bondage. To what extent other data processing on behalf of those responsible

or under Microsoft's own responsibility remains unclear. The section "Da-

privacy policy – type of data processing; Ownership” adds

nothing, because the service provision and the processing to "legitimate business

abilities of Microsoft” are allowed on the same level. The section "Privacy

provisions - processing to provide the online services for the customer"

Version 2.0 of February 18, 2021

- 24 –

only defines what is meant by "provision" of an online service and decides

agreed processing purposes, which are usually carried out under the responsibility of Microsoft

genes, “unless such use or processing takes place after

the customer's documented instructions”. It follows from this that this clause

sel both processing under Microsoft's own responsibility and on behalf of Microsoft

of the customer includes. The (insufficient, see below) specification

the purpose of the processing in the section "Privacy Policy - Processing personal

personal data; GDPR – Processing Details” helps with its reference to “the

Provision of the Online Service pursuant to Customer's volume licensing agreement and for the

Microsoft's legitimate business activities in connection with the provision of the online

services for the customer” no further because they obviously contradict the other

General regulations of the DPA July 2020, according to which at least the processing for the "legitimate

times business activities of Microsoft" do not constitute order processing

should, and because this definition also refers back to the section just discussed here "Da-

privacy policy – type of data processing; Ownership Structure”, of the DPA

July 2020 references. The delimitation and thus the existence of order processing

therefore remains open.

The July 2020 DPA applies materially as described in the “Privacy Terms – Scope” section.

parts not for "previews", even if the processing of personal data

in "Previews" is not excluded.

More detailed description of the processing, Article 28 (3) subparagraph 1 sentence 1 GDPR

The subject, duration, type and purpose of the processing are set out in the section "Privacy Policy".

moods – processing of personal data; GDPR – processing details",

if necessary i. V. m. the regulation in the section "Data protection regulations - type of data processing

processing; Ownership" of the DPA July 2020 insufficiently regulated. The "Plant 3

– Provisions on the General Data Protection Regulation of the European Union" refers to

Clause 2 to the "License Agreement of the Customer". Those responsible must therefore check for themselves whether

in the contract you have concluded, the subject, duration, nature and purpose of the processing

are sufficiently clearly defined.

The same applies to the type of personal data processed and the category

categories of data subjects, with additional reference to the list of processing

activities is referred to without it being apparent that this itself is also used for

content would. Annex 1 to the standard contractual clauses also does not contain any

closing lists, especially since the categories of data subjects mentioned as possible in

Regarding video conferencing services are incomplete and the nature of the data only relates to

"transferred" personal data limited.

Obligation to follow instructions and obligation to report processing without instructions, Art. 28

Paragraph 3 subparagraph 1 sentence 2 lit. a GDPR

Although "Annex 3 - Provisions on the General Data Protection Regulation of the Euro-

European Union" under item 2.(a) a regulation that in itself meets the requirements

of Article 28 (3) subparagraph 1 sentence 2 lit. a GDPR is sufficient, but this regulation is used by many

Positions of the DPA July 2020 restricted again without it being apparent that the all

common clause in Annex 3 to the detailed regulations elsewhere in the July DPA

would proceed in 2020. The introduction to the section "Privacy Policy - Process

processing of personal data; GDPR" of the DPA July 2020 may

– which in itself is a problem in terms of accountability

according to Art. 5 Para. 2 DS-GVO - to be understood in such a way that this section
other sections of the DPA. However, this does not apply to Appendix 3 in
relationship to the provisions of the section "Data protection regulations - processing of personal
personal data; DSGVO", which expressly apply "in addition", i.e. with equal priority, should
len. The regulations in the subsection "Data protection regulations - processing of personal
personal data; GDPR – processor and controller – roles and

Responsibilities" contain, on the one hand, restrictions on the right to issue instructions,
which the "Volume Licensing Agreement (including the DPA Terms and all applicable
available updates) along with the product documentation and usage
and configuration of the features of the online services by customers
complete and documented instructions from customers
Microsoft in relation to the processing of personal data" and moreover
Gen refers to the procedure for changing the volume licensing agreement. Another-
on the other hand, the subsection for exceptions to the distribution of roles as contract
workers and thus the obligation to issue instructions to the specific provisions of the respective
Gen online service and the DPA July 2020, thus also on the regulations under the
Item “Privacy Policy – Type of data processing; ownership structure",
where Microsoft is actually processing on behalf of processed personal data
reserves data for its own purposes, under the item "Privacy Policy - Of-
Disclosure of processed data", in which Microsoft discloses the disclosures of the
generally reserves the data worked on the basis of legal obligations, without
the requirements of Article 28 (3) subparagraph 1 sentence 2 lit. a GDPR are complied with
(Only law of the European Union or of the Member States to which the processor
subject), or under the item "Privacy Policy - Storage and Deletion

Creation of data", where Microsoft also refrains from deleting data, for example
then reserves if Microsoft is required to retain by any applicable law
obligated or just entitled.
Also the "Additional Safeguards Addendum to Standard Contractual Clauses" (known as "Ap-
pendix 3 to the Standard Contractual Clauses – Additional Safeguards Addendum" in das
DPA December 2020) do not meet the requirements of Art. 28
Paragraph 3 subparagraph 1 sentence 2 lit.
implicitly presupposes that Microsoft will use the data processed in the order without or in return
processed according to the instructions because in the context of data exports to third countries
provide for an obligation on the part of Microsoft to inform customers immediately about a
to notify forced disclosure to third parties, unless this is after the on
prohibited by the law applicable to the requesting third party.
The processing of personal data actually processed on behalf of our own
purposes by Microsoft, as Microsoft reserves them, requires a disclosure of personal
of personal data by the person responsible to Microsoft in the legal sense. One
There is no apparent legal basis for this disclosure. From the processing of
contract data also for Microsoft's own purposes, the problem of a common
Men responsibility according to Art. 26 DS-GVO. Such is the case law
of the ECJ, is at least based on the only rudimentary information in the DPA July 2020
not be ruled out. This is at least with regard to accountability (Art. 5
Paragraph 2 i. V. m. Art. 5 Para. 1 lit. a DS-GVO) a problem. In the case of the actual
gens there is also the fact that there is no agreement according to Art. 26 DS-GVO.
The obligation to notify processing without instructions prior to processing is also
Although shown in Annex 3 No. 2.(a) according to the wording of the law, it is
under the item "Privacy Policy - Disclosure of Processed Data" inadmissible
sig restricted in that, on the one hand, the bans also apply in accordance with Article 28 (3) subparagraph 1 sentence 2

lit. a DS-GVO inadmissible law (not only law of the European Union or the

member states to which the processor is subject) and on the other hand

the communication may not be prohibited (only) because of an important public interest

got to.

Confidentiality obligation, Article 28 (3) subparagraph 1 sentence 2 lit. b GDPR

The regulations under the item "Privacy Policy - Confidentiality Obligation"

ment of the processor" of the DPA July 2020 in connection with the un-

permissible restrictions on the right to issue instructions can only be understood in such a way that

the obligation to process the personal data to authorized persons

Confidentiality should be limited to the same extent, what the requirements of

Article 28 (3) subparagraph 1 sentence 2 lit. b GDPR does not comply.

Obligation to delete after completion of the order, Article 28 Paragraph 3 Subsection 1 Sentence 2 lit. g GDPR

With regard to the obligation to delete the data processed in the order after the order has been

2.(g) of Annex 3 to the DPA July 2020 does not meet the requirements

of Article 28 (3) subparagraph 1 sentence 2 lit. g GDPR. At this point, although largely

the legal text has been adopted, but unlike in the legal text, copies are not

calls. In addition, the “Privacy Policy – Storage

and deletion of data" of the DPA July 2020 various restrictions on the deletion or

Obligation to return contrary to Article 28 Paragraph 3 Subsection 1 Clause 2 Letter g GDPR, including a long one

Implementation period for deletion and exceptions to the obligation to delete if Microsoft

from (any) applicable law obligated to store or only

is legitimate (and thus not only if, under Union law or the law of the member

states there is an obligation to store the personal data).

With regard to the regulations in the section “Privacy Policy – Storage and

Deletion of Data" of the July 2020 DPA, while it could be argued that the (by itself

also not legally compliant) Annex 3 should apply with priority if one

Inclusion clause in the section "Privacy Policy - Processing of Personal

related data; GDPR" interpreted as a priority clause. However, this does not happen

from the wording and would also mean that a very general clause

would supersede very specific regulations. In any case, those responsible can

in the event of such unclear regulations of their accountability according to Art. 5 Para. 2

i. V. m. Art. 5 Para. 1 lit. a DS-GVO.

Obligations to provide evidence and rights of control, Article 28 (3) subparagraph 1 lit. h GDPR

Section 2.(h) of Schedule 3 to the July 2020 DPA contains a sufficient

Obligation to prove the obligations from Art. 28 DS-GVO. The relationship to

Section "Privacy Policy - Data Security - Checking Compliance" and in particular

However, the specificity of the confidentiality obligation contained therein is unclear. Out and out

the unclear scope of this confidentiality obligation, the problem could arise

that those responsible fulfill their obligations to provide evidence to us as the supervisory authority

or towards data subjects, for example in the context of defending against claims for damages

cannot meet claims.

Also with regard to the control rights of those responsible, point 2.(h) of Annex 3 to

DPA July 2020 sufficient on its own. However, in this respect the section contains

"Privacy Policy - Data Security - Checking Compliance" still difficult

major restrictions on the control rights of those responsible. This is how each test

only right if certain documents provided by Microsoft are not sufficient

In this case, Microsoft only has to “immediately respond to the additional

instructions" of the customer "react [s]", but not actually a control

enable and contribute to it, as required by Article 28 (3) subparagraph 1 lit. h GDPR.

Each test is also subject to the proviso that Microsoft and the customer

before about "scope, time, duration, control and verification requirements as well as the
fees for the examination" have agreed; only the authorization of is excluded
Microsoft to "unreasonably delay the completion of the exam." The customer or
the customer must also bear the costs if the control is carried out exclusively by
Microsoft was at fault for what the right to control under data protection law
impermissibly devalued. The mandatory requirements according to Art. 28 (3) subparagraph 1 sentence 2 lit.
obligation to enable and actively contribute to controls
limited to certain actions. Checks are only allowed by certain third parties
carried out, but not by the customer himself. The DPA July
2020 also provides for "reasonable advance notice" without clarifying that in

In special exceptional cases, an inspection without prior notification is also appropriate
can be.
Engagement of subcontractors, Art. 28 Para. 2, 4 DS-GVO
The regulations for the involvement of sub-processors by Microsoft are in
various points unclear and contradictory and contrary to the legal
minimum requirements.
In the section "Privacy Policy - Notes and Controls When Using Un-
sub-processors" in the DPA July 2020 it says first: "Microsoft can sub-
engage processors to provide certain limited or supporting services
gene for Microsoft to provide. The customer agrees that such a
order is made and that Microsoft companies act as sub-processors
be set." These clauses give the impression that the customers
Approve all "Microsoft companies" as sub-processors, i.e. only the
second sentence actually means a (limited) general written permission

of Art. 28 Para. 2 S. 1 DS-GVO. However, the next sentence speaks in the plural of
the "above authorizations", so it is unclear whether only "Microsoft companies
ten" are approved as sub-processors or other third parties. who did-
actually as a sub-processor, specifically what can be used for, results
not from the DPA July 2020, so that the second sentence - subject to other contractual
agreements - not even a specific approval of the possibly defined elsewhere
"Microsoft companies" described in their area of responsibility
can. The July 2020 DPA includes a blanket statement that Microsoft "information
made available via sub-processors on a Microsoft website". responsible
verbatim must therefore check whether their contract also specifically states what
cher (specifically named) sub-processor for which (specifically named) activity
may be involved in order to meet their obligations under Art. 5 Para. 2 DS-GVO
to be able to. A blanket reference to a (possibly changing) website on dyna-
mixedly defined (and thus suddenly without further ado in the case of changes in the group structure
other companies comprehensive) or not exhaustively and precisely listed
companies is not enough.
Whether new sub-processors are only engaged with the consent of the controller
may be allowed or whether an objection solution should intervene is not entirely clear. To
the wording of the section "Privacy Policy - Notices and Controls at
Use of sub-processors" in the July 2020 DPA is a specific consent in the
Case-by-case required ("If the customer does not assign a new sub-processor
true..."), unless the clauses discussed in the previous paragraph require a specific consent
agreement in individual cases (then elsewhere in the contract specifically and conclusively with their respective
respective areas of responsibility to be described) sub-processors in the Microsoft
to represent the group. However, Annex 3 No. 1 of the DPA July 2020 regulates that Microsoft
"in the case of general written approval [...] always inform the customer of any

Intended change in relation to the addition or replacement of other tasks

[will] inform the contract processor, giving the customer the opportunity to object to such

to object to any changes". Seen as a logical consequence of an objection solution

the DPA July 2020 in the event of a lack of consent does not require a termination

right for Microsoft, but exclusively a right of termination for the customer. natural

This could simply be a customer-friendly arrangement. It does appear though

hardly conceivable that Microsoft in the mass business the objection of a single customer

which will be sufficient to authorize the involvement of a sub-processor

forgo or at least for this one customer a separate technology without

relationship of this specific sub-processor. Speaks accordingly

a statement from Microsoft to us also gives us the option of termination

by the customer under the heading "Objection to new sub-processing

ter" on.

Any more detailed rules on how to object to new sub-processors

however, are missing. Only the notice period for new sub-processors is regulated

in the section "Privacy Policy - Notes and Controls When Using Un-

ter processors" in the DPA July 2020.

In particular with regard to the involvement of sub-processors, but also in

other contexts, such as information about violations of the protection of

personal data, the clause under "Introduction - Electronic notifications

Corrections" of the July 2020 DPA as problematic, according to which Microsoft "information and

Notifications about online services electronically, also by e-mail, via the portal of the online

service or via a website to be designated by Microsoft".

and such notices even "[are] deemed to have been given on the date they are given by

was made available to Microsoft". Such a "pull" system in which responsibility

verbal statements about new sub-processors, violations of the protection of personal

related data or similar have to actively inform themselves and not through the order processing

employees are actively informed does not meet the legal requirements.

Should Microsoft also use new sub-processors in individual cases without consent

the last sentence in the section "Privacy Policy - Notes

Wise and Controls over the Use of Subprocessors" in the July 2020 DPA

possibly massive restriction of the right of termination, in that in the event of a termination

namely the payment obligations for the canceled online service subscriptions

only omitted with the next bill.

According to Art. 28 Para. 4 S. 1 DS-GVO, subcontractors must be contracted

or any other legal instrument under Union law or the law of the relevant

Member State imposes the same data protection obligations as between

responsible and the processor are agreed. In the section "Privacy

Provisions - Instructions and controls when using sub-processors" in

DPA July 2020 is a written contract for purpose limitation compliance only

provided for the sub-processor. Unspecified "written agreements"

gen", which are not necessary legal instruments under Union law or the law of the

Member State concerned, must then be used by the sub-processors

tern require that they "provide at least the level of data protection" that the DPA July

2020 required by Microsoft. The law already not only refers to the level of data

protection, but requires a transfer of the same data protection obligations, i. H. it

Without exception, all contractual obligations of the processor must also be

be imposed on subcontractors. The July 2020 section of the DPA governs disclosure

According to its heading also the "Controls when using subcontractors"

such that Microsoft undertakes to "oversee the sub-processors

to ensure that these contractual obligations are met". law

The section does not provide for formal control rights for those responsible, but neither

sometimes an imposition of the - insufficient, see above - control rights as opposite

Microsoft. The same applies to the obligation to provide evidence. Should Annex 3 to the quoted section

proceed - which is not clear, so that in any case there is a problem with regard to Art. 5 para. 2

DS-GVO exists - the regulation there would not be sufficient either. Because even after the

According to this regulation, the sub-processor will not be given all contractual data

protection obligations imposed, but only "the same data protection obligations [...] as in these

GDPR provisions are described", i.e. only those listed directly in Annex 3

ten duties.

Data exports, Art. 44 GDPR

In the DPA July 2020 under the item "Data security - verification of compliance"

restrictions of the standard contractual clauses. These should "in addition to

sel 5, paragraph f and clause 12, paragraph 2 of the Standard Contractual Clauses" apply and it will

claims that this does not change the Standard Contractual Clauses. Although there is

in the introduction to the July 2020 DPA, a general statement that the Standard Contractual

Clauses take precedence over the July 2020 DPA, as do the Standard Contractual Clauses override theirs

Modification prohibition itself contain a corresponding priority regulation. Doubtful - and

with regard to Art. 5 Para. 2 DS-GVO is problematic - is already whether the general pre-

rank clause in the introductory part of the July 2020 DPA applies at all if the in

The specific limitation of the standard contractual clauses in question itself

claims not to represent a restriction, so that under this assumption the priority clause

sel cannot be applied logically. However, this can remain open

because any restriction of the rights and obligations under the standard contractual clauses,

depending on their wording and also if they are elsewhere for subordinate and

so that it is declared inapplicable, leads to an impermissible modification of the standard

carry clauses. Because this is intended and regularly achieved as a result,

that the Standard Contractual Clauses cannot be fully applied. dementia

Accordingly, recital 109 GDPR also emphasizes that other contractual clauses

neither directly nor indirectly contradict the standard data protection clauses

allowed to stand. Thus, the present restriction “additional” clause also applies despite

their presumed invalidity under civil law to an inadmissible modification of the

Standard contractual clauses so that they cannot justify data export.

Microsoft reserves the right to process the order data at any location where Micro-

soft or its sub-processors (DPA July 2020, section “Privacy

provisions - data transfers and storage location - data transfers"), i.e

also in the US. It is not apparent that sufficient additional measures are

would have been taken, in accordance with the case law of the ECJ in the judgment of

July 16, 2020 – C-311/18 (“Schrems II”) the insufficient level of data protection in the USA

at the same time. Also the "Additional Safeguards Addendum to Standard Contractual Clauses"

(which as "Appendix 3 to the Standard Contractual Clauses - Additional Safeguards Add-

dendum" were included in the DPA December 2020) are obviously sufficient for this

not, since in particular they do not allow US authorities to access the processed data

exclude persons who are still affected from legal protection against access

granted by US authorities.

NETWAYS Web Services Jitsi

With the Netways offer, you get moderator access to a pre-configured

punch by Jitsi Meet. The pre-configured moderation password is long, but cannot

be changed yourself. In the standard configuration, the conferences are not through

Password protected and the participants enter the conference with an active camera and

active microphone.

Those responsible should therefore before the start date and before other participants

enter conference open the conference and set a password. In addition, they should

Configure the conference rooms used so that participants with a deactivated microphone

enter the conference with the camera deactivated.

To permanently exclude a participant from the conference, it is

possible to set a new password and the function "eject"

apply to the person.

We did not find any shortcomings in the transport encryption. In the course of authentication

fication of persons who take on the role of moderation is carried out according to the

State of the art avoids the transmission of the password to the provider.

Open Source Company - BigBlueButton

With the offer provided by the Open Source Company (OSC), responsibility

literally an access with moderation rights on a BigBlueButton instance.

To enter the video conference in the default settings, participants only need the

address (URL) of the conference and join it with the microphone on and off

Camera. Those responsible should therefore configure for the conference rooms used

that participation is only possible for registered participants and guests with knowledge of an

additional access codes is possible and that participants with a deactivated microphone

enter conference. In addition, it is possible and advisable to set a release

must be done by the moderator.

In the default settings, the video conference is only started after the moderating

person who opened it. However, it is also possible for other authenticated participants

allow opening or grant moderation rights.

We did not find any flaws in the transport encryption.

safe-videoconferencing.de – Jitsi

There is no fixed moderation role. The moderator of a conference automatically becomes the first person to enter the conference room. If she leaves - even if it is because of communication problems - the conference room, the moderation role automatically goes to the person who has been attending the conference the longest. In use cases 2 and 3 this constitutes a defect.

We did not find any shortcomings in the transport encryption. The authentication procedure does not correspond to the state of the art and transmits the password within half of the TLS session to the service.

TeamViewer Meeting (formerly Blizz)

Provider reserves the right to process order data for its own purposes. defects in Order Processing Agreement.

The "TeamViewer order processing contract (AVV), version January 1, 2021" (fol-

2.2 only provides for a limited right of instruction for those responsible.

Section 2.9 sentence 3 AVV only permits checks and inspections if they are objectively established indications of a breach by the provider of the AVV or data protective regulations exist, and restricts the according to Art. 28 Para. 3 lit. h DS-GVO permissible involvement of third parties as auditors on unspecified "qualified" auditors.

Sections 2.5 and 2.6 AVV provide that the support by the provider in maintaining of the rights of those affected and compliance with Art. 32 to 36 DS-GVO is subject to a fee, "so-far and to the extent permitted by applicable data protection law". It is unclear whether of this cases should also be recorded in which the support is only due to a contractual or violation of the law by the provider, because such an agreement is permissible in principle, but devalues the obligation comprehensively, which in turn consequential problems under data protection law. This is at least with regard to the

Accountability (Art. 5 Para. 2 in conjunction with Art. 5 Para. 1 lit. a) problematic.

According to the wording, point 2.13 AVV contains at the end an only by the requirement, Art. 44 et seq.
GDPR compliance, limited permission for provider to use sub-processors in
involve third countries. Section 3.1 AVV does not expressly regulate that the provider
processors only with permission. Both are in any case with regard to the
Accountability (Art. 5 Para. 2 in conjunction with Art. 5 Para. 1 lit. a) problematic.
The AVV does not oblige the provider sufficiently within the meaning of Art. 28 Para. 4 Sentence 1 DS-
BER to impose the same data protection obligations on sub-processors as they apply to the
Providers exist (cf. Section 3.3 GCU).
Section 2.2 and Section 3.2 of the GCU contain references to the "TeamViewer end user license
agreement, version: January 1, 2021" (hereinafter: "EULA"), in which in particular

It is not clear whether this is intended to restrict the right to issue instructions. This is in any case
With regard to accountability (Art. 5 Para. 2 in conjunction with Art. 5 Para. 1 lit. a) problematic.
In Section 4 AVV, the provider reserves a right (with no further restrictions in terms of content) to change
amendment of the AVV. This does not even meet the requirements of § 308 No. 5 BGB, the
according to the case law of the BGH on § 307 BGB also in business dealings
is applicable (judgment of June 10, 2008 – XI ZR 283/07; see also default judgment of
September 10, 2014 - XII ZR 56/11), is also problematic insofar as
as giving the provider the opportunity to enter into an illegal contract
and even determine the purpose and means of processing.
Pursuant to Section 3 Appendix 1 to AVV diverse, processing on behalf of the customer is not the subject of processing
Processing of personal data by the provider, as described in the respective pro-
duct privacy policy described. According to Section 1.B (meaning: Section 1.C, these include the
subheading is missing) of the "TeamViewer Product Privacy Policy" (without version

number, retrieved February 4, 2021) (hereinafter: "PDSRL") various information about end devices,
Use, connection partners, etc., including for the purposes of product improvement
tion and direct advertising (cf. Section 1.D PDSRL). A legal basis for the related
Bound disclosure of personal data by those responsible is not evident.
From the processing of the order data also for the provider's own purposes follows
the problem of joint responsibility according to Art. 26 DS-GVO. a sol
che is obvious according to the case law of the ECJ, but is at least based on the information in
of the EULA cannot be ruled out. This is at least in terms of accountability
(Art. 5 para. 2 in conjunction with Art. 5 para. 1 lit. a GDPR) is a problem. In the case of the actual
In addition, there is no agreement under Art. 26 GDPR.
Due to the legal deficiencies, no technical examination was carried out.
Tixeo Cloud
Registration is mandatory to use the Tixeo offer. For this
registration requires the use of an e-mail address, Tixeo offers
e.g. B. Jitsi a slightly higher security with regard to the identity of the participants. Added
comes that only invited participants can join a scheduled meeting,
which enables those responsible to control the group of participants.
Tixeo Cloud requires the installation of a client on the device on which it is used
shall be. Use via a website is not intended for this offer. It
must therefore be considered whether an installation of software in the intended environment
exercise is possible.
Participants enter the conference with activated input devices (microphone and
mera). This is currently not configurable. In the applications described above
This represents a defect. The provider has to remedy this defect for
Version 16.5 (scheduled for mid-February 2021) announced.
The organizer of a meeting has the option of granting the rights to the participants

Allow and revoke use of camera and microphone. The function corresponds
the camera and mute function of the respective participants. Will the rights
given back to a participating person, they will be restored to the state they were in before the
deprivation of rights. This should be communicated to the participants, since as soon as the
Rights are revoked, the respective buttons disappear and with them the moderator
can switch on the input devices if they were switched on before the withdrawal of rights.
If this function is to be used, the participants should
be advised that they should disable their own camera or microphone,
so that even after the rights have been granted, they can determine when the input
Councils to be reactivated.
At the time of our review, we found that the provided Tixeo app
does not use certificate pinning. There is an increased risk that, for example

Man-in-the-middle attacks between the server and the client are successful and hence
the integrity and confidentiality of the communication is violated. At least with some cli-
ents, the person responsible can and should carry out a certificate pinning. Tixeo provides here-
ready for a guide.
Tixeo offers a weak version of end-to-end encryption.
Tixeo has indicated to us that it is a dual-use product under French law.
obligations to store the framework data of the video conferences for six years
subject. Tixeo was not able to tell us at the time this notice went to press
how far this obligation extends and on what legal basis it is based. responsible
should request detailed information about this, as far as possible the immediate deletion
request the frame data after the end of a conference and check whether they have a
Service that performs such comprehensive data storage for which

Controllers themselves regularly have no legal basis.

Werk21—BigBlueButton

With the offer provided by Werk21, those responsible receive access with

Moderation rights on a BigBlueButton instance.

To enter the video conference in the default settings, participants only need the

address (URL) of the conference and join it with the microphone on and off

Camera. Those responsible should therefore configure for the conference rooms used

that participation is only possible for registered participants and guests with knowledge of an

additional access codes is possible and that participants with a deactivated microphone

enter conference. In addition, it is possible and advisable to set a release

must be done by the moderator.

In the default settings, the video conference is only started after the moderating

person who opened it. However, it is also possible for other authenticated participants

allow opening or grant moderation rights.

Despite the provision of a function for controlling the recording, a recording

recording of the entire conference and this recording at a later date

Cut to size based on the set crop marks. This can be wrong

moderateness of processing and in any case contradicts the principle of data

minimization and regularly the expectations of the users. It will therefore

recommended to disable the feature permanently.

We did not find any flaws in the transport encryption.

Wire Pro

There are no options for moderating the actual video con-

references. Group moderators only have the option to exclude other people

to remove from the group. However, excluding a person from a group removes them

not from video calls already in progress.

The participants have control over the activation/deactivation of the camera or microphone.

participants themselves. If there are more than two people, the participants (except for the current

person) with disabled input devices.

Since the use of Wire for communication requires membership in a team,

However, those responsible have direct control over which persons in the context of the

application can communicate with each other.

Wire offers strong end-to-end encryption. The authentication of the

coming devices is done by comparing their digital fingerprints. a security

profit can be made if the comparison is carried out in person or via a

separate communication channel happens.

Version 2.0 of February 18, 2021

zoom

- 33 –

Deficiencies in the order processing contract. Impermissible restrictions on the binding

tion, the obligation to delete and control rights. Prohibited data exports.

The "Zoom Global Data Processing Addendum", November 2020 (hereinafter: "DPA") lists in

Clause 2.3 and 3.2 a new reference to the "Zoom Privacy Statement", which makes it unclear

makes whether and, if so, to what extent Zoom as a processor, as the sole controller or

acts as jointly responsible with the customers. The “Zoom Privacy

Statement" (last change August 2020) explains the case of order processing

namely expressly inapplicable.

The categories of data subjects in Exhibit A and Appendix 1 to Exhibit C DPA are un-

adequately described. Final, specific information must be provided.

The types of data processed in Exhibit A and Appendix 1 to Exhibit C DPA are invalid

adequately described. On the one hand, the list is not exhaustive, on the other hand, there are no

specific list of at least all the content of the communication. Although these are

ter described as “Cloud Recordings”, but only in the form of storage as MP4.

In fact, this data is also processed for the conference as such - just

not readily saved. For this technically necessary data to be processed

In any case, the IP addresses of the participants also belong. If other categories are missing,

should also be checked.

The binding instructions in Section 3.2 DPA still do not meet the requirements of Article 28

Paragraph 3 lit. a DS-GVO, since they process outside of the instructions

Obligations of the provider from law other than that of the European Union or the

Member States to which the provider is subject. As a result, the obligation to

Information about corresponding processing no longer meets the requirements of Art. 28

Paragraph 3 lit. a GDPR. It must be checked whether the reference to the Zoom Privacy Statement

illegal processing is permitted.

Clause 6.1 of the current DPA now limits the obligations for security measures

more on "customer's personal data" and could be understood in such a way that only the personal

related data of the contractual partners, but not the personal

nary-related data that the provider processes on behalf of must be protected.

In any case, this is problematic with regard to accountability (Article 5 (2) GDPR).

matic.

Section 3.4 sentence 3 DPA concludes the deletion of the processed personal data

after the end of the contract to a greater extent than permitted under Article 28 (3) (g) GDPR,

any applicable law justifying non-deletion. In addition, the

clause a reference to the "data retention and deletion policy" of the provider, which

is not part of the contract, which at least with regard to the formal requirement of the

Art. 28 (9) GDPR and the accountability according to Art. 5 (1) lit. a, (2) GDPR

GMO is problematic, and on the other hand, there are further impermissible restrictions on the

Deletion could include, especially since apparently a dynamic reference to the

the current policy is available, so that later unilateral changes by the provider

could take place, about which customers do not even have to be informed

senior Section 3 sentence 4 DPA implicitly restricts the obligation to delete even further by also

the case is regulated that the deletion is "impracticable or prohibited by law, rule or regula-

is. What has just been said applies to the legal prohibition; a deletion must be technically possible

become possible. Section 9.5 DPA could be understood in such a way that the instruction

law should be limited in the event of data breaches and should be clarified.

Clause 9.7 DPA excludes support by the provider in the event of data breaches if

these were caused by actions or omissions of the customers

the. Although the provider has inserted an exception that the exclusion does not apply if

the applicable data protection law requires this, but Art. 28 (3) lit. f GDPR requires it

not that the provider supports it, just that the contract is a support obligation

provides. This is at least with regard to accountability (Art. 5 Para. 1 lit. a,

Para. 2 GDPR) problematic.

Clause 9.3 contains a requirement that, taken in isolation, meets the requirements of Article 28 (3) lit

DS-GVO probably still sufficient clause. However, Clause 9.4 contains serious

Restrictions on the customer's control rights, which both Art. 28 Para. 3 lit. h

GDPR and the standard contractual clauses. So are at least one

30-day notice and prior on-site inspection agreement without

Exception prescribed, also in urgent cases and with the possibility for the provider to

to delay and prevent trolling by refusing to agree. The provider

may allow or deny third party auditors. On-site inspections may - also in the case of changes

ments in processing, even if there are several processing locations, even in the case of serious

the incidents – take place at most once a year. have customers

"any additional costs arising from this" to bear, which the wording only on

refers to the restriction of the controls to once a year, but in terms of meaning probably all

means controls, also in the event that these are only carried out through the fault of the

bidders have become necessary. Exhibit B clause 20.1 also contains this

serious restrictions of the control rights, which partly result from the aforementioned

speak, sometimes even go beyond that, by excluding any right of control

and instead refers to an audit report obtained by the provider itself

s, except in the event that a security incident (security breach) has occurred.

came that had a significant business impact on the customer,

or that an audit right is required by law. The latter is in the application

not the case in the scope of the GDPR, but Art. 28 (3) lit. h GDPR only stipulates that

the order processing contract must contractually provide for an audit right.

Section 5.2 DPA provides for a blanket approval of sub-processors who

a WWW page, which is at least in terms of accountability

is problematic, but is also dubious with regard to Art. 28 Para. 2 DS-GVO. The list

the subcontractor at the time of the conclusion of the contract does not have to

correspond to the version viewed and/or secured by those responsible, and

it is not even regulated whether the relevant time is that of the signing by the

is responsible or who signed by Zoom. This allows responsible

verbatim at least not their accountability (Art. 5 Para. 2 in conjunction with Art. 5 Para. 1 lit. a)

progeny. The sub-processors listed on the specified website

are also not properly named, in most cases not even with theirs

full name, in any case without address. The areas of responsibility are not clear

limited, and the information on the WWW site does not match the information provided

the provider has made to us what the meaning of a written fixation

of the approved sub-processors.

The procedure for information about new sub-processors in section 5.3.1 sentence 3 DPA
requires active action by those responsible and is therefore not sufficient for Art. 28 Para. 2
Sentence 2 GDPR. Those responsible who do not actively subscribe to the notifications themselves,
Furthermore, they cannot be held accountable (Art. 5 Para. 2 in conjunction with Art. 5 Para. 1 lit. a DS-
GMO) offspring.
Section 5.3.2.d) DPA makes it practically impossible for those responsible to take action against new sub-contractors
processor to object because they and the provider only have a right of termination for
have the DPA if the provider does not offer an alternative solution but their payment
obligations under the main contract survive. The provider can also unilaterally
Set service, Section 5.3.2.d) DPA. This completely devalues the right of objection, so
that there is a violation of Art. 28 Para. 2 Sentence 2 DS-GVO. In addition, the
Objection period against new sub-processors only ten days.
Section 5.5 violates Article 28 Paragraph 4 Sentence 1 GDPR because the current version is different
than in previous versions - sub-processors no longer have the same data protection
obligations must be imposed, but only equivalent ones. In addition, are contrary

Art. 28 para. 4 sentence 1 DS-GVO also legal instruments other than those under Union law or
permitted by the law of the Member States.
In Section 5.7 DPA, the standard contractual clauses are modified inadmissibly, so that
these cannot justify the data export (regardless of the question of whether these
conversion is effective under civil law or not).
Section 10.4 DPA gives the provider the unilateral right to change the contract under certain
ten conditions.
Due to the legal deficiencies, no technical examination was carried out.

Inspection obligations of the responsible persons

Even if our audits did not uncover any deficiencies, this does not mean that

these are not available and does not release those responsible from their legal obligations. It

it is expressly pointed out that no comprehensive examination of the offers

followed, in particular no comprehensive technical examination and usually none

Checking the data protection declarations. The latter only affect those who are responsible for themselves

Data processing by video conferencing system providers. Not covered by the privacy

ments are those data processing operations that are carried out by responsible bodies based in

Berlin perform when they use the Services.

We therefore recommend that those responsible check the following in particular:

 If the processor has acted contrary to the specifications in the process we have checked

tragswerk otherwise processing the usage data for its own purposes or purposes

reserved for third parties?

 Are there indications that the processor does not comply with the specifications in the

contract processing agreement?

 If the processor carries out user tracking that is not necessary for the operation of the solution

is required?

 Can be found in the data protection declarations sent to the conference participants in the course

of the conference participation presented or made accessible by the processor

be, references to data processing by the processor that is compatible with the

data processing in the contract cannot be reconciled?

Is the security of the processed data and compliance with data protection by technical

design and data protection-friendly default settings, also under the specific

planned deployment circumstances given?

 Does the processor have sufficient guarantees for the implementation of appropriate technical

nical and organizational measures in the operation of the service?

Continuous update of the provider list

The list of video conferencing solution providers will be added to on an ongoing basis, if within the framework

further offers were examined in our supervisory and advisory activities. changes,

We will check the providers listed and take them into account in the subsequent version.

view. We also strongly encourage vendors to expand their video conferencing solutions

those responsible in Berlin and want to know about special technical solutions

add - for example with end-to-end encryption, with integration into professional user ma-

nagement systems or for a large number of participants - tell us about your offer for in-

form and to provide us with the contract documents and test access.

However, we ask that you self-critically check before submitting or have the company

The data protection officer or members of the legal advisory professions check

whether the contracts meet the legal requirements. For this we recommend

also reading the comments on the contracts already checked and our "Recommendation

errors for the examination of order processing contracts from providers of video con-

reference services".21 This can also allow those responsible to review the contracts of providers

tern that are not yet included in the list. We also ask that you send a technical

Technical review of the video conferencing service in accordance with the DSK orientation guide

to do. Identified deficiencies should be remedied before submitting the documents to us

will.

21 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientation aids/2020-BlnBDI-Recommendation-

gen_Pruefung_Order processing contracts_Videoconferencing services.pdf.