Berlin data protection officer to carry out video conferences during the contact restrictions

The precautionary measures to contain the corona pandemic to restrictions in almost all areas of daily life. Around avoiding physical proximity between people as much as possible in many cases that professional contacts are no longer personal, but held over the network. If more than two or three people If you want to have a conversation together, telephone and held video conferences. Many companies and authorities chen well-functioning offers for their implementation and provide next back to checking whether they also claim data protection can be taken.

With this text, the Berlin Commissioner for Data Protection and Information Freedom of information to the companies and authorities subject to their supervision and other institutions information on the requirements for use of video conferencing systems and describe the risks that standing if they are not complied with. To avoid these risks or at least to reduce it and the data protection regulations are to be observed, those responsible are called upon to but not data protection-compliant solutions as soon as possible through data to replace or to improve accordingly.

Personal data in video conferences

Personal data play a role when conducting video conferencing role in two ways: first, the spoken word itself contain information about individuals. Second fall at the implementation of a video conference, data about the participants

and participants, i. H. their contact details, their names and details

informed of the time and place of their participation in the conference. Below are on

in any case, data on employees of the institution hosting the videoconference

organized, and possibly data about their interlocutors, be it

Business partners, employees of other institutions or private

fathers.

Basic requirements and recommendations

 Video telephony and video conferencing should be over encrypted channels

be settled. This applies both to switching the connection

genes as well as the transmission of audio and video data.

 If you do not use the video conferencing solution yourself and with

reasonable effort (which would be preferable), then

you can use a reliable video conferencing service

gen. The prerequisite is that you have an order processing contract

Friedrichstr. 219

10969 Berlin

Visitor entrance:

Puttkamer Str. 16-18

Telephone: (030) 13889-0

Fax: (030) 215 50 50

mailbox@datenschutz-berlin.de

office hours

daily 10 a.m. - 3 p.m., Thurs. 10 a.m. - 6 p.m

(or by appointment)

reachability

U6: Kochstr.

close with him and the operator does not provide any information about the

authorized and their communication or the use of the software for

processed for general purposes or passed on to third parties.

The service provider should process the data in the European Union, a

country of the European Economic Area or in a country deemed to be the same

in the applicable country and also have their registered office there. The

Equivalence is determined by the European Commission (see

https://ec.europa.eu/info/law/law-topic/data-protection/international-di-

mension-data-protection/adequacy-decisions_de). Alternatively, he can

data export are based on the conclusion of a contract whose

Text of the standard contractual clauses approved by the EU Commission

selen (see below). The requirement also applies to all subcontractors

mer, which the service provider makes use of.

 Unless it is excluded by encryption that the over-

communicated audio and video data by the provider.

can be taken, it is recommended that only providers in the European

European Union or the European Economic Area,

if sensitive data is discussed within the video conference

should. Persons subject to professional secrecy may only use service providers who

may be prosecuted in the event of a breach of confidentiality.

Medical service providers may only be certified service providers

use, see https://www.kbv.de/html/videosprechstunden.php.

risks

A major risk is that during the video conference,

listened to or the contents recorded and further evaluated

the, possibly to the detriment of the people attending the conference

taken or talked about. The risk is on

greatest when sensitive topics are addressed in the exchange

such as B. the state of health or the political views of a

Person.

Third parties may attempt to establish a conversation between the parties

to listen to the user and the operator of the offer or to

cut. But also the operator of the video conference system himself

may have an interest or be officially obliged to

to make a cut, be it just to adjust the quality of the transmission

judge, be it because the recording was made on behalf of third parties for their purposes

follows.

Video conferencing systems are usually designed in such a way that when

driver service the unencrypted images and sounds converge.

This enables him to control the flow of data and send the data to the abilities

adapt the capabilities of the devices of the participants. It can also be that

the performance of recordings forms part of the offer.

It is therefore generally unavoidable that at least the operator

service authorized or unauthorized recordings can be made

whether with his knowledge or against his will. Only services where

n the data is encrypted on one end device and only on

can be decrypted again by the remote station – so-called end

end-to-end encryption – ensure that no such

cuts can be made by the operator.

You should know: Telecommunications secrecy protects you when you use it

of video conferencing systems against the provider. It stretches

refers to the operator of your Internet connection, but not to yours

video conferencing service. This is a loophole in the law that the European

recognized by the legislature. He has committed member states to

at the end of this year the protection on "interpersonal communication

services", including to public web and video conferencing systems.

dilate These will then meet the strict requirements of the telecommunications

communication law, including telecommunications secrecy

ses. However, the old, incomplete rules still apply.

You therefore have no choice: you must contact the provider of your video conferencing

trust service. However, you can at least contractually bind him

the. You are also obliged to do this. Because you don't just contribute to the

not only to protect your own rights, but also to protect your employees

and communication partners. What is to be regulated by contract

stipulates the legislature. Reputable providers therefore have a

subcontract.

However, enforcement will go far for you and the named persons

more difficult if your contractual partner is based outside Europe

European Union and European Economic Area, so you can find yourself in the

would have to turn to a court in a foreign jurisdiction in the event of a conflict

order that may not protect your rights as well

like the European one. In order to counteract this circumstance, the Euro

European Commission developed standard contractual clauses (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087). Only However, their full application unfolds the intended comprehensive the protection of your interests and the interests of the persons concerned. The obligations from the standard contractual clauses must therefore not be be restricted.

This protection also extends to risks arising from the evaluation of the Circumstances of communication or other data for their own purposes provider or for third-party purposes. These risks also exist in the formation of personality and usage profiles of the conversation Participants who are advertising, political or through competitors and misused to recruit staff. To create such a profile exclude education, you must provide the provider with such an evaluation prohibit However, many providers keep the evaluation in their ren General Terms and Conditions. In such a case would be individual usage agreements required. seems more promising a change of provider.

recommendations

First of all, you should check whether tele-phone conferences could be sufficient to achieve the desired vote and bring about each other. These can be much more easily be carried out properly.

If video conferencing is necessary, it is best to use your own service in the source text of publicly available software (open source software) deliver. The use of commercial software is also a matter of course possible as long as it is ensured that this software does not itself store data

via your employees or their communication partners to the

manufacturer or to third parties for their own purposes. You can

also fall back on the support of a service provider for the operation

fen. Unfortunately, especially for small institutions, it is hardly

affordable with moderate effort, a well-functioning data protection-compliant

operate the solution or have it operated.

At the next level, we recommend you to check if one of the solutions

gene European providers meets your needs. Fulfills a

solution to your business needs, then check the provider

can be expected to process the data only within the permissible framework

and in particular not to third parties contrary to European data protection law

- including foreign authorities - that he is sufficient

Data security (e.g. through certification) can prove to you

the encryption of the data transmission is guaranteed and ready with

to conclude a legally compliant order processing contract for you

eat.

The provider must also explain to you whether he uses service providers

Outside the European Union or the European Economic Area

to provide the service. Some providers only act

as a reseller of services from US companies. At-

leave a significant part of the service to non-European

cal companies of the same group of companies. In the

In the last two cases you win a European

portable contact person. However, this does not guarantee

that the provider adheres to EU law in the event of a conflict and not to his

cold right.

In the latter case, as well as when directly commissioning one of the

non-European providers with a significant market share - as a rule

based in the USA - in addition to the questions that also apply to purely European

European providers play a role, which entails additional risks

and check the legal guarantees.

Unfortunately, some of the providers who offer technically mature solutions

provide genes that the data protection requirements have not yet.

This currently applies (as of July 3, 2020) e.g. B. on the services Blizz, Cisco Web

bEx, Cisco WebEx via Telekom, Google Meet, GoToMeeting, Microsoft

Teams, Skype, Skype for Business Online and Zoom too. With NETWAYS

Web Services Jitsi, Sicherheit-videokonferenz.de, TixeoCloud, Werk21 Big-

However, BlueButton and Wire are available as alternatives that

meet protection requirements.

For a detailed assessment, we refer to our "Notes for

liner responsible for providers of video conferencing services", the regular

moderately updated and the data available at https://www.datenschutz-ber-

lin.de/infothek-und-service/themen-a-bis-z/corona-Pandemic.html

are. If the provider you are considering is not in this

be included in the list, to facilitate your check, you will find

website also referred to our “Recommendations for Auditing

contract processing contracts from providers of video conferencing services",

the certain frequently observed deficiencies in order processing

contracts.

Organizational regulations

Finally, forget about organizational regulations for the vi-
deoconferencing in your institution does not. These should present the procedure
to be observed when recording a video conference
should, and possibly also contain provisions on which topics in a
video conference should not be spoken. In the regulations should
the contact details of persons who are subject to data protection law
in case of doubt or in the event of information technology problems,
give lung. It should also explain how to proceed if a
violation of the protection of personal data is suspected.

Above all, those professional groups who work with particularly sensitive data
work, for example in a medical or psychological context
Consultations should focus in particular on compliance with data protection
respect legal principles. The use of platforms for vi-
Deodorant-assisted online counseling often involves a variety of risks that
must be carefully weighed against the benefits.

Conclusion

Even in this time of an extremely accelerated and sometimes over-
overthrown digitization of the world of work, the protection of personal
ner data are always considered. Where the urgency of the current
measures to be taken does not allow this to the necessary extent,
must be continuously improved. If data protection law
Imponderables or even grievances occur, these must be reported immediately
remedy.