Berlin data protection authority: Position paper and a checklist on the issue of data protection in connection with video conferencing

Article by Dr. Carlo Piltz and Stefan Hessel

Services from Microsoft (particularly Teams and Skype) and Zoom do not conform to data protection requirements

In providing information about data protection during the coronavirus pandemic, the Berlin data protection authority has issued a position paper and a checklist, both of which are dated 8 April 2020 based on the document metadata, in which it discusses the issue of data protection in connection with video conferencing. While it is good to see the authority take this initiative, and particularly its decision to provide specific guidelines, its determination that the services provided by Microsoft, specifically Teams and Skype, and the video conferencing software Zoom cannot be used in a manner conforming to data protection requirements appears debatable.

In its position paper, the Berlin data protection authority pursues the goal of avoiding or at least minimizing risks to data subjects in connection with video conferencing. At the same time, it urges businesses to use solutions which conform to data protection requirements instead of the non-conforming solutions which have been introduced at short notice in response to the current situation. Specifically, the authority recommends that video calls and video conferences should be conducted exclusively through encrypted channels. This recommendation may be called sensible, even though data encryption is only one of the possible technical data protection measures cited in Article 32(1)(a) of the GDPR. However, the authority does not specify the degree or type of encryption required (e.g. transport encryption and/or content encryption).

The authority also recommends solutions operated by the controllers themselves (self-hosted solutions). But such solutions are likely unrealistic for many companies because of the enormous expense. The authority acknowledges this fact and allows for the possibility of engaging a reliable service provider as a processor. This view is generally welcome, but the fact that the authority goes right to the option of a processing arrangement is curious. After all, it is also possible that the use of encryption means that the GDPR will not apply for the video
service provider because it will have no access to personal data. It is also possible that the video service provider is itself responsible for ensuring privacy, e.g. if the latter. A mixture of these categories may also apply, depending on the individual case.

In addition to providers based in the EU or elsewhere in the European Free Trade Association (EFTA) zone, the authority also expressly states that service providers based in third countries are acceptable if they offer an equivalent level of data protection. Aside from a decision from the EU Commission finding an equivalent level of protection for personal data, the authority also rightly points out the use of standard contractual clauses as another possibility. In practice, an adequacy decision from the EU Commission should be of particular importance in this context for transfers of data to US controllers subject to the EU-US Privacy Shield. Despite some criticism from the data protection authority, the level of protection actually guaranteed by the EU-US Privacy Shield continues to be an important and valid basis for data transfers to the US, satisfying legal requirements.

The authority's other statements do not appear to adhere strictly to current law. For example, the data protection authority recommends that only providers in the EU or the EFTA should be used in cases involving the processing of sensitive data where the provider cannot be prevented from accessing the transferred audio and video data. But such a distinction based on the provider's location is not found in the Chapter of the GDPR beginning with Article 44. As we have seen, the relevant criterion is in fact the level of data protection. As a result, this recommendation is likely not meant to be legally binding.

**Risks of Data Processing**

In its position paper, the supervisory authority also addresses the risks of video conferencing, which it identifies as the risk of unauthorized listening or recording, as well as further exploitation of the content. According to the data protection authority, this could result in adverse effects for the people who take part in the video conference, as well as those who are mentioned in the discussion. The authority notes that this risk materializes not only if the conference is recorded by third parties, but even if the recording is made by the operator of the video system. The authority reasons that the operator can make a recording of the conference unless it is blocked by means of encryption, even if this recording is made for analytical purposes only. The authority also cites telecommunications secrecy as another argument that such a risk exists. In doing so, it makes the factually correct observation that telecommunications secrecy does not apply for video service providers, at least until now, because they do not provide telecommunications services and instead function as "over-the-top" providers. But it does not follow from this observation that video services should not be used: in fact, even the
authority concedes that this risk can be substantially minimized through a contractual arrangement, such as e.g. a processing contract. The authority’s view that recording is never allowed, even for the purpose of improving the service, is in any case unconvincing. After all, improving or developing the service is a legitimate purpose and may actually be in the user’s interest. From a legal standpoint, the provider may have a legitimate interest in improving the service in accordance with Article 6(1)(f) of the GDPR, and recording may also be conducted based on the user’s consent in accordance with Article 6(1)(a) of the GDPR. In cases involving providers based outside the EU and the EFTA, the authority also sees a vague risk in connection with the fact that the processing contract and other contractual arrangements will have to be enforced in a foreign legal system, and it recommends that the agreement consist entirely of standard contractual clauses. In this document, the authority does not devote any further discussion to the fact that standard contractual clauses are not the only legal basis for transfers to third countries in accordance with the GDPR.

The Authority’s Recommendations
In its recommendations, the Berlin data protection authority advises companies to use conference calls wherever possible instead of video conferencing, noting that conference calls are "much easier to conduct in a manner conforming to data protection requirements." Regardless of the question as to whether this is actually the case, this recommendation will likely be unhelpful for many companies in practice: the use of video conferencing software, featuring moderation options and the ability to share one’s screen, offers whole new possibilities for collaboration. The authority also makes reference to solutions which are operated by the controllers themselves and by European providers, but does not mention any specific products, as the Data Protection Commissioner for the State of Baden-Württemberg recently did.

Statements Concerning Services from Microsoft and Zoom
The authority then once again addresses the issue of "non-European service providers," but mentions only providers from the US. It observes that the aforementioned risk of recording exists even with providers which have a contractual contact person in Europe, but whose service is largely provided by non-European service providers which are members of the same corporate group. The authority states that this risk has to be minimized through separate guarantees, which is often not the case. Specifically, the authority states as follows: "The most prominent examples are the services provided by Microsoft Corporation (e.g. Microsoft Teams), including its subsidiary Skype Communications SARL, which is based in Luxembourg (with the product of the same name)."
The authority does not discuss how it reached the conclusion that there is a significant risk that Microsoft will fail to honor its contractual agreements and that it will not be possible to enforce any claims or contractual rights in the US. It also fails to mention Microsoft's data residency model, which expressly assures German customers of Microsoft Teams and Skype for Business that their data will be stored in Germany. Taking these aspects into consideration, the authority's conclusion with respect to minimizing risk seems by no means compelling.

The authority sees the aforementioned risks even in cases where a contract is concluded with these providers directly. Even in that case, it takes the view that additional legal guarantees are required in order to overcome the risk arising from transfers to a third country. In the case of Zoom Video Communications Inc., the authority states that such guarantees have not been provided, at least as of 2 April 2020. The authority does not cite more specific grounds for its decision in this document, but the authority's press release of 31 March 2020 states as follows:

"Note: there are service providers from the US with large market shares which do not meet this requirement because they are not adequately registered or offer the standard contractual clauses only in modified form. As of this printing, one example is Zoom Voice Communications, Inc."

But even from this statement, it is not clear why the Berlin data protection authority finds Zoom's registration under the EU-US Privacy Shield to be inadequate. It is also not evident which defects the authority has identified in the standard contractual clauses used by Zoom. Both of these would be very helpful for controllers to know, since otherwise instructions cannot be issued to Zoom in the processing contract.

**Conclusion**

It is clear from the published documents that the Berlin data protection authority takes the position that services from Microsoft, specifically Teams and Skype, and the Zoom video conferencing solution (the latter updated as of 2 April 2020) do not conform to data protection law. The authority expressly clarifies this point once again in its published checklist, which states as follows:

"We would point that the providers of some widely used products do not satisfy the conditions cited above, including Microsoft, Skype Communications and Zoom Video Communications."
However, since the documents deal both with the legal requirements for the use of video conferencing solutions and with the authority’s recommendations, it is not necessarily the case, in our view, that the authority is taking the position that using these products would violate the law. This interpretation is supported by the fact that the authority merely says that these services "should" be replaced, not that they "must" be replaced, as well as the fact that the authority does not cite any specific defects. Nevertheless, controllers which use the aforementioned services should remain alert. Responses from affected companies and further statements from the Berlin data protection authority may bring further clarity.

[April 2020]