University of Basel

# Data Protection
Video Transcript

**Contract data processing**

[Danielle Kaufmann]: Up to now, we've mostly looked at how a public institution may collect and process data. In some cases however, the data processing is outsourced to third parties. § 7 IDG permits this. However, only the processing of information is affected by this kind of outsourcing: the legal task itself that underlies the data processing is not outsourced, nor is personal data simply disclosed.

But let's start with a basic question: when is it permitted to have data processed by a third party?

Data processing can be outsourced to a third party as long as no legal or contractual provision precludes it. This is regulated in § 7 Para. 1 IDG. So first we have to check whether there are any confidentiality provisions, for example, that would prohibit third-party processing of the data.

The general principle of professional confidentiality from personal law does not necessarily conflict with this. But there may well be other special legal confidentiality provisions that prohibit outsourcing of data processing, for example tax secrecy, victim confidentiality or medical confidentiality. When this is not the case, the data processing can be outsourced to third parties.

What cannot be outsourced, however, is the responsibility that we as a public institution have toward the affected individuals. We are not only responsible when we are processing the data ourselves, but also when we outsource the data processing out to a third party.

This is regulated more detailed in § 7 Para. 1 letter b IDG. It stipulates that the public institution that grants the contract must ensure that the data is processed by the third party in the same way that the public institution itself would be required to. For this reason, the public institution must do three things very carefully.

First, it must be very careful in its selection of the third party to be entrusted with data processing in support of the legal task.

Second, it must provide careful instruction to the third party. For this purpose, we must stipulate in the contract what the third party is permitted to do with the data, and what is not. This includes, for example, not permitting the third party to use the data for their own purposes or to share it with a fourth party. In some cases, we must also stipulate who the third party is allowed to involve, who is permitted access to the personal data, and that they must sign a non-disclosure agreement. We also have to stipulate whether the data is to be returned or destroyed after the contract data processing is complete.

Third and finally, the public institution must carefully monitor how the contract is being carried out while processing is ongoing. We must take on a certain supervisory or monitoring role.

What such a contract looks like will depend, of course, on the kind of data processing that has been contracted. Hosting of a website requires different security measures than analysis of sensitive health data.

University of Basel

For further guidance, the Data Protection Officer of the Canton of Basel-Stadt has published guidelines on contract data processing on their website. It summarizes the key points and provides examples of possible wording for contracts. A link to these guidelines is provided under the video.