Thursday, April 23, 2020 2: Press releases Contact Tracing *with* Data protection by design - seize the opportunity now German Translation "Data protection by design" - this is what the Independent State Center for Data Protection Schleswig-Holstein (ULD) has been campaigning for decades. So far, concepts for innovative data protection technology have mainly been found in academic papers. Although the General Data Protection Regulation requires "data protection through technology design", the ideas have only rarely found their way into practice. For the contact tracing app, “data protection by design” is possible – and necessary. "Contact tracing" is currently being discussed worldwide as one of many building blocks for combating the pandemic, in order to warn people who may have been infected with the novel corona virus. This should also be saved via an app on the smartphone if there was close contact with other people who also use such an app. If it later turns out that one of the people involved in such encounters was infected, the others can be notified via the app - even if you don't know each other. Marit Hansen, the state commissioner for data protection in Schleswig-Holstein, has dealt with the concepts in detail: "Contact tracing works like a kind of digital diary with entries about close contacts on the smartphone, which can be compared later. Such an app can be helpful for containment in addition to other pandemic measures. However, this will only work if the users can have legitimate trust in the app - and "data protection by design" is essential for this. This means, for example, that names and locations are not saved and everything is stored in encrypted form. The crucial question when assessing the risk of misuse is where the data is stored during the comparison and whether this enables additional evaluations – including monitoring.” The architecture of the system is fundamental to the technical development: the contact details are initially only collected from the smartphones of the users. The question is whether the comparison and notification of those who may be affected is carried out via a central server or whether the comparison takes place decentrally in the apps of the users and only the users themselves know the result. This directional dispute "central - decentralized" became particularly clear when, on April 20, 2020, data protection researchers from all over the world, many of whom are involved in various development projects on contact tracing, formulated their conditions for such an app design in an open letter: In particular, a contact tracing app should only serve the purpose of tracing contacts and full transparency and data minimization must be guaranteed. They emphasize that when there are several design options, the one that best guarantees data protection should be chosen. On April 21, 2020, the European Data Protection Board (EDSA), in which the data protection supervisory authorities of the federal and state governments - including Hansen's team - work, made it clear that compliance with data protection regulations is essential. Last but not least, this is important in order to be able to establish legitimate trust in the

population, which is a mandatory prerequisite for the acceptance of a voluntary solution. It is one of the tasks of the national legislature to ensure that this voluntary nature actually exists. Persons who do not want to or cannot use such an application must not suffer any disadvantages as a result. It must also be ensured that processing only takes place for the purposes specified in advance. As with all other such measures, a time limit is also necessary here. Because the use of an app is associated with high risks for the rights and freedoms of data subjects, a data protection impact assessment must be carried out, the publication of which is strongly recommended by the EDPB. Among the numerous conditions listed by the EDPB, as with the data protection researchers, is the demand for the greatest possible transparency. The source code of the application and the backend must be open (open source); likewise, the technical specifications must be published to enable verification. The EDPB emphasizes that the principle of data minimization and the principle of data protection by design must be carefully considered. As in its letter to the European Commission on April 14, 2020, the EDPB notes in this context that the principle of data minimization is better preserved with a decentralized approach. This is also important from Hansen's point of view: "It is important to minimize the risk of identifying the persons concerned - also with regard to unauthorized access, which would affect all participants in the case of central infrastructures. The corresponding know-how and viable concepts are there. Not reaping the fruits of years of research work now and not considering concepts that promote data protection to a large extent through sophisticated technology would be a major oversight." Hansen welcomes the transparency of the work of the data protection researchers to date: "Through the disclosure of concepts, the honest discussion of possible risks and countermeasures and the provision of source code will enable data protection authorities and the interested public to review and further develop the results. It is also important that not everyone works on their own solution in private, but that suitable and data protection-preserving models can function interoperably worldwide. The first steps have been taken: The "data protection by design" experts from various projects have joined forces and are cooperating in the interests of a good overall solution with built-in data protection." Hansen also wants the German Ministry of Health to make a clear commitment to "data protection by design “, data minimization and maximum transparency. Further information: European Data Protection Board (04/14/2020): EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic [external] European Data Protection Board (04/21/2020): Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak [Ext.] Forum Computer Scientists for Peace and Social Responsibility (FIfF) e. V.: Data protection impact assessment for the Corona app (V1.0 from April 14, 2020, several updates)

[External] Data protection researchers on contact tracing: Joint Statement on Contact Tracing (April 20, 2020) [External] "Decentralized Privacy -Preserving Proximity Tracing (DP-3T)" [External] “A Global Coalition for Privacy-First Digital Contact Tracing Protocols to Fight COVID-19 (TCN Coalition)” [External] “Private Automated Contact Tracing” [External] “CovidSafe” [External] The information from the State Commissioner for Data Protection on topics related to the corona pandemic is provided under the following link and updated regularly: https://www.datenschutzzentrum.de/corona/ If you have any questions, please contact: The State Commissioner for Data Protection Schleswig -Holstein

Independent State Center for Data Protection Schleswig-Holstein Holstenstraße 98, 24103 Kiel Tel: 0431 988-1200, Fax: -1223 E-Mail: mail@datenschutzzentrum.de Tags for this article: corona, data protection by design, DSK, news, press releasesArticle with Similar topics: E-prescription procedure: protect machine-readable codes! Property tax reform 2022 - Responsibility of the BfDI No loopholes in communication with authorities and for foundations with public tasks - Further develop the right to freedom of information Announcement - "Save the date!": Summer academy "Freedom of information by design - and data protection?!" on September 12, 2022 in Kiel Data protection and social work in schools – practical knowledge in the new ULD brochure