Donnerstag, 23. April 2020 2: Pressemitteilungen Contact Tracing *with* Privacy by Design - Take the chance now! English Translation of press-release Contact Tracing *mit* Datenschutz by Design - jetzt die Chance nutzen The Independent Centre for Data Protection Schleswig-Holstein (ULD) has been advocating “data protection by design” for decades. Until now, concepts for innovative data protection technology were mainly found in academic papers. Even though the General Data Protection Regulation calls for “data protection by design”, relevant concepts have rarely found their way into practice. When it comes to a so-called “Contact Tracing App”, “data protection by design” is possible - and essential. “Contact tracing” is currently being discussed worldwide as one among many components in the fight against pandemics. Its purpose is to notify people who may have become infected with the novel corona virus. The idea behind such applications is to store the information that a close contact has been made with other people who also use such an application on their smartphone. If it later turns out that one of the people involved was contagious at such encounters, the others can be notified via such an app - even if they do not know each other. Marit Hansen, the State Data Protection Commissioner of Schleswig-Holstein, Germany, has taken a closer look at the concepts: ‘Contact tracing works like a kind of digital diary with entries about close contacts on the smartphone, which can later be matched. Such an app might be helpful to contain the spread of the virus if it is used in addition to other pandemic measures. However, this will only work if such an app can be trusted by its users - and for that, “data protection by design” is essential. This means, for example, that names and location data are not stored and all data are stored in encrypted form. A decisive factor in assessing the risk of fraudulent use is the question of where the data are stored, when they are matched and whether this enables additional analysis, including surveillance.’ The architecture of the system is fundamental. Initially, contact data are only collected on the users' smartphones. The question is whether matching and subsequent notification of those persons potentially affected will be carried out on a central server or whether the matching will be decentralised in the users' apps and only the users themselves will know the result. The dispute between “centralized” and “decentralized” models became evident on 20 April 2020 when data protection researchers from all over the world, many of them involved in various development projects on contact tracing, formulated their requirements for such an app design in an open letter: In particular, a contact tracing app shall only serve the purpose of tracing contacts, ensuring complete transparency and data minimization. They stressed that if several design options are available, the one that guarantees data protection best must be chosen. On 21 April 2020, the European Data Protection Board (EDPB), which is composed of representatives of the national data protection authorities, clearly stated that ‘data protection is indispensable to build trust, create the conditions for social acceptability of any solution' that necessarily has to be carried out on a voluntary basis. It is up to the national legislators to 'incorporate meaningful safeguards including a reference to the voluntary nature of the application' and to ensure that this voluntary approach is actually guaranteed. '[…] additional safeguards should be incorporated, taking into account the nature, scope and purposes of the processing. Finally, the EDPB also recommends including, as soon as practicable, the criteria to determine when the application shall be dismantled […].' '[…] the EDPB considers that a data protection impact assessment (DPIA) must be carried out before implementing such tool as the processing is considered likely high risk [… and] the EDPB strongly recommends the publication of DPIAs.' Furthermore, the EDPB stressed that '"individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all.' Among the numerous conditions listed by the EDSA, the demand for the highest level of transparency can be found, just as it is demanded and practised among data protection researchers. The EDPB states that "the source code of the application and of its backend must be open, and the technical specifications must be made public, so that any concerned party can audit the code, and where relevant, contribute to improving the code, correcting possible bugs and ensuring transparency in the processing of personal data." The EDPB underlines that the principle of data minimisation and the principle of data protection by design must be carefully taken into account. In this context, as already stated in the EDPB's letter to the European Commission from 14 April 2020, the EDPB notes that 'in general, the decentralised solution is more in line with the minimisation principle'. For Hansen this is crucial: 'It is now important to minimize the risk of identifying the data subjects concerned - especially with regard to unauthorized access, which in the case of centralized infrastructures would affect all data subjects participating. The necessary expertise as well as suitable concepts are at hand. It would be deplorable not to harvest the fruits of years of research work and a major oversight to disregard those concepts that enhance data protection through advanced technology to a high degree.' Hansen welcomes the transparency of the data protection researchers' work to date: 'By disclosing concepts, honestly discussing possible risks and countermeasures and providing source code, data protection supervisors and the interested public will be able to assess and further develop the results. It is also important that not everyone is working on their own solution in isolation. Instead, it has to be ensured that suitable models that respect data protection can function interoperably worldwide. The first steps towards this have been taken: "Data protection by design" experts from various projects have joined forces and are cooperating in the interests of a good comprehensive solution with built-in data protection.' Hansen would also like to see a clear commitment from the German Ministry of Health to "data protection by design", data minimization and maximum transparency.   For further Information: EDPB (14 April 2020): Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic [Extern] EDPB (21 April 2020): Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak [Extern] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V.: Data Protection Impact Assessment fort he Corona App (Version 1.5 – 24 April 2020) [Extern] Data protection researchers on contact tracing: Joint Statement on Contact Tracing (20 April 2020) [Extern] “Decentralized Privacy-Preserving Proximity Tracing (DP-3T)” [Extern] “A Global Coalition for Privacy-First Digital Contact Tracing Protocols to Fight COVID-19 (TCN Coalition)” [Extern] “Private Automated Contact Tracing” [Extern] “CovidSafe” [Extern]   The State Data Protection Commissioner of Schleswig-Holstein Independent Centre for Data Protection Schleswig-Holstein Holstenstraße 98, D-24103 Kiel Phone: +49 431 988-1200, Fax: -1223 Email: mail@datenschutzzentrum.de   Tags für diesen Artikel: corona, data protection by design, pressemitteilungenArtikel mit ähnlichen Themen: E-Rezept-Verfahren: maschinenlesbare Codes schützen! Keine Schlupflöcher bei Behördenkommunikation und für Stiftungen mit öffentlichen Aufgaben – Recht auf Informationsfreiheit weiterentwickeln Ankündigung – „Save the date!“: Sommerakademie „Informationsfreiheit by Design – und der Datenschutz?!“ am 12. September 2022 in Kiel Datenschutz und Sozialarbeit in Schulen – Praxiswissen in neuer Broschüre des ULD Gutachten zu Facebook-Fanpages: Betrieb noch immer nicht datenschutzkonform – der öffentliche Bereich muss handeln