Tuesday, June 11, 2019 2: Press releases For future-proof digitization Promote information security instead of sabotaging it - an appeal on the occasion of the conference of interior ministers in June 2019 in Kiel The federal and state interior ministers will meet in Kiel from June 12 to 14, 2019. From a data protection point of view, the reports of the last few days about plans by security authorities to facilitate access to encrypted communication via messenger applications and to data in the smart home are problematic. For Marit Hansen, the state commissioner for data protection in Schleswig-Holstein, this is reason to warn: "What is more or less bluntly demanded here are built-in back doors in hardware and software, which the security authorities should use for their access. Such ideas are not compatible with the fundamental right to guarantee confidentiality and integrity of information technology systems, as determined by the Federal Constitutional Court. For decades, IT security experts have been demanding that manufacturers urgently increase the security level of the technology used in our information society, instead of undermining it through legal coercion. Because nothing else happens when back doors or targeted vulnerabilities are implemented: Unauthorized persons can then access as well as authorized persons - and e.g. E.g. recording the communication or copying, deleting, changing or even deliberately substituting data." At the beginning of 2019, personal data about politicians and other celebrities that had been collected with the help of Internet attacks was published. This doxing scandal briefly fueled the discussion about more encryption and better access protection. At this point it was almost forgotten that a few years ago the federal government – probably as a reaction to the Snowden revelations – had issued the route: "Germany will be the No. 1 encryption location" (see https://www.krypto-charta.de /). The federal government has made little progress on the way to this noble goal in recent years and now even seems to be taking a wrong turn, because the push from the Federal Ministry of the Interior is going in the opposite direction. Hansen explains: "When more and more messengers finally offered end-to-end encryption, I saw this as a big step towards more information security and data protection. Data protection "by design" - this is also required by the General Data Protection Regulation! But apparently the providers should be obliged to be able to provide unencrypted chats and telephone calls. But that would only work if the important end-to-end encryption was torpedoed with predetermined breaking points. There can then no longer be any question of real security. "Hansen considers the decision of the Ministers of Justice Conference from last week on the new 5G mobile communications standard, which finally has an improved security standard so that eavesdropping is not easily possible – actually, to be just as critical. Because the majority of the state justice ministers are calling for a softening in order to continue to allow technical attacks, against which the new standard is actually intended to protect. These so-called Stingray attacks (also "IMSI catchers")

can neither be specifically limited to suspicious persons, nor can their use be restricted to criminal prosecution. Rather, all end devices in the vicinity of the attack are always affected. The emergency call functions are also interrupted. Confidentiality and integrity of the IT systems used for personal communication (mobile phones are no different these days) in 5G networks is not guaranteed in this way, but massively undermined for all users. Hansen sees great added value in state-of-the-art encryption: “The digitized world will require a strong foundation for information security. Confidential communication and reliable data processing must be guaranteed. This is independent of whether data is exchanged in networked driving, in telemedicine or in Industry 4.0 applications, or whether smart homes for private households or smart cities are controlled for the common good. One does not have to be a prophet to predict that the use of backdoors and weak points cannot be limited to state actors for legitimate actions. Such an idea does not protect against crime, but on the contrary opens up further opportunities for criminal activity.” Hansen appeals to the ministers, manufacturers and standardization bodies to implement more data protection and information security instead of sabotaging the advances in secure technology that have been achieved so far. If you have any questions, please contact: The State Commissioner for Data Protection Schleswig-Holstein

Independent State Center for Data Protection Schleswig-Holstein Holstenstr. 98, 24103 Kiel Tel: 0431 988-1200, Fax: -1223 E-Mail: mail@datenschutzzentrum.de Tags for this article: news, press releasesArticles 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