

Tuesday, March 30, 2021 2: Press releases Data protection report for 2021: With more data protection to better solutions - also in the pandemic Marit Hansen presenting the 39th activity report Marit Hansen, the state representative for data protection Schleswig-Holstein, has her activity report for presented the year 2020. The report covers a wide range of data protection and freedom of information issues. One focus of the work resulted from the corona pandemic - this is shown by the different aspects of fighting the pandemic and digitization. Overall, numerous complaints and data breach reports make it clear that many organizations still have some catching up to do in the area of data protection and information security. 39th activity report of the ULD Hansen's summary for the year 2020: "More complaints again, more data breaches, and above all more attacks on data protection. A widespread misunderstanding needs to be cleared up here: data protection does not prevent the fight against a pandemic! Data protection is particularly important in times of crisis. In the ongoing pandemic situation, it is even particularly relevant that data protection is not perceived as an annoying and dispensable appendage, but is considered and built in right from the start. Anyone who does not do so not only risks breakdowns or misuse of data, but also jeopardizes all trust." Hansen is annoyed by the prejudice that data protection would prevent necessary data processing: "Like the alleged – and often talked up – conflicts in specific cases in the short term in practice that can be resolved and where improvements need to be made is a focus of our work." The "corona topic of the year" runs through the activity report: On the one hand, it dealt with measures such as questionnaires, temperature measurement or recording contact details at the entrance, procedures for measuring a high density of people or the data protection concept the Corona Warn App, which, in an exemplary manner, manages without naming names and locations. On the other hand, the employees of the ULD had to deal with numerous inquiries about the use of technology and rules in the home office, in home schooling and in online sessions. The guidelines of the ULD "Data protection: Suddenly in the home office - what now?" and "Suddenly video conference - and data protection?" came at the right time to offer assistance. Paragraphs 4.1.1, 4.1.2, 4.3.2, 5.3, 5.4.1, 5.4.2, 5.4.3, 7.1, 8.1, 6.3.3

Nevertheless, data breaches and data leaks were not absent: The activity report contains descriptions of cases in which the data protection requirements were not met, for example data leaks or intentional misconduct when working from home or when using contact data. Areas such as the "perennial" video surveillance, the protection of patient confidentiality, employee data protection, police data processing or the analysis of data security deficiencies also take up a large part of the work of the ULD in addition to the topics of freedom of information. Overall, the number of complaints (1,219 written complaints in own

responsibility, increase of 27%) and the data leaks reported to the ULD (406 reports, increase of 16%) have increased again.

Data breaches: Paragraphs 4.1.11, 4.1.12, 4.5.8, 4.5.9, 4.5.10, 4.5.11, 5.5.1, 5.5.2, 5.5.3

As expected, the year 2020 brought a boost for digitization due to the corona pandemic - this was reflected, for example, in the increased use of technology for working from home and via video conference. This did not always work without problems. It was to be expected that data breaches in the home office would increase if the computers used were not integrated into the secure infrastructure of the organization. The numbers of reported data breaches also show a slight increase in this area. However, Hansen suspects that there were many more incidents that did not become known because employees did not inform their employers about small mishaps and perhaps did not even know that there was an obligation to report them. At the latest, it becomes critical when employees actively circumvent the security measures of their organization in order to be able to work from home: In one case, an employee installed a program for remote use on a branch's service computers in order to be able to access them from outside. Without the knowledge of his employer, he had put himself in the home office. He forwarded customer e-mails to his private e-mail address. On the one hand, customer data left the secure area of the company, on the other hand, no unauthorized remote access options could be created that could possibly be exploited by third parties. Hansen therefore warns against circumvention strategies: "A data protection-compliant and secure procedure must be established at the workplaces that are suitable for working from home. Security requirements must not be tunnelled."

The obligation introduced by the Corona Control Ordinance for restaurateurs and organizers, for example, to collect the contact details of their guests also led to many questions and problems, because not everyone understood that this data was only used for the purpose of contact tracing and was to be released at the request of the health department. but otherwise had to be protected against unauthorized access. Typical privacy violations and sloppiness included lists laid out where each guest could see the details of previous visitors, collecting additional information, and using it for purposes other than intended: for marketing campaigns, for making personal contact with a Complaint and even for attempts to flirt via messenger. Contact data collection: Items 5.3, 5.4.1, 5.4.2

Most of the cases investigated by the ULD were not intentional violations, but those responsible did not realize what their obligations were or had forgotten to take care of compliance with data protection requirements. This includes, for example, the case "When professional firefighters become movie stars": It was thought that it would be a good idea to have firefighters accompanied by a film team and equipped with bodycams from the film company. However, in a real fire brigade operation,

you cannot ask the people to be rescued for their consent to the recording and subsequent publication. A legal basis for the filming could not be named; We have pointed out that the film company's bodycams may not be used. Firefighters as movie stars: Paragraph 4.1.8

However, there are always cases in which data protection violations are part of the business model or happen intentionally. An example of intentional activity is covert video surveillance, some of which is reported to the ULD each year, for example in locker rooms, toilets or during medical examinations. Because the secret creation of video recordings can be a criminal offence, the ULD has to hand over these proceedings to the public prosecutor's office. Covert video surveillance: Paragraph 5.6

If complaints accumulate in an industry, the ULD carries out similar checks if possible - this is also the case in the case of advertising campaigns by dating agencies: Hardly anyone appreciates receiving unsolicited e-mail advertising. If these e-mails also come from dating agencies, some people start to ponder how they ended up on the mailing list and what data is collected there about you. This is hardly comprehensible for the recipient. In the cases of complaints that the ULD investigated, it was also not clear who the recipients could contact to assert their right to information or to object to the processing. For this reason, eight dating agencies in Schleswig-Holstein were examined that carried out such advertising measures with the help of commissioned service providers such as list brokers. Numerous deficiencies were found here, which in many cases led to the termination of cooperation with the list brokers. In individual cases, the ULD also had to enforce the provision of information with coercive measures. Examination of dating agencies: Paragraph 5.2

Cases in which processors promise a high level of information security but are then unable to fulfill this are also critical. Rapid remedial action is required here: Any data protection deficiencies at the service provider mean that the client cannot meet their accountability. The condition is always that the risks are controlled in accordance with the protection requirement and that this can also be proven. In such cases, it may be necessary for the supervisory authority to prohibit the processing of personal data. (In)security in the data center: Note 4.1.10

However, Hansen does not find it reassuring that most of the violations found in Schleswig-Holstein are probably not intentional: "If data misuse is caused by the fact that the companies or authorities do not know their obligations or do not have sufficient competence to manage the risks of their Having data processing under control is not a good sign. Digitization requires professionalism and a well-planned approach." This is where the on-site data protection officers can help. However,

this work is not easy: For some time now, there has been a great deal of dissatisfaction with the situation in the form of verbal abuse of data protection and those who represent it, i.e. the supervisory authorities and the official and company data protection officers who are doing their job. This is not easy in a world in which data protection requirements are often not sufficiently taken into account in the development and operation of information technology. The failure to design a data protection-compliant system – which those responsible must demand – must not be blamed on the official and company data protection officers, who advise correctly in accordance with the legal regulations and the highest court decisions. For example, ECJ ruling on the Privacy Shield: Sections 2.5, 11.5

Facebook fan pages: Note 7.2

Hansen comments: “I am concerned that in some cases the work of local data protection officers is being made difficult and that they are being attacked for their opinions. It's not OK. For a good level of data protection across the board, we need competent and motivated official and company data protection officers.” Helpful information Even if the mass of complaints and data breaches ties up a large part of the resources of the data protection supervisory authority, the ULD tries to deal with the seemingly complex topic of the data protection authority for typical questions and issues To explain data protection in a practical way and to provide information on data protection-compliant design, for example in the handouts for working from home and video conferences and the brochures of the practice series, which are available online. The activity report also contains specific tips on the technical design of confirmation e-mails for online forms, on blacking out digital documents and on integrating maps on websites without data being passed on to third parties. Confirmation e-mails: Section 10.1

Redaction: Section 10.3

Map services: Item 10.5

The publications of the ULD also help in the area of freedom of information. The information access right, according to which any person can consult information held by public authorities, does not seem to be known to all public bodies yet, or has failed to introduce the working processes to fulfill the legal obligation. The petitioners who contact the ULD therefore complain about the lack of replies or incomprehensible refusals of their requests for information. A topic in high demand in 2020 was information on the corona pandemic. Freedom of information - TOP 5 of the complaints: Paragraph 12.2

Looking to the future One instrument of the General Data Protection Regulation has still not been filled with life: certification.

Here, however, the certification working group, headed by the ULD, has laid the foundation for certification bodies to be

accredited. Certifications according to the General Data Protection Regulation will probably play a role in future when choosing service providers and also in international data transfer. Certification: Paragraph 9.3

With the certification, the built-in data protection – through technology design and data protection-friendly default settings – will hopefully become more important. Hansen considers the topic to be urgent: “The dependency on technology has increased in recent years, data about us and our behavior is collected in all sorts of places, and digital sovereignty has so far only been wishful thinking. Digitization must be fair, not desolate. Current political ideas about installing back doors and weakening encryption are also of concern - this is the wrong way. We need more data protection and security, as required by the General Data Protection Regulation.” Digital sovereignty: Paragraph 2.1

Encryption: Section 2.2

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 Data protection report for 2020: facts and figures In 2020, the ULD based on

Complaints from data subjects under their own responsibility 1,219 procedures initiated. This means an increase of 27%

compared to the previous year (959 initiated procedures under own responsibility). The proportion of complaints in the public area was around one third, the majority related to the non-public area (primarily data processing by companies). Another part

of the complaints received was passed on to other supervisory authorities due to the ULD's lack of responsibility. Complaints processed in 2020 In addition, 406 data breaches were reported to the ULD in accordance with Article 33 of the General Data

Protection Regulation. Compared to the previous year, the average number of reported data breaches per month has

increased from 29.1 to an average of 33.8 cases. This corresponds to an increase of 16%. Reports processed according to

Art. 33 GDPR In addition, the number of consultations in 2020 rose from 759 in the previous year to 808. This corresponds to an increase of almost 7%. Tags for this article: news, press releases, uldArticles 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