

## State commissioner publishes data protection activity report 2020

Today, the state commissioner for data protection and the right to inspect files, Dagmar Hartge, is presenting her activity report on data protection for 2020.

The past year was also and especially in the area of data protection marked by the challenges of the corona pandemic. Last but not least, the sudden upswing for digitization in very different areas of life is also reflected in the activity report. Dagmar Hartge:

There is no question that pragmatic solutions are needed during a pandemic to keep society, the economy and the state running. At the same time, citizens expect their fundamental right to data protection to be protected. The results of numerous complaints and consultations from the past year show me that this balancing act is worthwhile. Including data protection in the solutions from the outset also prevents time-consuming subsequent improvements.

While the digital instruments for tracing contacts are currently being discussed, last spring and summer the focus was on the analogue collection of contact data. Numerous visitors complained about open Corona guest lists. The results of an inspection in over 50 Brandenburg restaurants were sobering: In 30 cases, more data was collected than was required and in 36 cases, cafés and restaurants did not implement the deletion deadline or did not implement it in time. In individual cases, companies used the collected contact data for their own advertising purposes in violation of the regulations (A I 2, page 16). The use of guest lists to track administrative offenses that had nothing to do with containing the pandemic was disproportionate.

Specifically, it was about the use of the contact details for the imposition of a warning fine on the basis of the forest law of the state of Brandenburg. The occasion was a birthday party with 50 guests in the forest (A I 3, page 18).

The basis for recording the contact details of guests were the various Corona regulations of the state government. The state commissioner worked early on to ensure that the principle of data economy was taken into account. For example, she recommended dropping the term "attendance list" in favor of "proof of attendance" to make it clear that the data was recorded on individual sheets. This made it easier to prevent unauthorized persons from viewing the data and the deletion deadlines for the recorded data could be implemented in the first place. The Ministry for Social Affairs, Health, Integration and Consumer Protection has implemented this advice and also made it clear in the ordinance that the proof of attendance is to be used exclusively for the purpose of providing information to the health department (A I 1, page 14).

Most schools were completely unprepared for the challenge of implementing distance learning overnight. School authorities and teachers had to improvise and the students and their parents were confronted with new challenges almost every day. Some schools used Microsoft cloud solutions to keep classes going under pandemic conditions. In some cases, they continued to do so even after a serious data breach had occurred in some cases. As a result, the state commissioner did not consider this to be permissible. Neither was it possible for students or teachers to agree to the processing of their personal data - consent would have been voluntary and lacking in information. The responsible bodies were still able to prove the necessary data protection-compliant contract with the service provider for order processing. It was also completely unclear which data was transmitted to the manufacturer and what Microsoft intended to do with it (A IV 5, page 72). Dagmar Hartge: From my point of view, there is no reason to rely on commercial learning platforms that cannot be used in a permissible manner. Finally, with the Brandenburg school cloud, there is a nationwide and data protection-compliant alternative. I can only appeal to all schools that are not yet participating to take advantage of this offer.

The need to reduce personal contacts led to an unprecedented boom in video conferencing during the reporting period. In addition to complaints about the use of certain products, we also received numerous requests for advice. Many expected concrete product recommendations from the state representative, which are not part of our tasks. However, the state representative participated in the development of an orientation guide for the data protection conference on the use of video conference systems. As a result, solutions that are based on your own existing IT infrastructure are recommended. It is also possible to commission a service provider, but only providers based in Europe should be selected. The regulations for order data processing must be observed. Video conferencing services that are easily accessible on the Internet are usually to be viewed critically from a data protection point of view. In any case, the respective office remains responsible for compliance with data protection and must ensure and document this before using the programs. (A I 6, page 26). In this sense, the state representative also advised the state universities and technical colleges of the state of Brandenburg after she had obtained an overview of the programs used for online teaching in a survey there. This year we will check to what extent the universities have followed our advice (A I 7, page 28).

The European Court of Justice has again set the course for greater consideration of European data protection in the context of international data processing. With the "Schrems II judgment" he declared a key basis for data transmission to the USA - the EU-US Privacy Shield - to be invalid. If the protection of the data required by Union law cannot be guaranteed, its transmission

must be terminated. Otherwise, as a supervisory authority, we are obliged to prohibit the transmission according to the judgment of the European Court of Justice. Companies and associations are therefore faced with major challenges. The state representative advised many of them during the reporting period (AV 2, page 106). The effects of the judgment were also the subject of their consultations with schools and universities in connection with the use of learning platforms and video conferencing systems.

The state representative was also involved with many other pandemic-related issues. For example, we advised a non-profit company on the development of cloud-based health applications. This involved the collection of anamnesis data when patients were admitted in connection with Corona and the development of a symptom diary (A I 4, page 20). In order to support companies and authorities in the data protection-compliant implementation of home work, we have summarized and published the most important requirements and the resulting technical and organizational measures for the processing of personal data in the context of home work (A I 5, page 22). The state commissioner issued a warning to the investment bank because it did not use sufficient encryption of e-mail communication when implementing the procedure for submitting applications for Corona emergency aid, collected some data that was not required and also provided insufficient information about data processing (A II 3, page 40).

As in previous years, video surveillance was once again a long-running issue of data protection in the reporting period. The number of written inquiries and complaints about this increased from 42 in 2014 to 190 in 2020. The number of cameras we checked also increased again (A VI 2, page 113). The State Chancellery of the State of Brandenburg drew special attention to the topic. As part of the four-week unit EXPO on the occasion of the 30th anniversary of German unity, she had several exhibits in downtown Potsdam monitored by video cameras to protect against destruction and to enforce the pandemic-related distance requirement. While night-time operation of the cameras would have been permissible, the State Chancellery used the cameras mainly all day long and observed large areas. There was initially no adequate signage that would have pointed this out. There was also no documentation from which the justification for the video surveillance and the technical measures to protect the use of the camera in accordance with data protection law should have emerged. The State Chancellery ignored the requirements of the data protection supervisory authority or only implemented them half-heartedly. As a result, the state commissioner issued a warning. Instead of video surveillance, there would have been less intrusive means. Greater weight was attached to the legitimate interests of the citizens captured by the cameras (A II 2, page 37).

The fact that cameras do not only appear as permanently installed technology was shown by the use of drones by a real estate company. To improve the marketing of a property, it had drones fly over the neighborhood and take aerial photographs. The adjoining properties could also be seen in the pictures published by the company on its website – including the neighbours' private gardens and sun terraces. Such use of drones with cameras was already illegal under aviation law. He was also not required under data protection law and inadmissibly interfered with the rights of the neighbors. The company voluntarily deleted the footage from its website. The State Commissioner therefore only issued a formal legal notice to clarify the legal situation (A IV 3, page 67).

Numerous complaints were received as part of the implementation of the Measles Protection Act, which came into force in the reporting period. Among other things, the law stipulates that schoolchildren must provide proof of adequate vaccination protection against measles. In practice, copies of the vaccination cards were sometimes simply placed in the student file for this purpose. Such data storage is not permitted, the data volume of the evidence usually exceeds the required level. Against the background of many complaints and inquiries, we supported the state school authorities in developing appropriate information for the schools (A IV 1, page 64).

One of the most important data subject rights contained in the General Data Protection Regulation is the right to information about the processing of personal data. It is an indispensable prerequisite for the exercise of further claims such as the right to correction, deletion or objection. A complainant initially tried unsuccessfully to obtain information about the data stored about him from a debt collection service provider. After our intervention, it turned out that the company had assumed that it was a question of a request for creditworthiness information, which could not be given due to the lack of a creditworthiness assessment of the person concerned. It was only when you searched in a completely different area of the company that you found the applicant's data, namely data from a debt collection process. The information was finally provided and the company agreed to train all employees on this topic (A II 6, page 45). In another case, however, the state commissioner issued a warning to a car rental company. The latter refused to provide information about the origin of his data to a driver who had offered a rental vehicle as a replacement for an accident vehicle. Without further inquiry, it justified this with the unproven authorization of the motorist's lawyer working on the matter (A II 7, page 47).

The fact that it is not enough to protect the internal computer systems was shown by the case of a nationwide aid and welfare organization whose website turned out to be a gateway into their databases. The reason was a security gap in the content

management system that made the unauthorized attack possible. The database contained personal data that had been collected via a registration form on the website. The number of personal data affected by the unauthorized access was in the hundreds of thousands, some of which also contained information on the state of health. The complex organizational structure of the facility and the commissioning of external service providers made it considerably more difficult to clarify the matter. The state commissioner is currently examining the initiation of administrative offense proceedings (A IV 6, page 76).

During the reporting period, the state representative dealt with the data protection-compliant use of e-mail communication just as intensively as with the provision of information. In her activity report, she describes three cases in which the IT systems of companies were attacked by malware and ransomware. In each case, insufficient technical and organizational protective measures were the cause of the infections and thus of the violations of data protection. It is also important to sensitize employees to deal critically with e-mail attachments or Internet links sent in e-mails (A IV 9.1, page 82). The sending of unencrypted e-mails is also often reported to us as a data breach notification - especially if the message was sent to the wrong address and contained sensitive information. In the reporting period, the state commissioner asked the Brandenburg youth welfare offices to use end-to-end encryption for the transmission of particularly sensitive social data. In our circular, we explained concrete assistance and recommended training to raise employee awareness (A IV 9.3, page 86). Sending with open mailing lists is just as common as sending e-mails incorrectly. The danger here is not so much in the particularly sensitive data, but rather in the potentially very high number of people affected. We recommend making the careless use of the CC function more difficult in advance, for example by implementing a warning message in the e-mail program or by ensuring a four-eyes principle depending on the size of the recipient group (A IV 9.2, page 84).

There is good news about the automated number plate recognition process KESY on Brandenburg autobahns. The license plates stored in connection with investigations up to June 2019 (old data) were ultimately deleted. In addition, the police headquarters has taken a number of measures to restrict the accumulation of license plate data and its use in the future (B 2.2, page 128). The further development of the process is associated with a comprehensive redesign. It takes into account the essential requirements of the state representatives with regard to data separation and data deletion as well as differentiated access rights. Nevertheless, the submission of the security concept and a revised version of the data protection impact assessment, which we criticized in the first draft, was still pending at the end of the year (B 2.3, page 131). Irrespective of this, in our opinion there is no legal basis for automated license plate recognition in recording mode from the outset.

Against this background, the federal government has proposed a legal regulation for license plate searches for criminal proceedings. She wanted to limit the procedure to the search mode (storing only the hits) in a proportionate manner. The draft law is being discussed in the Bundestag and Bundesrat. In the state chamber, however, the state government once again advocated a regulation that would allow the further recording of all passing vehicles. Dagmar Hartge:

I am also of the opinion that continuous operation of the automated number plate search in recording mode represents a disproportionate encroachment on the right to informational self-determination. It remains to be seen whether the legislative process at federal level will come to the same conclusion. In any case, legal certainty is finally needed.

Since January 1, 2021, the statutory health insurance companies have been obliged to offer the insured an electronic patient file. The patient data protection law regulates the implementation of this project and was passed by the German Bundestag in the reporting period without taking into account the criticism of data protectionists and the Bundesrat. In essence, it is u. a. In the first implementation phase, patients are faced with the decision of either making all electronic documents known to all those treating them or none at all. A way of assigning differentiated access rights is required here. A year ago, the state representative issued a warning regarding authorization management to both of the health insurance companies under their supervision (A II 1, page 34).

Another project that was decided at federal level, but will also have significant effects in the state of Brandenburg, is the Register Modernization Act. With this law, the tax identification number is introduced as an overarching classification feature for particularly relevant registers in order to be able to offer digital administrative services in a citizen-friendly manner. In view of its wide range of uses, the identification number is nothing more than a personal identification number, the inadmissibility of which the Federal Constitutional Court had already determined in its census judgment. In a later decision, the Federal Fiscal Court also emphasized the earmarking of the tax identification number for tax purposes only. The data protection conference's suggestions for improvement and alternatives did not get through. The German Bundestag passed the law during the reporting period. At the working level, we campaigned until the very end for a data protection-compliant register modernization (AV 1.1, page 92).

Overall, the employees of the state representatives processed 1,322 complaints from natural persons in the past year - in the previous year there were still 878 (A VI 1, page 112). The number of consultations for private individuals, administrations and companies has increased by more than 50% year-on-year (A VI 3, page 115). While we still had 362 reports of data protection

violations to process in 2019, we already received 409 such reports in the reporting period (A VI 4, page 115). More than half of these related to the incorrect dispatch of documents. The relatively high proportion of technical defects that were the reason for a report shows that companies and administrations are still required to take technical and organizational measures to protect personal data and keep them up to date, for example to ward off digital attacks. In 37 cases, the state commissioner made use of powers such as warnings, warnings or orders (A VI 5.1, page 118). Dagmar Hartge:

The renewed increase in the number of complaints and consultations makes it clear that citizens are very consciously demanding their fundamental right to data protection in times of a pandemic. At the same time, the associated workload makes it clear that my authority has reached the edge of its capacity in the past year. The prioritization of cases has meant that more and more complainants have to wait significantly longer for an answer. The fact that we were able to manage the work despite the organizational challenges caused by the corona-related restrictions is the result of the commitment of my employees. They have now reached their stress limit in many areas of work. I would like to take this opportunity to expressly thank you.

The number of administrative offense proceedings rose from 47 to 70 in the reporting period (A VI 5.2, page 119 and A II 8, page 49). The largest part was forwarded by the responsible police authorities or public prosecutor's offices to the fines office of the state commissioners. In 16 cases, the state commissioner imposed a fine; the total amount of fines imposed was 331,200 euros. For example, the operator of a ballet school had published pictures of underage dance students on the Internet without prior written consent. In another case, a doctor's assistant used a patient's telephone number stored in the practice for the purpose of making private contact - an approach that not only displeased the wife of the person concerned. Finally, private curiosity motivated a police officer to inquire about official information systems about the data of a prominent citizen of Potsdam.

The state representative, Dagmar Hartge, presented her activity report to the President of the Brandenburg state parliament, Prof. Dr. Ulrike Liedtke, presented.

ID number 04/2021

Date 03.05.2021

Responsible: Sven Müller, Poststelle@LDA.Brandenburg.de

ID number 04/2021

Date 03.05.2021

Responsible: Sven Müller, [Poststelle@LDA.Brandenburg.de](mailto:Poststelle@LDA.Brandenburg.de)