03/24/2020 | 03/2020

State commissioner publishes data protection activity report 2019

The state commissioner for data protection and the right to inspect files, Dagmar Hartge, published her activity report on data protection for 2019 today. It is the first report since the introduction of the General Data Protection Regulation that covers a full calendar year.

In 2019, the State Commissioner received 878 complaints from individuals who believed that the processing of their data violated data protection law. In over 400 cases, we provided written advice to private individuals as well as to administrations and companies. In twenty cases, the state commissioner made use of powers that are available to her independently of the fines (warning, warning, instruction/order). We received 362 data breach reports. More than half of these related to errors in sending documents or emails. In ten cases, more than 1,000 people were affected by the data breaches (AV, page 87).

Dagmar Hartge:

It is true that the processing of reports of data protection violations already represents a considerable effort for my authority. Despite the high number of reports, I assume that this is only the tip of the iceberg. Those responsible who fail to report reports, submit them incompletely or late, or who do not inform the persons concerned despite the high risk involved, risk a fine.

In 2019, too, citizens complained to a large extent about video surveillance. In her report, the state commissioner describes the case of a cultural and commercial center whose property management has used cameras on a large scale (A I 5, page 22). In addition to a butcher's shop and a car repair shop, there was also a discotheque and a theater in their area of coverage - and with them the visitors. The property management justified the prevention of theft and damage to property, but was only able to justify this with a legitimate interest in the case of two cameras. We prohibited the operation of the remaining cameras. This differentiated approach was consistent with the case law of the highest court. During the reporting period, the Federal Administrative Court had confirmed an order by the state commissioner to align the camera in a dental practice in accordance with data protection regulations (A I 4, page 19). The dentist justified her cameras with medical emergencies, the prevention of criminal offenses and savings in personnel costs. The Federal Administrative Court, on the other hand, emphasized the need to first consider milder means that serve the same purpose. In particular, it found that cost savings alone cannot justify the admissibility of video surveillance.

The fact that digitization affects almost all areas of life is also confirmed in schools in Brandenburg. Online learning platforms, so-called school clouds, are increasingly being used there (A II 2, page 36). The Hasso Plattner Institute has taken over the central piloting of a corresponding project. In cooperation with us, it provided the participating schools with templates for the necessary data protection documents for using the school cloud. As part of this constructive cooperation, the state representative was able to achieve a high level of sensitivity to data protection. Nevertheless, we have recommended only including external providers of learning content if they themselves meet the data protection requirements. Our tests on the part of some schools also revealed some implementation deficits. However, the voluntary consent of the students or their parents to data processing, which is still necessary, seemed more problematic to us. If this is revoked, the children and young people concerned may no longer use the school cloud. This result is not practical. We have therefore suggested to the legislature that an authorization norm for the use of online learning platforms be anchored in the Brandenburg School Act.

In some public election announcements, the full address of the candidate may no longer be given, only his or her place of residence (A II 3, page 38). This is now regulated in two ordinances, which the state government had changed as a result of our suggestion. Nevertheless, numerous municipalities continued to publish the full addresses of the candidates, especially in the context of municipal elections. To mark this occasion, we conducted a survey among the communities and asked them to review their publication practices. The reason for continuing the previous practice turned out to be simply ignorance of the new regulations. Dagmar Hartge:

Against the background of various threats to local politicians, the required refraining from publishing the full addresses of election candidates is of current importance. The regulation shows that data protection is not an abstract legal interest, but rather guarantees the protection of individuals. It is therefore a very specific prerequisite for social commitment.

Anyone who processes personal data must inform those affected at the time of data collection about the type of processing and their rights. On the one hand, this is a core regulation of the new data protection law, on the other hand, many patients will have already experienced that doctors deal with these information obligations in very different ways. When we checked the data protection information in selected medical practices, we saw this assumption as confirmed (A II 4, page 40). In some cases, those treated should confirm that they have taken note of the information by signing it - this is not legally required. Information about data processing was also often inadmissibly mixed up with consent. In most cases, however, there is no need to request a declaration of consent at all. The authorization for data processing for treatment purposes results in principle

from an existing contractual relationship. After all, those affected cannot object to medical documentation. As a result, the state representative was able to achieve a welcome sensitization to questions of data protection in medical practices through their examination.

To ensure security in the immigration office, one district used a private security company. As it turned out during an unannounced on-site inspection, the company already carried out a kind of "admission control" at the entrance and had the visitors' IDs shown to them. The security guard took personal documents several times, disappeared for a few minutes to copy them and handed over previously received documents to the responsible clerks. There was therefore a thoroughly intensive division of labor between the authorities and security guards (A III 2, page 49). However, only the responsible clerks were authorized to process the personal data of foreigners. It is obvious that this division of labor was inadmissible under data protection law. We have since issued a warning to the district.

As part of the mandatory reporting of a data breach, a Brandenburg company informed us that its website had been compromised by malware (A III 5, page 53). Visitors to the website risked having their computers misused for complicated calculations in the context of digital currencies. The cause of the incident was a missed software update. At the time of the notification, the software for providing and maintaining the website had not been updated for almost two years. The contract with an external IT service provider had expired a year ago. In the meantime, the company hadn't bothered to update the software anymore. It only concluded a contract for order processing with the new service provider at our express request. The fine office at the state commissioner initiated administrative offense proceedings due to the lack of technical and organizational measures and the lack of care in the design of the order processing. Dagmar Hartge:

Regular software updates are not optional as a technical measure, but an absolute must. This applies all the more if the computers on which such programs run are connected to the Internet and are therefore exposed to the risk of attacks with malware. Updating operating and content management systems protects companies and administrations as well as private individuals from nasty surprises.

In the past year, the fines office of the state commissioner conducted 47 administrative offense proceedings - twice as many as in the previous year (A I 8, page 27 and V 4.2, page 91). About half of them had to be evaluated according to the new legal situation. 24 procedures ended with the imposition of a fine. They were still largely based on the old legal situation, since the administrative offenses committed had mostly been ended before the introduction of the General Data Protection Regulation.

In total, the fines office imposed fines of 69,150 euros in 2019. For example, the operator of a swimming pool illegally monitored guests and employees with a video camera and violated other data protection obligations. Another company used a service provider to provide data subjects with information about the data processed about them. It failed to conclude in writing the contract for order processing that is obligatory for such cases. Aggravating came u. added that the information was given under the logo of the service provider and it was therefore not possible to identify the connection between the service provider and the company. The fine office conducted another procedure against a doctor who commissioned an acquaintance to back up patient and employee data from his doctor's office. He saved the data entrusted to him on his computer at work, where the employer finally discovered them. The physician remained responsible for this incident.

On June 22, 2019, the Brandenburg Police, Prison and Correctional Measures Data Protection Act came into force. This cumbersome designation hides the implementation of a European directive that regulates data protection for the legal areas of police action, penal systems and penal institutions. The General Data Protection Regulation does not apply here. The law mentioned contains an independent, annual reporting obligation for the state commissioners, which we are complying with for the first time at the same time as the report on general data protection law (B 3, page 98).

In the field of police work, automatic license plate recognition (KESY) was the focus of the data protection supervisory authority (B 3, page 100). The stumbling block was the rather coincidental announcement in spring 2019 of the comprehensive and long-lasting recording of license plates on Brandenburg motorways in recording mode. As a result of a comprehensive examination of the procedure operated by the Brandenburg police, the state commissioner initially complained to the police headquarters about the violation of the duty to provide support. It had refused to submit to us the resolutions and orders required for an examination. In the further course, we also complained about the violations of data protection law. In particular, the provision of Section 100h Paragraph 1 Sentence 1 No. 2 of the Code of Criminal Procedure used by the police does not, in our opinion, constitute a sufficient legal basis for the use of automated license plate recognition. In addition, other serious data protection deficiencies were identified. The police did not delete the data that was no longer required, as requested by us. Rather, it merely transferred some of the data sets from the central KESY server to other data carriers in order to make them available to the public prosecutor's office. However, she continues to use the procedure in a modified manner.

KESY is just one example of the large number of processes that the Brandenburg police use to process personal data. At least as important are the police transaction processing system ComVor, the information and information process POLAS and the

operation control system for authorities and organizations with security tasks ELBOS. A prerequisite for legally compliant handling of personal data is a well-founded IT security concept derived from a risk analysis. Such a concept describes minimum requirements for IT security, serves as a guide for their implementation and should help to identify threats at an early stage. The police had definitely planned to create a systematic framework security concept for the individual systems and components, but despite repeated requests, they were unable to submit this to us in full over the years (B 2, page 98). Deadlines were not met and the completion of the concept was repeatedly postponed. The state commissioner complained about this in 2019. The documents finally submitted to us showed that, despite some progress, there were still significant deficits in the implementation of the technical and organizational measures.

Ms. Hartge presented the 2019 data protection activity report to the President of the Brandenburg State Parliament, Prof. Dr. Ulrike Liedtke, sent. Due to the current situation, we have decided not to hand it over personally and the press conference that is usually associated with it. However, Ms. Hartge is available by phone for questions or interviews.

ID number 03/2020

Date24.03.2020

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

ID number 03/2020

Date24.03.2020

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