09.05.2022 | 05/2022

State commissioner publishes data protection activity report 2021

Today, the state commissioner for data protection and the right to inspect files, Dagmar Hartge, presented the President of the Brandenburg state parliament, Prof. Dr. Ulrike Liedtke, her activity report on data protection for 2021.

The impetus for digitization in administration and business, which was already noticeable in previous years, did not lose momentum in the reporting period. This was also reflected in the focal points of our activities, which were in the field of technical and organizational data protection.

The Online Access Act requires the federal and state governments to offer administrative services in digital form via administrative portals by the end of 2022. However, the implementation always raises new problems; the nationwide need for coordination is very high. The data protection supervisory authorities of several federal states participated under our leadership in a working group set up on behalf of the data protection conference. The working group dealt in particular with the question of how administrative services can be implemented in compliance with data protection. She summarized her findings in a status report that was submitted to the Federal Ministry of the Interior and Homeland. The report forms the basis for further talks and coordination with the ministry and, if necessary, for an amendment to the law (A I 1.1, page 15).

A digitization project of the Online Access Act, which we have dealt with in detail and which is coordinated by the Ministry of the Interior and Municipal Affairs, was the "Residence permit for gainful employment" project. The focus is on issuing residence permits, residence cards and residence-related certificates as well as permanent residence certificates. The Ministry involved us in the preparation of the extensive project documentation during the pilot phase. Among other things, we were involved in the creation of the framework concept, the data protection concept and the IT security analysis. The municipal immigration authorities remain responsible for the procedures under data protection law (A I 1.2, page 18). Dagmar Hartge:

The digitization of administrative services promises great benefits for citizens. On the other hand, the authorities are faced with the challenge of designing the necessary processes in such a way that personal data is processed just as securely as in the context of classic administrative procedures. My employees will continue to support the implementation of the Online Access Act in an advisory capacity to the extent that the human resources of our authority allow for this.

In the second year of the pandemic, data protection issues were often the focus of discussions about technical solutions to contain the corona virus. The main burden continued to be borne by the municipal health authorities. You should e.g. B. Trace

contacts and isolate infected people or quarantine contacts. The software systems SORMAS and Luca were among the tools available to them. Unfortunately, we had to realize that both did not take data protection sufficiently into account:

SORMAS, a software specially adapted to COVID-19 for the management and analysis of infection outbreaks, should unify contact tracing and support health authorities. The Ministry for Social Affairs, Health, Integration and Consumer Protection had instructed them to be used in all Brandenburg health authorities. However, the program had deficiencies in terms of data protection law, in particular the documentation of data processing was inadequate. This does not only serve to ensure formal completeness, but represents a central component that, among other things, describes the measures to be implemented for data protection-compliant operation. For SORMAS, there were ambiguities about the data flows, the authorization concept, encryption, the deletion concept and other essential components.

Against the background of the high burden on the health authorities in the pandemic, we refrained from further burdening them with regulatory procedures and instead strived to achieve central improvements for all participating authorities. The independent data protection supervisory authorities of the federal and state governments initially worked towards improvements with specific recommendations for remedying the deficiencies to the project managers. This did not lead to success. In a second phase, representatives of some data protection supervisory authorities (including us) and the project managers at federal level held monthly consultations. More and more shortcomings became apparent: self-imposed deadlines for rectifying defects passed, the processing purposes of SORMAS were expanded, some data processing was not covered by legal bases and the software was suddenly also intended to be used for the long-term storage of personal data. Those responsible for the project agreed to take the points of criticism into account, but for the most part it stayed that way. As a consequence of the insufficient progress of the project, we have stopped working in the working group. As a result, it is incomprehensible to us that the health authorities were urged to use SORMAS as a product that did not fully comply with data protection (A I 2, page 22).

From the point of view of data protection, dealing with the use of the Luca system was just as frustrating. Here, too, we aimed to place as little additional burden as possible on the health authorities, who were already under a lot of strain during the pandemic. That's why we wanted to coordinate uniform specifications for the use of data from the Luca system with the Ministry for Social Affairs, Health, Integration and Consumer Protection and selected health authorities. We informed the Ministry of Health of our fundamental concerns at an early stage. In addition to proven security gaps, this also included our

doubts about the basic suitability of the Luca system for contact tracing purposes. The Ministry of Health nevertheless stuck to its decision to use the Luca system and adjusted the country's containment ordinance accordingly. The use of the data-saving Corona-Warn-App, which we recommended as an alternative, was therefore not possible.

For a long time it was not even known how the Luca system was actually used by the health authorities. We therefore initiated a corresponding survey. We asked the Ministry to send out questionnaires and to statistically evaluate the answers. As a result, only one health department reported that it had used contact details from the Luca system for contact tracing. This confirmed our view that the project was not suitable for combating a pandemic. The results of the survey also showed that the majority of the health authorities had not taken sufficient precautions to process contact data using the Luca system in accordance with data protection. Only in the current year did the state government decide to stop using the Luca system (A I 3, page 29). Dagmar Hartge:

With all understanding for the intention of the state government to contain the threatening corona pandemic as quickly as possible: With SORMAS and Luca, no suitable means were available from a data protection point of view. Anyone who checked into a restaurant with the Luca app could expect to be notified if another guest was infected. In fact, that is exactly what did not happen. The storage of the data was therefore completely useless. Those responsible should have recognized this much earlier and pulled the ripcord.

Last year, our authority took part in a cross-nationally coordinated inspection of the websites of various media companies. It was about advertising tracking - a data processing that is increasingly the subject of complaints. Anyone who visits an Internet site usually does not realize that a large amount of personal information is transmitted to hundreds of companies and evaluated there. Such data processing requires the consent of the user. For this purpose, cookie banners are used, which often offer consent with one click, but rejection involves much more effort. However, consent is only effective under data protection law if the selection is offered in an equal manner. There are often deficiencies in the information about the further processing of the data transmitted for advertising purposes.

With the help of a questionnaire, the data protection supervisory authorities involved in the audit asked about the tracking methods used, among other things. The publishing house audited in our area of responsibility, for example, transmitted the user-specific data to up to 150 integrated partner companies, but only provided general information about the use of cookies. While the company subsequently made improvements, it failed to meet the requirement to offer an equivalent opt-out option. In

the end, it settled on a model that offered the choice of opting in to be tracked for advertising purposes, or opting into a paid subscription and being spared from advertising tracking in return. This model, which is being used more and more frequently, is currently still being legally examined by the data protection supervisory authorities (A I 4, page 36).

Shortly after a security gap in the Microsoft Exchange Server software became known, tens of thousands of companies and some public authorities were affected in Germany alone. Over a period of several weeks, we received numerous reports of data breaches. Many of those responsible responded appropriately, professionally and quickly. However, this did not happen in five cases, so we carried out checks there. Three of these responsible persons did not sufficiently clarify the matter in the reporting period or did not respond to our inquiries. We will examine the next steps and, if necessary, initiate sanctions. The incident shows how important it is to constantly monitor the current threat situation in information technology and to take suitable countermeasures immediately (A IV 1, page 80).

Credential stuffing is a form of attack based on stolen user credentials. Here, criminals use automated mass queries to try out whether stolen access data such as e-mail addresses and passwords also enable registration on other Internet platforms. During the reporting period, a group of companies reported a data breach affecting more than 250,000 user accounts. The person responsible informed those affected, reset their passwords and asked them to assign new passwords. (A IV 4, page 88). Dagmar Hartge:

Companies must operate warning systems that can detect digital attacks. At the same time, however, their customers are also in demand. With relatively simple means, they themselves can contribute to the fact that attacks come to nothing. For example, you should use a different password that is as secure as possible for each Internet service and, if this is offered, use two-factor authentication. It may be more convenient to do without it, but it is definitely not safer.

We dealt in detail with a complaint about the use of the WhatsApp news service in a care facility for the organization of work and for communication with residents and their families. In addition to internal data, information on life in the facility and group photos of those in need of care were exchanged. The employees used their private mobile phones as a matter of course. When we took action, the care facility changed the short message service, but was unable to explain to us without a doubt which specific precautions to ensure data protection were actually implemented. As a result, we recommended a number of measures, including refraining from offers from third countries in favor of a solution within your own IT infrastructure or with a web host in Europe, using pseudonyms to name employees and those in need of care, and banning their use employees'

private mobile phones (A IV 2, page 82).

The Ministry of the Interior and Municipal Affairs asked us for information on the extent to which research by the immigration authorities in social networks, in particular on Facebook, to determine identity is permissible. We doubted the legality for various reasons and explained our position in detail. Among other things, it is generally not possible to check the authenticity and truthfulness of information in social networks and data from uninvolved persons can be recorded during research. In addition, the use of platforms based in the United States of America is prevented by the fact that adequate protection of personal data can only be guaranteed through additional measures (AV 6, page 120).

Again, we received many reports of data breaches involving children's data, often through break-ins and thefts at day care centers. In most cases, electronic devices were stolen, such as cameras or laptops. In order to clarify the causes of these incidents, we launched a survey. To our astonishment, the thefts happened both during and outside the opening hours of the facilities. We therefore recommend not only locking the devices after work, but directly after use. In addition, camera recordings should only be kept on the devices for as short a time as possible and then transferred to a protected storage system. In order to protect the sometimes sensitive data of the children, it is essential to use encrypted data carriers wherever possible. We recommended that the data protection officers of the day-care centers and their sponsors sensitize the employees to these issues (A II 3, page 68).

However, other responsible persons also reported data protection violations (A VI 4, page 135). Dagmar Hartge:

The renewed surge in mandatory data breach notifications, known as data breaches, worries me greatly. Such reports are often based on the exploitation of known security gaps and targeted hacker attacks. This makes it clear that those responsible must pay more attention to the use and updating of technical and organizational data protection measures. IT security is essential as the basis for effective data protection. Increasingly, this applies not only to large corporations, but also to small and medium-sized enterprises.

Against the background of various inquiries, which revealed a considerable need for advice from the responsible authorities, we checked compliance with data protection regulations when performing tasks under the Asylum Seekers Benefits Act by the social authorities of three districts and found deficiencies. The benefit files contained, among other things, prescriptions, transfer slips and diagnoses, from which a detailed picture of the state of health of the persons concerned could be taken. It also contained personal data of uninvolved persons, which allowed conclusions to be drawn about their state of health.

Protective measures that would have been appropriate to the high sensitivity of this health data were missing. The data were not necessary for the granting of services. We have complained about the violation of data protection regulations and asked the social authorities to make corrections (A III 4, page 70).

During the period under review, a member of a garage association complained that the board had posted his confidential correspondence in display cases on the association's premises. All other members and guests of the association could take note of the details of the correspondence. It was neither necessary nor lawful. We have therefore issued a warning to the club (A II 3, page 50).

The case of a file loss seems bizarre: An employee of a public body left a file with personal and company-related data, which should have been kept particularly carefully, on the car roof and drove off. The vehicle and the briefcase then took different routes; the documents could no longer be found later. The person responsible reported this data protection violation to us and made the entire workforce aware of the need to handle such sensitive data more carefully (A IV 7, page 95).

The state commissioner continued to support the pilot project on the use of bodycams by the Brandenburg police. We focused on the technical and organizational measures that must be taken to ensure safe and data protection-compliant operation of the body cameras. The police finally presented us with a coherent risk analysis. Of course, the resulting measures to ensure data protection must also be implemented. In our consultation, we attached great importance to measures that prevent the manufacturers of these cameras from gaining unauthorized access to the data recorded by the camera (B 3.1, page 152).

A large information network such as that of the Brandenburg police requires a process-independent framework concept for IT security. It serves as the basis for partial security concepts that build on it for the individual automated processes. The development of such a framework security concept has shown considerable deficits over the years. In the meantime, fortunately, both the implementation planning and the implementation status, in particular of the technical and organizational measures recognized as having high priority, have improved significantly. The state commissioner will continue to support the work of the police on the framework security concept in a constructive and critical manner (B 3.2, page 154). Dagmar Hartge: I have repeatedly complained about the Brandenburg police's lack of an IT framework security concept. The fact that it is finally available and that we are now only discussing the details is a great step forward. The police also involved me comprehensively and in good time in preparing for the use of bodycams. Data protection-compliant solutions are particularly important where the state interferes deeply with the basic rights of citizens.

However, we also have to note that the number of transactions involving fines in connection with unauthorized data processing by police officers in the state of Brandenburg has risen again compared to the previous year. Overall, around 26% of our fine proceedings relate to such processing (A II 4.4, page 56).

The fine office of the state commissioner also pursued data protection offenses in other cases. In 23 cases, it imposed fines for the violations of data protection law that had been identified. The total amount of fines imposed was 13,430 euros (A VI 5.2, page 137).

For example, a gardening company published a video recording of a complainant's trial work. For advertising purposes, it published the recordings both on the social network Facebook and on the online platform YouTube and the company's website. We punished the intentional publication of the video and the failure to delete it with a fine (A II 4.2, page 53).

A former employee of a company - when she was still employed there - sent a table with the data of other employees from her work computer to her private e-mail address. In addition to the full names, the table included e.g. also an overview of vacation days, sick days, wage data, overtime worked and social security contributions. This was not necessary to fulfill their operational tasks and was therefore illegal. We also punished this violation with a fine (A II 4.5, page 58). The same happened to an employee who forwarded application documents that had been received by his employer to his private e-mail address. He wanted to be inspired by this for the visual design of his own applications (A II 4.6, page 58).

A doctor specializing in child and adolescent psychotherapy shared her new practice address with a large WhatsApp group. This included parents, therapists, social workers and teachers. The phone numbers of the other members were revealed to them. Anyone who kept these numbers as their own contacts could draw conclusions that children from families they knew were being or had been treated by the doctor. We imposed a fine on the doctor (A II 4.7, page 60).

ID number 05/2022

Date05/09/2022

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

ID number 05/2022

Date05/09/2022

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