State commissioner publishes data protection activity report 2022

- Released on April 17, 2023 - press release 04/2023

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 the year 2022.

For several years now, the state commissioner has been dealing with the compatibility of the operation of Facebook fan pages by public authorities with data protection law (A I 1, page 14). Obtaining statements from the highest state authorities should give them the opportunity to check the legality of their fan pages themselves. Ultimately, however, it was only said that the state had to be present on this communication channel in order to reach the citizens. The data protection conference dealt with the topic in detail. Last year, she published a short report that questioned the legality of operating Facebook fan pages. We then asked the state government to provide this proof of legality. But she only said that a statistics function had been deactivated. The state government is no longer responsible for data processing and all requirements are met. Both the state commissioner and the data protection conference saw things differently. Furthermore, fan pages transmit personal data to Facebook or its parent company Meta, without this being necessary for their operators. The state commissioner is now examining, in close cooperation with other supervisory authorities, whether to issue a prohibition order. The hearing is currently being prepared. Dagmar Hartge:

The state government will probably still not be able to prove that their Facebook fan pages are operated in accordance with data protection regulations. It is therefore a mystery to me why she continues to transmit personal data to Facebook without need. Rather, public bodies – and this does not only apply to the state government – should live up to their role model function and avoid data protection risks for interested citizens. Public relations works without Facebook.

Cookies are small text files that are stored on the user's device and read from there. The information they transmit can usually be assigned to natural persons and, for example, enables their individual behavior on the Internet to be evaluated. The so-called cookie banners are used to obtain consent. For example, a cookie banner is not sufficient for the use of cookies and tracking on the Internet if you can accept the tracking with just one click but only reject it with additional interactions (A I 2, page 18, 23). In the past year, a large number of users complained about the design of the cookie banner, insufficient options for setting preferences or the lack of transparency in data processing. Since the state commissioner was also aware of the complexity of the subject in terms of data protection law and the legal uncertainty that had prevailed in recent years, she

initially pursued the goal of advising the responsible persons and ending possible legal violations by means of information and recommendations. In most cases this succeeded. For the future, however, the state commissioner does not rule out enforcing compliance with the legal regulations with orders, prohibitions or fines.

Despite years of extensive dialogue between the data protection supervisory authorities and Microsoft, the use of the Microsoft 365 online service for authorities, companies and associations is generally not permitted (AV 1, page 82). Even improvements made by the group could not eliminate the main point of criticism: Microsoft processes personal data from order processing for its own purposes without presenting this in a sufficiently transparent and comprehensible manner. His data protection addendum, which was revised in the course of the talks, restricts this processing conceptually, but still does not disclose which personal data is used for which "business activities" and for how long it is processed. A responsible body that wants to use Microsoft 365 cannot carry out the necessary balancing of interests on this basis. Public bodies, such as schools, are also faced with the problem that their legal bases for processing personal data typically do not legitimize the transfer of data to a company that processes them there for their own "business activities".

We have already reported several times that complaints about video cameras are increasing in each reporting period. Smaller cases from the neighborhood as well as video surveillance of larger companies, in which a large number of cameras are used (for statistics, see A VI 3, page 105), are criticized. The operation of the checked cameras is not always prohibited; in some cases, a different orientation or switching off individual devices is sufficient.

However, the legal situation is clear when it comes to video surveillance in a sauna area (A II 3, page 33). At least inside the sauna rooms, the use of cameras represents a serious encroachment on the rights of the guests, who are usually lightly or undressed, and is not permitted. We thought word had gotten around by now, but we had to deal with another such case during the reporting period. Two cameras were used for live monitoring of up to five daily show infusions with light and sound effects with up to 200 visitors. The cooperative sauna operator deactivated these cameras immediately after we approached the company.

A case of video surveillance in community accommodation for refugees by a municipal operator kept us very busy (A IV 7, page 72). We found that over 120 video cameras are in use there. They covered practically all publicly accessible areas of the accommodation. In addition, cameras were aimed at the doors of the refugees' apartments and the access doors to the sanitary facilities. The security service was able to observe the images in real time, and all video cameras also permanently

save their recordings. The aim of those responsible was to be able to react more quickly to escalations in the company. There are often violent clashes. This is the only way to ensure adequate protection for employees and residents. However, this did not justify their constant surveillance. Many cameras were not permitted under data protection law, for example video surveillance of children's playgrounds was generally not permitted. The monitoring of the access doors to the sanitary facilities was also illegal. We informed the person responsible about measures that enable video surveillance to be operated in accordance with data protection law. This includes changing numerous camera detection areas, limiting the recording time, leaving out particularly sensitive areas and reducing the number of video cameras in operation. However, the documentation delivered after the implementation deadline still showed deficiencies. The state commissioner is still in the process of voting in order to be able to establish a lawful situation as quickly as possible.

The fines office of the state commissioner imposed fines in 13 cases last year for identified violations of data protection law. The total amount of fines imposed was almost 123,000 euros (A VI 5.2, page 110).

Probably the most serious case that the fines office had to deal with was the appearance of live images from the video surveillance of a bank on the Internet (A II 5.1, page 37). The camera used was aimed at the foyer of a branch, including the entrance area, statement printer and ATM, as well as the sidewalk and parking lot in front of the branch. Unknown third parties finally compromised the video camera and made the real-time images available to everyone on the Internet. To a limited extent, it was even possible to control the camera. The bank had failed to implement suitable technical and organizational measures to prevent this. In addition, there was no order processing contract with the service companies. After all, the camera shouldn't have captured the sidewalk or the parking lot. We imposed a fine in the upper five-digit range for these violations.

During the corona pandemic, a restaurant operator required visitors to fill out the paper sheets laid out in the restaurant on the occasion of the legally required contact tracing. In addition to other information, the e-mail address had to be entered, although the relevant regulation did not provide for this. In addition, the guests were asked to mark on the paper that they agreed to the restaurant being contacted. The restaurant operator finally used the e-mail addresses to send out a newsletter for advertising purposes (A II 5.2, page 39). That had nothing to do with the only official corona contact tracking that was allowed. We set a fine in the low five-digit range.

The fine office also pursued a hacker attack on the website of an association in the health sector (A II 5.4, page 42). Among other things, it offers transport services for patient transport. Employees entered the necessary customer data records in the

password-protected internal area of the website. The association's website was vulnerable for several days due to a technical vulnerability. As a result, they were actually compromised and the contents of the database were read out - after all, 89,000 data records, some of which allowed conclusions to be drawn about the state of health of the people concerned. The incident was based on several breaches of data protection law; we imposed a five-digit fine.

In an unprovoked inspection of car dealerships (A III 1, page 48), the focus was in particular on the handling of documents such as vehicle registration documents, invoices and copies of ID cards as well as the verification of compliance with data protection requirements. As a result, we found a consistently lax handling of personal data. Data protection declarations were inadequate, documentation requirements were not met, the car dealerships often kept data twice and stored it for far too long. The main reason for the excessive storage of personal data turned out to be the use of manufacturer's own IT systems. None of these allowed personal data to be deleted once financial transactions were in place. It was also unclear whether the systems provided for data transmission to non-EU countries. Dagmar Hartge:

On the one hand, companies are being urged to use their own IT systems, on the other hand, in many cases this harbors the risk of possible data protection violations. Technical and organizational deficiencies can ultimately also threaten the companies themselves. However, they remain responsible under data protection law at all times. I appeal to the manufacturers to assume their responsibility and to take data protection requirements into account from the outset when designing their systems.

A hospital had published the photos with numerous other details about the children born there and in some cases the names of the parents in an online baby gallery that was accessible to everyone (A IV 1, page 62). The latter presumably happened even though the parents had released this data only for publication in the daily newspaper in a declaration of consent that covered several purposes. We pointed out that the declaration of a parent is not sufficient for the worldwide publication of the information and that the data is sensitive because the mere stay in the hospital is to be regarded as health data under data protection law. The hospital immediately took up our recommendations. The information in the baby gallery has been reduced to the picture, first name and date of birth of the newborn. In addition, the hospital developed an independent declaration of consent limited to this purpose only.

We found that a large amount of personal data from members of an anglers' club could be called up on the Internet (A IV 4, page 66). It was not just the full names and addresses, telephone numbers, email addresses and dates of birth of the approximately 100 members, but also their account details and transfers. Children's personal data was also visible to

everyone. We informed the association; he immediately took the website offline. It was not possible to explain how the incident had happened. In our view, the data breach was serious. Financial losses or other economic disadvantages may result from the publication of account details. The other freely accessible data could be used for identity theft. In addition, the special protection of children's personal data fundamentally prevents publication. We are still examining the introduction of sanctions against the club.

Recreational anglers who were checked in Brandenburg waters complained about fishing checks with private smartphones (A IV 5, page 68). Officially appointed fisheries wardens photographed their fishing licenses and identity cards in this way. To clarify the facts, we first turned to the responsible districts as the lower fisheries authorities. One of these authorities referred us to the responsible ministry and a corresponding guide. Consequently, we made it clear to the ministry that the use of private smartphones for government oversight purposes is unacceptable without further precautions. This facilitates unauthorized access by third parties to personal data, official control over the data cannot be guaranteed and the use of the photos for private purposes cannot be ruled out. In addition, taking photos of ID documents is not required under data protection law; a note in the control report is sufficient. While one district has now banned the use of private smartphones, we are still in talks with another district and the ministry.

A significant number of data breaches reported to us by those responsible are the result of hacking attacks on external service providers (AV 2, page 85). Against the background of increasingly complex data processing processes and at the same time reduced resources, there is a growing tendency to outsource data processing to external companies - from individual processing steps to a complete outsourcing of the entire IT landscape to the cloud. Many responsible persons think that they could also get rid of their data protection obligations in this way. However, this conclusion is incorrect: From a data protection point of view, a service company remains bound by instructions. In particular, the person responsible is obliged to monitor the execution of the order. Small companies or associations often lack the necessary data protection and IT skills. If there is a successful hack, they must believe the assurances given by the processors – both regarding possible data leaks and that the necessary data protection and security measures are in place to prevent a recurrence. Dagmar Hartge:

Authorities, companies and associations are called upon to keep their own human, financial and time resources available in the areas of data protection and information security on a permanent basis. The on-site data protection officers, whose importance is often underestimated, play a key role here. You advise those responsible and monitor compliance with data

protection regulations. Strengthening their position can also have a positive influence on the legally compliant design of order processing.

The State Commissioner gives a positive assessment of the results of her monitoring of police projects (B 1, page 116). The Brandenburg police involved us intensively in various procedures and digitization projects over the past year. The foundation of police IT security in Brandenburg - the framework security concept - has made further progress. The important agreements on order processing have also made significant progress in terms of content. A regular exchange also took place in the run-up to the preparation of data protection impact assessments by the police and on sub-projects of the P20 program. This is an overarching federal and state project; it serves to modernize and harmonize police information processing. The subject of the further exchange with the Brandenburg police was a newly developed mobile messenger, the use of newly procured service phones during operations and the scope of the documentation for the pilot phase of IT services by the police. Dagmar Hartge: I am pleased that my authority is not only used by the police as a supervisory authority, but also as an advisory body. This allows us to get involved at an early stage in the event of questionable developments for IT security or data protection and we do not only evaluate procedures after the planning has been completed.

As part of an examination of personal alerts in the Schengen area coordinated with other federal and state supervisory authorities, the state commissioner examined a total of ten national and Schengen-wide personal alerts from Brandenburg (B 2, page 118). This is a measure that leads to covert observation or targeted checks of the persons concerned by the police or border authorities, either for the purpose of preventing crime or for criminal prosecution. We selected four alerts each, which were for preventive and repressive purposes, and two that served to supervise conduct. Overall, we could not find any serious deficiencies in the control of the selected personal advertisements in Brandenburg. In two cases, we only found that the deadlines for the legally required checks on the further necessity of the measure were exceeded, as well as documentation deficiencies. We have made it clear to the authorities issuing the order that the follow-up orders must be dealt with in good time in order to meet the test deadlines. The weighing decisions made must be fully documented. It is necessary for the facts justifying the order to be compiled in each individual case so that the process of consideration is comprehensible and is not reduced to formulas.

binder

ID number 04/2023

Date17.04.2023

ContactAstrid Oehme Poststelle@LDA.Brandenburg.de