04/09/2019 | 05/2019

State representative presents activity report data protection 2018

The state commissioner for data protection and the right to inspect files, Dagmar Hartge, published her activity report on data protection for 2018 today:

For companies, administrations and associations, the past calendar year was dominated by the introduction of the new data protection law (Chapter I, No. 1, Page 10). The two-year preparation period ended on May 25, 2018. Since then, all those responsible have had to apply the General Data Protection Regulation, which is directly applicable throughout Europe. This caused enormous uncertainty in some cases.

In numerous training events, we conveyed the legal and technical-organizational innovations to over 1,900 executives and data protection officers from administrations and companies at almost 40 events (Chapter I, No. 2.1, page 12). In addition, there were numerous individual consultations, especially for small and medium-sized companies. Among other things, it dealt with the future implementation of data subject rights, the limits of permissible advertising and the appointment of data protection officers (Chapter I, No. 2.2, page 13 and No. 2.7, page 21). Clubs, for example, inquired about the lawful processing of their members' data and about the conditions for sending newsletters (Chapter I, No. 2.3, page 16). Some cases in the healthcare sector thrived in particular: Some practices suddenly made the treatment dependent on whether the patient had previously "voluntarily" consented to the data processing - although the treatment contract would have been completely sufficient as a basis for this. While a brief reference to the legal situation was usually sufficient here, our advice on the practical design of the new information obligations towards patients was more intensive (Chapter I, No. 2.4, page 17). Many of the inquiries and complaints we received about the data protection-compliant handling of photographs were probably due to the initially very sweeping public debate. Although we consider clearer legal regulations to be desirable overall, we were able to give the all-clear in most cases. The changes were not that revolutionary; In particular, according to the old legal situation, the depiction of persons required either their consent or a legal basis (Chapter I, No. 2.6, page 20). Dagmar Hartge:

In 2018, my employees were fully occupied with answering inquiries, conducting training courses and sometimes calming people down. Not everything was new. Rather, it became apparent that bodies that had previously treated data protection as a stepmother or stepfather were now faced with the problem of having to implement everything at once.

Although the demand for advice has meanwhile decreased, meeting it remains an important task for our office.

Companies or administrations that operate a Facebook fan page cannot escape their responsibility under data protection law. The European Court of Justice decided this last year (Chapter IV, No. 1, page 64). For example, they have to enter into certain agreements with Facebook and explain in a comprehensible manner that the processing of user data is compatible with the General Data Protection Regulation. As a rule, they will not be able to do this, since Facebook has not yet provided sufficiently transparent or specific information about this. The main criticism is the opaque processing of user data - including that of fan page visitors who are not members of the social network. Under these conditions, the operation of Facebook fan pages is illegal. The conference of the independent data protection supervisory authorities of the federal and state governments recently pointed out this. In the current year, the state commissioner will put those responsible who run such fan pages to the test.

Facebook also kept us busy with very specific complaints over the past year. For example, an employer published on the public Facebook profile of her former employee that she owed several thousand euros in taxes and her wages therefore had to be seized (Chapter IV, No. 2, page 66). It is obvious that such denunciation goes far beyond what is permissible under data protection law. The state commissioner has therefore - still according to the old legal situation - imposed a four-digit fine.

Authorities and companies have repeatedly asked whether they can use the WhatsApp messenger service for their respective purposes in accordance with data protection (Chapter IV, No. 3, page 66). In all cases, our answer was a resounding no. Anyone who uses WhatsApp automatically reads their contact details (telephone book) and stores the data on the company's own servers. The consent of those affected is unlikely to be available for this. Dagmar Hartge:

At the latest when Facebook plans to merge the messenger services of WhatsApp, Instagram, Messenger and Facebook, companies and authorities should take the opportunity to look for alternatives. I recommend only using communication channels that are under your own control and ensure secure, confidential communication.

The amendment of the Brandenburg Police Act caused intensive discussions in 2018 (Chapter V, No. 1.1, page 82). Some far-reaching powers of intervention – such as electronic surveillance to avert danger and so-called online searches – were removed from the draft law even before the parliamentary debate. Later, the state commissioner's criticism of the originally planned, but ultimately canceled surveillance of messenger services (source telecommunications surveillance - "Quellen-TKÜ") was also heard. Nevertheless, the law just passed by the state parliament significantly expands the police data processing powers. In particular, interventions to counter terrorism are permitted prior to a specific threat, so that bystanders can more

easily become the focus of police attention. We also consider the extension of the storage period for police video recordings from two days to two weeks, which we believe to be disproportionate, to be questionable.

During the review of the police operations control system for authorities and organizations with security tasks ("ELBOS"), we identified several violations of data protection law in the reporting period (Chapter III, No. 1, page 54). For example, thousands of employees were able to read mission logs or conduct research on missions that had already ended. Among other things, a more restrictive assignment of access rights and an encryption of sensitive personal data were missing.

Together with our Berlin colleagues, we checked the clinical cancer registry of the states of Brandenburg and Berlin (Chapter III, No. 3, page 59). We were particularly interested in whether the technical and organizational measures required for efficient data protection had been taken. We also checked the procedures and processes for processing social data. The security of the premises and the handling of the paper documents were not objectionable. However, among other things, a comprehensive extinguishing concept was missing; Reports of findings sent by post were also – contrary to the rules – completely scanned and permanently stored electronically.

Until the introduction of the General Data Protection Regulation, the so-called objection to public authorities was the most important instrument for data protection supervision. In the first half of 2018, the state representative used it several times. For example, she complained about the integration portal of a job center (Chapter II, No. 3, page 44). With the help of this portal, the district regularly transmitted sensitive social data of the beneficiaries to a commissioned company, which reported suitable job offers back to the job center. Although there was no data protection-compliant procedural concept for this and its own IT security officer had doubts about its legality, the district introduced the procedure. His promises to make improvements came to nothing. It was only when the state commissioner, after complaining, offered the prospect of instructions for documenting the procedure based on the new data protection law, did the job center stop operating the portal. Last but not least, this speaks for the effectiveness of the additional supervisory powers over public authorities.

The new data protection law already provides for a larger range of instruments for data protection supervision in the run-up to an instruction: A warning indicates to the person responsible that the intended data processing is likely to violate the General Data Protection Regulation; a warning in the event of a violation that has already occurred corresponds to the previous complaint. The state representative issued a warning to a court after the electoral register had been sent to too many recipients as part of the election of the committee of honorary judges and it could not be ruled out that this error would be

repeated in the future (Chapter II, No. 4 , page 45). We warned a provider of riding holidays who informed the children's parents about the cancellation of their booking (Chapter II, No. 5, page 48). He did this using an open mailing list so that all recipients could see all addresses.

With the General Data Protection Regulation, the cooperation between the European data protection supervisory authorities has intensified considerably (Chapter VII, No. 4, page 116). Complaints about the cross-border processing of personal data are processed using an EU-wide, electronic register, in which all such cases are entered for the purpose of cross-border processing. Since May 25, 2018, the state commissioner has had to check a total of 597 cross-border cases to see whether we are involved in the processing. In 55 cases we did this because the person responsible had a branch in Brandenburg or the reported processing of personal data could have a significant impact on citizens of our state. In one case we took the lead. We reported a further 18 complaints that we received to the register; in 36 cases we participated in the development of a common position. Dagmar Hartge:

The complex coordination process between the European supervisory authorities, which is conducted exclusively in English, is new for everyone involved. With its establishment, the European legislator has reacted to the realization that the processing of personal data does not stop at national borders. The aim of the procedure - a uniform application of the General Data Protection Regulation in all Member States - was and is an important part of the data protection reform.

However, a modus operandi both in dealing with the register and in cross-border coordination still has to be established.

The General Data Protection Regulation provides for a significant tightening of the obligation to inform the supervisory authority in the event of a breach of data protection (Chapter VII, No. 3, page 116). As a result, the number of data breach reports has increased massively since May 25, 2018. By the end of the year, we had received a total of 124 reports based on the new legal situation. A large proportion of the cases involved the incorrect dispatch of documents; Also reported were, for example, the theft of a daycare center's digital camera with children's photos and the loss of a file that an official had left on the car roof when driving off. Attacks on computer networks in which personal data was captured also accounted for a significant proportion. In many such cases, the new regulation forces those responsible to inform the persons concerned about what has happened. The purpose of the extended reporting obligation is to make companies, administrations and associations aware of the fact that they themselves take measures to ensure data protection - if only to avoid attracting attention from the data protection supervisory authority.

As has been the case for years, we again recorded a significant increase in complaints and inquiries about video surveillance (Chapter VII, No. 1, page 112) to a total of 118 cases in the reporting period. We processed 87 of them as complaints. Partly it was about the surveillance of the publicly accessible space, but partly the complaints were also related to long-standing neighborhood disputes. Checking video surveillance is particularly complex when several cameras are used. This is often the case with companies. Here we have to evaluate for each individual camera whether it meets the requirements of data protection. Based on the complaints alone, we checked 360 video cameras in this way over the past year.

The General Data Protection Regulation has not yet had an effect on the scope of the fine proceedings conducted by the state commissioner (Chapter VII, No. 5, page 118). Since administrative offenses are always to be assessed according to the law in force at the time they were committed, most of the new procedures from 2018 still relate to the old legal situation.

Finally, a note on our own behalf: So far, the state commissioner has submitted its activity report both for data protection and for the inspection of files every two years. The new regulation of data protection law means that we now publish our activity report on data protection annually, while the report on file inspection continues to be published every two years.

ID number 05/2019

Date09.04.2019

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

ID number 05/2019

Date09.04.2019

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