Press release from the State Commissioner for Data Protection and Freedom of Information Mecklenburg-West Pomerania

One year DS-GVO - The State Commissioner for Data Protection and Freedom of Information presents its 14th activity report and takes stock

No.20190521

|

05/21/2019

|

DSMV

|

datenschutz-mv.de

For the processing of personal data, the European General Data Protection Regulation (GDPR) has been in force for a year - time to take stock. The State Commissioner for Data Protection and Freedom of Information for Mecklenburg-Western Pomerania, Heinz Müller, presented his authority's activity report for 2018 today.

Main topics 2018

The number of complaints to the State Commissioner tripled in 2018 compared to the previous year. Heinz Müller says: "My constitutional task is to protect the right of citizens to the protection of their personal data. The GDPR has significantly strengthened this role. I am pleased that citizens are using their extended rights."

As a result of the GDPR, the State Commissioner for Data Protection and Freedom of Information has been given over 50 new tasks. His authority no longer only processes complaints against authorities and companies in Mecklenburg-Western Pomerania. Since May 2018, he has been obliged to also receive complaints against bodies that are not based in Mecklenburg-Western Pomerania or even in Germany. He remains the point of contact for those who have lodged a complaint with him throughout the entire process. In the case of cross-border data processing in particular, where the competent supervisory authority is located in another European member state, this entails a considerable coordination effort.

The application of the GDPR from May 25, 2018 caused widespread hysteria in both the public and private sectors. The GDPR had already come into force throughout Europe in 2016. However, the two-year transition period remained largely unused. In May 2018, one could get the impression that the new law had come about overnight. The demand for information, training and

advice exploded. "In numerous training courses and information events, we have repeatedly made it clear which requirements are really new and which are based on existing German law, and thereby contributed to an objectivity in the debate," says Müller in retrospect.

The GDPR poses particular challenges for clubs. Association board members are mostly volunteers and since May 2018 have had to deal with questions such as: “Do we need a data protection officer? Do we have to obtain consent from our club members in order to be allowed to process their data in the club? May we put photos from the last football tournament on our homepage?”. The state representative has therefore developed a guide together with the voluntary foundation for the clubs, which has been available free of charge from the state representative since October 2018.

As chairman of the working group “Technical and organizational data protection issues” of the conference of independent federal and state data protection authorities (DSK), the state commissioner advises the IT planning council. The IT planning council deals, among other things, with the digitization program for public administration. The Online Access Act obliges the federal and state governments to also offer their administrative services electronically via administrative portals by the end of 2022. In this context, the German administrative registers are also to be modernized and identity management improved. The Federal Ministry of the Interior has therefore proposed to the IT Planning Council the introduction of a so-called identifier for reliably locating data records of a person in various registers. This is only permissible within very narrow limits, since the introduction of such personal identifiers massively interferes with the right to informational self-determination of the citizens concerned. The federal and state data protection authorities will ensure that the regulations of the GDPR are observed when implementing the digitization program.

One of the authority's core tasks is to provide target group-oriented information on data protection. According to the GDPR, special attention should be paid to specific offers for children and young people. Since 2012, the state representative has been showing children and young people the opportunities and risks of the digital world with the joint project Medienscouts MV. The goal is a self-determined, critical, but also creative approach to Instagram, Google & Co. The so-called peer-to-peer approach is fundamental. The media scouts learn to pass on their knowledge directly to other children and young people. With the funds currently available, 60-70 media scouts are trained each year. Overall, the project, which is carried out jointly by the State Commissioner, State Youth Council, State Criminal Police Office, State Media Authority and State Coordination Office for Addiction Issues, sensitizes around 3,000 to 3,500 people per year. Müller: “We data protection officers cannot be everywhere.

That is why citizens, starting with children and young people, must take the protection of their data into their own hands. They can learn how to do this from the media scouts."

For many years, the state representative has pointed out that e-mails with sensitive content should be encrypted, because an e-mail can be compared to a postcard in terms of security: what you would not entrust to a postcard should not be sent by send unencrypted email. Nevertheless, e-mails are very often sent unencrypted, even with sensitive data. Müller: "It is not always necessary to use criminal energy to gain unauthorized access to the content of unencrypted emails." This was shown by a tip from a citizen received by the state commissioner. He had received an e-mail from a public body in the country that was obviously not intended for him. Attached to the e-mail was a list of people with their names, addresses, identity card numbers, vehicle license plates and information about their security checks by the federal police. The correct addressee of the e-mail had the same name as the wrong recipient, except for the spelling of an umlaut. The sender accidentally chose the wrong recipient's spelling, so that recipient received the email.

The number of petitions on video surveillance remains at a very high level. It is often not considered that video surveillance of publicly accessible rooms is only permitted under certain conditions. Not much has changed with the GDPR. In any case, video surveillance is only permitted if the legitimate interests of the operator of the camera are weighed up against the interests or fundamental rights and freedoms of the data subject. Surveillance measures that violate privacy, for example in the case of saunas, toilets or shower stalls, are generally inadmissible. Interests worthy of protection also often prevail where people communicate, eat and drink or relax, for example in the seating areas of restaurants or parks. A legitimate interest can generally be assumed if the purpose is protection against burglary, vandalism or theft, provided that an actual risk situation has been proven. Webcams, which transmit live recordings to the Internet, are also being used more and more frequently. The recordings of these cameras are accessible to an indefinite number of people worldwide. They are therefore only permitted if no persons can be identified in the pictures.

Since the application of the GDPR, the state commissioner has been responsible for fine proceedings against police officers resulting from data protection violations in their employment. So far, responsibility for this lay with the Ministry of the Interior and Europe. The state commissioner had to deal with unpleasant cases. Among other things, police officers used their official position in two cases to get the contact details of underage girls. In both cases, the state commissioner imposed a fine.

The state representative issued a warning to the Rostock Higher Regional Court because data security was not observed there

when using the fax machine. A citizen had informed the state representative that in two cases decisions by the Higher Regional Court in criminal matters had arrived on her fax machine by mistake. These were the complete orders in the execution of sentences for manslaughter and other offences. In contrast to letter post, fax is a type of open delivery. Therefore, when personal data is sent by fax, measures must be taken to prevent unauthorized reading, copying, changing or deleting of this data during transmission. Before sending sensitive data using the fax service, those responsible should check whether this type of shipping is really necessary and whether another type of shipping is more appropriate.

Serious violations of the protection of personal data, so-called data breaches, must be reported to the state representative within 72 hours in accordance with Art. 33 GDPR. In the reporting period, the state commissioner received 36 such reports, including the notification that the council information system of an office administration had been hacked, so that unauthorized access to personal data in non-public draft resolutions and minutes could not be ruled out. The office administration determined that all documents from the meetings in the years 2012 - 2018 were affected. As an immediate measure, she deactivated all access to the platform. In addition, it had to be considered that if there is a high risk according to Art. 34 DS-GVO, the persons concerned must be informed immediately. So the official administration informed the affected community representatives about the data breach. However, since the data of a large number of other people was also contained in the draft resolutions or minutes, including information on the economic circumstances of applicants, they also had to be informed accordingly. Due to the large number of people affected, the official administration, in consultation with the state commissioner, made use of the public announcement of the data breach in accordance with Article 34 (3) (c) GDPR.

Current topics 2019

As a member of the "Artificial Intelligence" task force, the state representative was involved in the preparation of the DSK's "Hambach Declaration on Artificial Intelligence". In it, data protection requirements for the use of "self-learning" systems are formulated. In particular, the right of the data subject must be guaranteed not to be subject to a decision based solely on automated processing. "Only if the protection of fundamental rights and data protection keeps up with the process of digitization is a future possible in which people and not machines ultimately decide about people," the statement says verbatim.

Data protection advocates have been observing the use of Microsoft products for many years and have repeatedly warned of an impending monopolization of the market. The current discussion on the Windows 10 operating system shows how justified

these warnings are. Only with massive interventions in the operating system and the associated IT environment can an attempt be made to prevent data transmission from Windows 10 to Microsoft. Since a large part of the data is sent to Microsoft in encrypted form, it cannot be conclusively determined whether and, if so, which personal data is transmitted to Microsoft. From the point of view of the state commissioner, it is extremely doubtful whether Windows 10 can be operated in compliance with data protection regulations. The DSK is in discussion with Microsoft and is working on a detailed statement. Although the risks of using these products in the state administration have been known for many years, the state government has not yet developed a strategy for minimizing these risks, for example by switching to open source products over the long term.

outlook

The authority of the state commissioner has had to cope with the sharp increase in workload with an unchanged number of staff. Five new jobs were created in January 2018. However, this did not increase the number of employees because only five temporary jobs were converted into permanent jobs. "I expect," says Müller, "that the suspension of the personnel concept recently decided by the state government will also affect my authority."

The DS-GVO is just about to face its big test. More than 10,000 citizens have lodged complaints with French colleagues against Google, Amazon, Facebook, Apple and Microsoft. These are violations of the law that affect all citizens. "We data protectionists will have to be measured by whether we enforce the GDPR against large corporations," says Müller. "The fact that politicians do not ensure a balanced balance of power here and do not provide data protection supervision with resources that meet their needs shows great short-sightedness."

Investments

14. Activity report on data protection

(PDF, 0.56MB)

Back to overview