DetailHomeNewsDetail

09/30/2020

Data protection advocates are committed to "digital sovereignty" in public administration - data protection conference makes various decisions Against the background of growing dependence on dominant software providers, the conference of independent data protection supervisory authorities of the federal and state governments (DSK) has taken a data protection policy position on the digital sovereignty of public administration. Digital sovereignty is understood here as the possibility of being able to act independently, self-determinedly and securely in the digital world. In practice, however, many public administrations are currently unable to act independently because they are dependent on large software companies and because there are particular technical constraints in the IT landscape. The DSK sees the digital sovereignty of public administration as being impaired and therefore encourages the increased use of alternative software products and open source products. As a result, "the independence of public administration from market-dominant software providers can be permanently ensured," says the resolution that is now available and was decided last week at the data protection conference. The DSK has passed a series of recommendations for action with a view to digital sovereignty. Specifically, she calls on the federal, state and local governments to only use hardware and software products in the long term that allow those responsible to have exclusive and complete control over the information technology they use. In the short term, products and services should be better assessed in terms of data protection law - both during selection and during operation. The DSK is in favor of certifications that make testing and control easier for those responsible if they cannot independently form a valid picture of the complex functioning of information technology. In addition, product developers should use open standards so that those responsible are actually able to switch providers and products if they can no longer or only insufficiently implement the data protection requirements with their products and services. The DSK also has a preliminary rating of " Microsoft Office 365" and a corresponding position paper of the working group administration was acknowledged and approved by a majority. This comes to the conclusion that on the basis of Microsoft's order processing documents (as of January 2020), data protection-compliant use of Microsoft Office 365 is not possible. The DSK has therefore decided to set up a working group to start talks with Microsoft on the basis of these assessments in order to achieve timely improvements in accordance with data protection regulations. The DSK agrees on the need for such improvements. At the DSK interim meeting, it was also decided to set up a task force for the groundbreaking judgment of the European Court of Justice (ECJ) on data transfer to the USA

(Schrems II), which would allow nationwide coordination of the procedure ensure and develop a strategy for enforcement. The DSK has also passed a revised "short paper" on employee data protection: It serves as an initial orientation, especially for the non-public sector, and shows how the General Data Protection Regulation should be applied in practice. In addition, the DSK calls for the regional courts to retain their first-instance jurisdiction for fines of more than 100,000 euros. Further information: Resolution "Create digital sovereignty in public administration" Brief paper no. 14 "Employee data protection" Resolution "Data protection needs regional courts - also in the first instance"

return