Berlin, August 19, 2020

Press release 20/2020

BfDI on the consequences of the legislation of the PDSG

The Federal Commissioner for Data Protection and Freedom of Information (BfDI) Professor Ulrich Kelber points out the consequences of processing personal health data in violation of European law as a result of the Patient Data Protection Act (PDSG): My authority will have to take supervisory measures against the statutory health insurance companies under my responsibility , if the PDSG should be implemented in its current version. In my opinion, introducing the electronic patient record (ePA) solely in accordance with the specifications of the PDSG violates the European General Data Protection Regulation (GDPR) in important places.

In its statements during the legislative process, the BfDI pointed out several times that patients must have full sovereignty over their data when the ePA is introduced. Here the PDSG passed by the German Bundestag, which is currently being discussed in the Bundesrat, shows deficits: health data reveal the most intimate information about the citizens. That is why they are also specially protected in the GDPR, which applies throughout Europe. If the PDSG were passed unchanged, I would have to formally warn the statutory health insurance companies under my supervision, which have around 44.5 million insured persons, against only implementing the ePA in accordance with the specifications of the PDSG, as this would constitute behavior that violates European law. In addition, I am preparing further measures in this context to remedy an implementation of the ePA that is contrary to European law. According to the GDPR, I have instructions as well as prohibitions at my disposal.

The PDSG only provides users of suitable end devices such as mobile phones or tablets with access to their own ePA that is sufficient under data protection law, namely document-specific control of which parties can view which information. And even this option will only be available a year after the introduction of the ePA. This means that in 2021 there will be no document level control. With regard to the data stored by the service providers in the ePA, the users are forced to make an “all or nothing”. Any person who is granted access to this data by the insured person can view all the information contained therein. For example, the treating dentist could see all the findings of the consulted psychiatrist.

The Federal Commissioner sees with incomprehension that the specifications relevant for the start of the ePA on January 1st, 2021 do not enable the health insurance companies to grant their insured persons so-called fine-grained access to the contents of the ePA stored by the service providers: digitization can never be an end in itself. The protection of the insured and

their health data must always be in the foreground.

In addition, the PDSG does not regulate independent access to the ePA for people who cannot or do not want to use the so-called front end on a cell phone or tablet, nor does it regulate whether the data has been accessed. Alternatively, from 2022, a representative should be able to control and view these front-end non-users, but the insured would then have to grant full control over their data.

The BfDI is firmly opposed to this unequal treatment of citizens' fundamental right to informational self-determination: The ePA is an important step towards further improvements in healthcare. The resulting health data requires a level of data protection as required by the GDPR and as has been firmly agreed in Germany for years for the ePA. The PDSG in its current form does not adequately do justice to this. As the responsible supervisory authority for a large part of the statutory health insurance companies, I will therefore use the regulatory means available to me to ensure that these health insurance companies do not violate European law with the ePA they offer.

Another point of criticism is the authentication procedure for the ePA, with which insured persons register via the frontend. So far, this has not been sufficiently secure from a data protection point of view and does not meet the requirements of the GDPR. The BfDI prepares appropriate warnings and instructions so that health insurance companies only allow access to health data after using a state-of-the-art, highly secure authentication process. This applies in particular to authentication procedures without using the electronic health card (so-called alternative authentications), for which a transitional period granted expires in May 2021.

The BfDI is responsible for 65 statutory health insurance companies. A list of the affected health insurance companies is available on the BfDI website.

contact finder

Here you can find out in just a few clicks who is responsible for your inquiry or complaint about data protection.

public bodies

The term public body not only includes the traditional administrative authorities, but also courts, parliaments and public foundations. This also includes social insurance, such as health insurance.

company

Private companies are mostly supervised by state authorities, but there are some exceptions. Private organizations such

as clubs and associations also fall into this category.

Press, radio, church

Special responsibilities apply in these areas. Churches and public broadcasters have e.g. B. via their own data protection officers. The federal and state supervisory authorities are not responsible for other organizations either.