50th activity report

The Hessian Commissioner for Data Protection and Freedom of Information presented an activity report for 2021

06/08/2022

The Hessian Commissioner for Data Protection and Freedom of Information presents its 50th activity report on data protection and its 4th activity report on freedom of information.

Fotolia_191229458_S.jpg

The 50th activity report on data protection records the developments in 2021. The Hessian Commissioner for Data Protection and Freedom of Information (HBDI) Prof. Dr. Alexander Roßnagel summarizes: "During the reporting period, no serious violations were found in Hesse - in contrast to developments in Germany and the world." Roßnagel continues: "In Hesse, data protection was largely accepted and not fundamentally questioned." In many areas, the requirements of the General Data Protection Regulation (GDPR) are still not sufficiently implemented, leading to complaints, requiring the intervention of the data protection supervisory authority as well as orders and enforcement measures in individual cases.

In the fourth year since the European GDPR came into force, many of the uncertainties that the abstract legal framework brought to the practice of data protection have now been overcome - e.g. on data protection in associations or on the rights of the persons concerned. The number of complaints is very high, but seems to have stabilized at this high level compared to the previous year. In the meantime, however, more complex issues that have to do with larger technical systems and new business models are coming to the fore and shaping the supervisory activity - such as advice on the digitization of administrations and companies. Reports of cyber attacks, exploitation of software vulnerabilities and data breaches have increased by half from 1,433 in 2020 to 2016 in 2021. Notices of fines have also increased significantly from 2 in 2020 to 29 in 2021 and court proceedings relating to HBDI decisions from 25 on 34

The framework for the HBDI's supervisory activities is increasingly shaped by the European data protection infrastructure of which it is a part. The European Data Protection Board (EDPB) has found its feet and has decided many controversial issues in cross-border individual issues and provided helpful clarifications in the form of recommendations, guidelines and opinions. Since decisions are primarily made in Brussels on how the abstract provisions of the General Data Protection Regulation are to be understood in practice, the HBDI is becoming more actively involved in the work of the EDPB and its working groups.

The GDPR requires intensive cooperation between the supervisory authorities of the member states in cross-border supervisory procedures. These collaborative practices have increased from 812 in 2020 to 1419 in 2021. Since it is also decided in these procedures who will have an influence on the future understanding of data protection in the European Union, intensive participation is necessary.

individual topics

Corona pandemic and data protection

The corona pandemic also shaped supervisory activities in this reporting year. The measures to combat the pandemic and the legal regulations, which are constantly changing rapidly, have resulted in ever new supervisory tasks. Examples were data processing when organizing vaccination appointments, as part of test procedures, contact tracing, maintaining the functions of day care centers, schools and universities and the processing of data on the disease and immunity status in employment relationships. To combat the pandemic, the HBDI has accepted that data protection has been restricted – e.g. when recording restaurant visits or processing employee health data. However, the HBDI complained that the fundamental rights were being restricted too far - e.g. the restriction of the rights of those affected in one of the Corona Protection Ordinances, which was then also eliminated. Overall, the HBDI comes to the conclusion that data protection was an effective support during the pandemic in the reporting period because it was an important prerequisite for trust in the state corona policy and the individual measures taken by state agencies.

video conferencing systems

Another challenge was to adapt the non-data protection-compliant conditions that had been accepted at the beginning of the pandemic to the data protection requirements. For example, video conferencing systems (VKS) were used, which illegally transferred personal data to the USA. Structural corrections were sought for these and the time necessary for the conversion was granted. After advice from the HBDI, data protection-compliant solutions could be found for the universities through the technical and organizational design of the VKS or by switching to other systems. The schools have been given the time they need to switch to a country-wide, uniform and data protection-compliant VKS. Unfortunately, the introduction of this VKS was delayed due to problems in the tender.

Digitization of work and digital tools for employee monitoring

The digitization of work makes it possible to monitor employees more and more intensively with regard to their performance

and behavior. However, it is by no means permissible to place all employees under general suspicion and to monitor them preventively from the outset. Even the mere suspicion that employees are doing private matters in the home office is not enough for complete monitoring. The argument of vehicle safety, troubleshooting or increased efficiency is also not sufficient for GPS tracking in the logistics sector.

Increasing cybercrime

The increase in cyber crime through phishing and other forms of social engineering is increasingly leading to attacks on IT systems. There have also been an increasing number of attacks using known vulnerabilities in certain software systems. In order to blackmail those responsible, the attackers encrypt the data of a company or an authority and offer the decryption key for large sums of money. They publish part of the extracted data on the dark web and threaten to publish all the data. Such attacks must be reported to the HBDI, who will review and advise on mitigation measures to be taken and how to prevent recurrences of successful attacks. These forms of cybercrime require stronger precautionary measures, quick reactions to known vulnerabilities and the repeated education of all employees about the possibilities of attacks and the measures to avoid them

cookies

On the Internet, the use of cookies is often necessary in order to recognize users and provide them with the desired services. Cookies are also often used to identify preferences, interests, behavior, habits and relationships from the surfing behavior of users and to create detailed profiles about them, which make it easier to influence them through advertising. These profiles can also contain sensitive data, e.g. B on health or sexual orientation. The Telecommunications Telemedia Data Protection Act (TTDSG), which came into force on December 1, 2021, has restricted this practice and tied it even more closely to the consent of the user. This will also be obtained in future in cookie banners. This ensures the self-determination of the user, but is annoying in everyday life. However, many providers of websites and apps now have to change their practice. Checking this will be another task of the HBDI.

video surveillance

In the year under review, the HBDI carried out intensive testing and advice on the design and realignment of video surveillance systems for the Hessian police and security authorities. Prerequisites include a crime analysis for the area where video surveillance is intended. It should also be noted that the necessary privacy zones are masked out during video surveillance so

that, for example, living rooms, interiors or the outside area of restaurants are not also recorded. The private use of video surveillance systems is also only permitted to a limited extent and may not cover public areas or the property of neighbors. In both cases, the HBDI's control resulted in a number of video cameras having to be removed.

Freedom of Information

In the year under review, there was growing interest in the freedom of information that has existed in Hesse for four years. In contrast to other federal states and the federal government, this freedom of information only applies in the state administration and in the municipalities and districts that have adopted it through statutes. Since this has still only been done by a minority, freedom of information in Hesse is practically limited. Nevertheless, the number of complaints has increased. The HBDI participated in the conference of freedom of information officers in the legal and political development of freedom of information.

With the activity report for the year 2021, the Hessian Commissioner for Data Protection and Freedom of Information Prof. Dr. Alexander Roßnagel presented his first activity report, which he was responsible for. According to Art. 59 GDPR and § 89 Para. 4 HDSIG, he is obliged to prepare a report on his activities every year.

Downloads: HBDI 50th Activity Report (PDF / 3.33 MB)

Contact for press representativesPress spokeswoman: Ms. Maria Christina RostPress and public relations: Telephone: +49 611 1408 119The Hessian Commissioner for Data Protection and Freedom of InformationP.O. Box 316365021 Wiesbaden