Digitization, data protection and pandemic

Digitization, data protection and pandemic - HmbBfDI presents the 29th activity report on data protection for the 2020 reporting year

Digitization, data protection and pandemic - HmbBfDI presents the 29th activity report on data protection for the 2020 reporting year

02/25/2021

•

activity report

The pandemic year 2020 has clearly shown that data protection is a cross-cutting issue that now extends to all areas of public and private life. Digitization has received an enormous boost from the current crisis. Just a few decades ago it was unthinkable that technical developments would open up such possibilities for communication and information. Digitization connects people with each other, makes the world accessible from the limited local perspective of the home office and ensures permanent individual participation and participation in professional and private matters. This creates technical, ethical and legal challenges. Some are entirely new, while other well-known issues are surging onto the agenda. The range of data protection-specific questions ranges from video communication systems in schools and universities for the collection of health data by employers, contact storage of visitors to public facilities to the possibilities of tracking or tracing infected people and data protection-compliant work in the home office.

The difficult task of finding an appropriate balance between the requirements of health protection and the rights and freedoms of citizens during the pandemic affects numerous fundamental rights - including the fundamental right to informational self-determination. It is part of the constitutional state's DNA to avoid all-or-nothing solutions and instead to gently balance conflicting legal positions. Contrary to popular belief, it is not about abstract priority relations between "data protection or health protection" and "data protection vs. the right to education", but about sounding out in concrete collision cases how both legal interests can be taken into account as optimally as possible. It is clear that the goal of combating the pandemic justifies significant restrictions by encroaching on civil liberties and thus also on the right to informational self-determination. It is equally clear: A transparent and rational social discussion about this cannot succeed without being informed, open and fair.

Better communication is required not only in the context of public discussions, but also between public bodies and supervisory

authorities, who not only control and instruct them, but also have to advise them. Advice on important decisions affecting privacy by bodies directly connected to the Senate is by no means a mere formality. Advice has a preventive function and can help to avoid undesirable developments as early as possible. The activity report shows that there is clearly room for improvement in some areas.

Regarding the 29th activity report, Johannes Caspar, Hamburg Commissioner for Data Protection and Freedom of Information: “This report is the last of my constitutionally stipulated maximum 12-year term of office, which ends in June. This gives reason to look back on the past few years and at the same time to look ahead. In addition to positive developments, there are unfortunately also worrying developments to be noted.”

Among the things that have developed positively are the significantly increased demand and interest in data protection help and advice from citizens. In 2020, the number of complaints and submissions has once again grown to an all-time high. On the other hand, the number of serious cases of sexually motivated recordings in Hamburg, of which children and women in particular fall victim, is alarming. However, all of these developments, as well as additional checks and fine procedures, are currently exceeding the authority's human resources and are now leading to questionable delays in the task of helping people exercise their rights in terms of the rule of law.

Johannes Caspar on this: “Data protection is fundamental rights protection and a right of the little people. The right to informational self-determination is an individual fundamental right that does not have to be enforced by individuals themselves, for example by means of expensive private lawsuits. In the EU, those affected are therefore entitled to support from the data protection supervisory authorities as completely independent bodies. In order to be able to fulfill the tasks assigned to them by law, the control bodies must be adequately equipped by the Member States. Unfortunately, this has not happened to the required extent in Hamburg in recent years. The activity report therefore contains concrete proposals for a future procedure that can help the right to complete independence and the corresponding equipment of the control body to be better enforced in the budgetary procedure as well.

Against the background of the equipment deficits, it may come as a surprise that the economic balance sheet of the authority has developed positively over the entire last decade. Due to a larger fine procedure in the reporting period, it can be stated that the authority has not only been able to bear the costs for the entire staff, the room rent and all material expenses retrospectively since 2010. In addition, the HmbBfDI has paid an average of 1.4 million euros to the Hamburg budget every

year since 2010.

Johannes Caspar: “There is a good reason why data protection supervisory authorities are not oriented towards profit principles and are politically and economically independent. Nevertheless, it is good news for taxpayers that the data protection supervisory authority has reported an overall positive balance since 2010 in Hamburg. Against this background, too, it should be assumed that in future politicians will offer the support that a modern and future-oriented data protection authority needs for its work on protecting the digital rights of citizens.”

Data has become a central economic resource with a high level of desirability. Unfortunately, the implementation of the EU General Data Protection Regulation for cross-border data processing at the European level has so far proved to be ineffective. The large internet services and platforms in particular, which process data globally and mostly have their EU headquarters in a few member states, have so far been largely spared from enforcement. The reasons for this are, among other things, bureaucratic and cumbersome procedures for applying the law, which meanwhile mean that the EU supervisory authorities are largely in a self-dealing mode.

Johannes Caspar: “Effective enforcement of the law is not only required for the rights and freedoms of those affected in the EU, it is also a key requirement for fair competition in the digital single market. The European legislature must give up its passivity and in future ensure procedural regulations that really ensure harmonized implementation and do not reward location decisions. At the same time, the central question of effective and efficient enforcement should play a much greater role than before and be prioritized in the European Data Protection Board.”

Finally, a look at the future of digitization in Hamburg, a task that is particularly relevant from the point of view of data protection: Beyond the important digitization of specific administrative procedures, which is being promoted by many individual projects at the FHH, this topic is primarily about one basic strategic positioning.

Johannes Caspar: “Hamburg's path to the digital future is already being decided today. The 2020 coalition agreement on the subject of digitization contains a clear commitment to the use of open source software in public administration and the associated transparency. The digital sovereignty of the Hamburg administration is expressly to be strengthened. This also entails considerable opportunities for data protection. The neighboring state of Schleswig-Holstein has already bravely taken this path. It is not only in Hamburg that the dependence on Big Tech, especially when using software products in the public sector, should be solved in the future. Digital sovereignty decides about a self-determined future beyond digital developments.

Only if we ourselves determine the rules of the game, according to which our information and our communication will be designed in the future, will we be able to face the difficult challenges and questions of our time in a self-determined, open and transparent manner. There is a considerable need for action here."

Individual key issues, pandemic-related and general issues from the past year are presented below.

The electronic version of the data protection activity report can be accessed here (PDF).

The following selected topics from the 29th activity report of the Hamburg Commissioner for Data Protection and Freedom of Information:

Data protection questions about Corona (p. 34 ff.):

Corona warning app:

With the development of the Corona-Warn-App (CWA), the federal government has broken new ground, both in terms of its development model and the way it works. After initial discussions about different concepts, a welcomely transparent path was chosen. The app is based on the principles of voluntariness, decentralization and open source. This has strengthened public trust in the CWA and is the reason for the now more than 25 million downloads. The Hamburg Commissioner for Data Protection and Freedom of Information has critically monitored its creation and particularly welcomes the technical advancement with several new functions.

Contact data collection:

Since May 13, 2020, the Hamburg SARS-CoV-2 Containment Ordinance has required business owners to record the names and contact details of all guests in order to trace infection chains. As a result, the HmbBfDI received almost daily complaints from citizens about restaurants with open, freely accessible contact lists. In addition, inquiries from restaurants have shown that there is often uncertainty as to how contact data can be collected in practice without violating the data protection rights of visitors. In order to sensitize innkeepers, the HmbBfDI randomly visited 100 commercial and restaurant businesses in June 2020 and checked the implementation of the contact data collection. The HmbBfDI initially focused on advising and raising awareness of those responsible on site in the implementation of contact data processing in accordance with the rules of the General Data Protection Regulation. Inadmissible open lists were found in a third of the cases. A follow-up inspection carried out in August showed that the vast majority of restaurants followed the instructions on the legal situation and successfully changed their practice. However, the same grievances persisted in four restaurants. After the first sample campaign was

primarily aimed at providing advice and raising awareness of the new legal requirements, intervention by means of the supervisory authorities was required.

Video communication systems:

Within a very short time, contact restrictions made it necessary to find alternative forms of communication with which social exchange could be maintained. In the education sector in particular, there has been a wide range of needs for video conferencing solutions since March 2020, combined with a significant increase in requests for advice in this area of responsibility. In many places, pragmatic solutions were initially sought, in which the more precise consideration of data protection issues had to take second place. In order to set clear guidelines for those responsible as to how video conference systems can be operated in compliance with data protection, the HmbBfDI was intensively involved at the level of the data protection conference in creating the orientation guide for video conference systems and was also responsible for developing a common checklist for this area. The initial response from users shows that this support is well received in practice and makes a valuable contribution to safeguarding the rights and freedoms of those affected. Particular difficulties arise when using video communication systems in schools. Due to the continuing deficits in the performance of the service provider used for the Hamburg-wide learning software, the use of different providers is the order of the day in practice. This is problematic, not only because these often do not meet the legal requirements, but also because the required on-site expertise is sometimes lacking when using and configuring them. The school authorities must counteract the resulting dangers for the personal data of those affected and the integrity of the teaching through possible disruption by third parties. Here we are waiting for feedback to support it.

H&M fine proceedings (p. 103 ff.):

H&M Online Shop AB & Co. KG was fined 35.3 million euros for breaches of employee data protection. The company has waived appeals, so that the decision has become final. The extensive collection and storage of information about the private living conditions of employees was sanctioned by superiors. These included, for example, symptoms of illness, holiday experiences and family disputes. In a complex investigation, the HmbBfDI evaluated a data set of around 60 gigabytes and interviewed numerous witnesses. The company showed understanding and, in addition to the fine, made lump-sum and unconditional compensation payments to the employees.

International data traffic according to Schrems II (p. 89 ff.):

In a groundbreaking judgment, the European Court of Justice called for a U-turn in the practice of international data traffic. The Privacy Shield and Standard Contractual Clauses, which have mainly been used to date for transfers from the EEA, can no longer be used as before. If the recipient country does not have a level of data protection comparable to the EU standard, additional measures must be taken to prevent mass surveillance by security authorities without cause. Where such additional measures are not possible, it is usually necessary to switch to European service providers. A nationwide task force, headed by the HmbBfDI, is implementing the new requirements using broad-based random samples.

Police queries (p. 109ff):

Police officers have access to various databases for official reasons. However, it happens again and again that police officers access these databases for personal reasons. The police conduct random checks to check the official justification of queries. The crimes pursued by the HmbBfDI have so far mainly related to inquiries from their own personal environment, for example about former partners or assistance for acquaintances who wanted to know whether investigations were being carried out against them. There has also been data use for attempts to flirt with informers. So far, queries from the "NSU 2.0" area have not been positively identified. However, the HmbBfDI is investigating three different cases in which such a connection to police inquiries cannot be ruled out at the current time of the investigation.

Abusive "private" recordings by third parties (p. 120ff):

Cases are increasingly being brought to the HmbBfDI in which private individuals secretly photograph or film other people on the street without their consent. These are not general street shots or shots taken in the context of disputes. Rather, it is primarily about sexually motivated shots of scantily clad women (sunbathing in the park) or shots of strange children who are often photographed or filmed in public places accompanied by their parents. So-called upskirting (i.e. filming in the intimate area under the skirt) in buses or in the park also occurs regularly. These cases are handed over to the HmbBfDI by the police or public prosecutor's office after no criminal offenses could be identified (upskirting has only been an independent criminal offense since the middle of last year). The HmbBfDI regularly punishes these violations with fines that are based on the severity of the violation and the income of the perpetrator.

press contact

rot13("Znegva Fpurzz", "xiltkpcgzdjvbons");mmehcS nitraM

Phone:

+49 40 428 54-4044

Email: rot13("cerffr@qngrafpuhgm.unzohet.qr", "lrhfmyujsncdqzwe");ed.grubmah.ztuhcsnetad@esserp