Fundamental right to data protection - high demand, long delivery time

02/13/2020 • HmbBfDI

The Hamburg Commissioner for Data Protection and Freedom of Information presents its 28th activity report on data protection for the 2019 reporting year.

The activity report presented today by the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) for the 2019 reporting year provides both an opportunity to look back and to determine where we stand in order to be able to envisage future goals. In May it will be two years in which the General Data Protection Regulation (GDPR) will be in force. Enforcement and implementation of the new regulations of data protection law are gaining momentum in Hamburg and in Germany as a whole. At the same time, however, there are also negative effects of the limited resources of the authorities on the one hand and dramatic differences in European implementation on the other.

On-site privacy

Modern data protection is multifunctional. The public must be made aware of the risks and rights associated with the processing of data. The state and society must be made more aware that the rights of citizens must be effectively protected in view of ever-increasing networking and the ever-increasing dependence of business and administration on the processing of data. At the same time, it is important, especially among young people, to promote the ability to protect their own data and respect the data of others. Here, the HmbBfDI has taken up an initiative on data protection in media education, which is currently starting with a project to promote the topic in schools.

With the help of the regulatory instruments, it must in turn be ensured that the rights of those affected are protected by the data processing bodies. Since the GDPR came into force, there has been a dramatic increase in complaints from citizens. In the last year alone, the number of complaints to the HmbBfDI grew by 25% after the number of complaints had already doubled in the year the GDPR came into force. In view of this development, the increase in personnel at the authority by just two posts in the current budget falls well short of what is required.

Johannes Caspar, Hamburg Commissioner for Data Protection and Freedom of Information: “The new awareness of citizens about their data protection rights cannot be overestimated. Complaints also give us important information about possible structural data protection problems. However, if it is not possible to use the current resources to answer the inquiries within a reasonably acceptable period of time, those affected will have a negative impression of the subject of data protection. With

additional, temporary staff, it has at least been possible to keep the number of entries and exits roughly in balance. These forces must be consolidated. In addition, the steady increase in cases and the significant backlog necessitate further reinforcement."

Privacy of the two speeds?

The extensive sanction powers to punish data protection violations are crucial for enforcing the rights and freedoms of those affected in an ever faster turning carousel of data capitalization. Unfortunately, the sanction instruments that have been harmonized across Europe are implemented very inconsistently.

Depending on where the responsible body is located, different national authorities are responsible for all activities in the case of cross-border data processing (so-called one-stop-shop procedure). This involves voting procedures among many European supervisory authorities, including referral by the European Data Protection Board, a body of all EU supervisory authorities. This is cumbersome, time-consuming and ineffective, and the results are often disappointing. Legally binding measures against global Internet services have largely failed to materialize, even after complaints. Related directional decisions on the interpretation of the GDPR are on hold.

The goals of the GDPR are thus turned into their opposite. Instead of a harmonized law enforcement, a highly different and non-transparent milieu of law enforcement cultures is emerging. Instead of establishing legal protection for the persons concerned, proceedings are postponed until they are almost forgotten. Instead of fair competition on the common market for digital services, national biotopes for digital groups are solidifying, which secure and expand their market position in Europe compared to other competitors. The impression that the big market participants in particular stand outside the regulations is fatal for the acceptance of the data protection rules.

Johannes Caspar: "The fact that no legally binding measures have been taken against the majority of the world's leading Internet service providers and platforms since the GDPR came into force, despite numerous reports of data protection violations in the last two years, and that there are not even draft decisions on this is a bad sign in the year 2 after Introduction of the GDPR. Different legal and cultural traditions in enforcement, a lack of opportunities for corrections for inactive leading authorities, different national regulations on administrative procedures and a concentration of companies in a few member states show that the concept of the one-stop shop may be well thought out, but it is not practical.

The deficits are structural and, in my view, cannot be remedied solely on a cooperative basis between the supervisory

authorities. Legal change is required. The hope that time will heal this situation is deceptive and only prolongs the current state. Time is the scarcest resource in the digitalization process. The ball is now in the European Commission's field to present suitable proposals for changes to the law as part of the evaluation report to be presented at the end of May. Waiting until the next evaluation would be fatal, because this is not scheduled to take place until 2024."

A selection of topics from the current activity report can be found below.

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

Selected topics from the current activity report below:

Digital radio fire brigade (p. 38ff): As early as 2016 it became known that the Hamburg fire brigade transmits sensitive personal data unencrypted during emergency alarms, although encryption methods have been available for this for a long time. After many delays, the Hamburg fire brigade surprisingly announced in February that the start of the introduction, which was scheduled for the beginning of the year, had to be postponed to March 2020 because the software was still faulty. That means: Even after more than 3 years, sensitive data from the emergency alarm are still being transmitted unencrypted. From the point of view of the HmbBfDI, the Hamburg fire brigade must finally do everything possible to ensure that the first aid services are equipped with the new app across the board immediately after the release of the procedure, in order to then stop the unencrypted transmission of personal data. This status makes it clear that the Hamburg fire brigade does not give sufficient priority to designing its systems in accordance with data protection.

Tracking (p. 47ff, p. 57ff, p. 83ff): Users of internet offers are often extensively observed. Tracking services track their clicks both within individual offers and across providers. This practice, which is particularly widespread on press websites, does not stop at sensitive areas such as online banking. Most of the time it is about the targeted insertion of advertising and the optimization of the offers. These are legitimate goals, but with many tracking services they can only be pursued with the consent of the user. In the reporting period, the HmbBfDI called for the introduction of corresponding consent solutions from various large providers as well as at the level of associations. This only takes effect gradually and must therefore be continued in the current year.

Videmo (p. 96ff): In 2018, the HmbBfDI had issued a deletion order to the Ministry of the Interior and Sport against an automated facial recognition software used by the Hamburg police in connection with the investigation into the G20 riots. After the interior authority had filed a complaint against this order in January 2019, the responsible administrative court in Hamburg

rendered its judgment in October 2019. The complaint of the interior authority was upheld and the deletion order was declared unlawful. The judgment of the VG Hamburg raises a number of fundamental questions in terms of data protection law, which, in addition to the legitimacy of such measures by law, also affect the scope of the HmbBfDI's inspection competencies. The HmbBfDI has therefore submitted an application for approval of the appeal.

Amendment to the Constitutional Protection Act (p. 116ff): During the reporting period, the Ministry of the Interior and Sport presented its draft amendment to the Hamburg Constitutional Protection Act. The set of regulations included significant changes in the area of data protection. Despite the very short participation periods, the HmbBfDI subjected the drafts to a critical data protection review. The Ministry of the Interior and Sport has already taken some of the concerns of the HmbBfDI into account within the coordination between the authorities. Unfortunately, other data protection concerns of the HmbBfDI were not remedied and they have now found their way into the law adopted by the citizenship in January 2020. The HmbBfDI continues to be particularly critical of the concrete design of the lowering of the protection of minors as well as new transmission powers of the state office to public and private external bodies.

Promotion of data protection competence by the HmbBfDI (p. 154ff): Digital competence is a key topic of the 21st century. Therefore, the promotion of data protection competence and media education are also among the core tasks of the HmbBfDI, because the skills of young people to protect themselves against possible risks in the digital world must be strengthened. In workshops at schools, current data protection issues are discussed and awareness-raising work is carried out. Through intensified cooperation with state media authorities and educational institutions, funding approaches could be advanced and new projects initiated. Furthermore, the HmbBfDI offers a wide range of information on data protection issues for citizens on its website.

Private photography in day-care centers and schools (p. 133 ff): With regard to the question of the admissibility of private photographs in day-care centers and schools, there is considerable uncertainty, which is reflected both in media reports and in numerous requests for advice from the HmbBfDI. In practice, photos taken by parents are to be assessed differently from a data protection point of view than photos taken by the school itself. For example, they are covered by the so-called household exception of the GDPR for purely personal or family purposes and are therefore permissible without obtaining the consent of the person depicted. However, the sharing of such photos on social networks may be different. The GDPR sets strict limits.

press contact

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

Phone:

+49 40 428 54-4044

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