PRESS RELEASE

The Hamburg Commissioner for Data Protection and Freedom of Information

25 February 2021

Digitization, Data Protection and pandemic

The Hamburg Commissioner for Data Protection and Freedom of Information presents the 29th Data Protection Activity Report for the reporting year 2020

The pandemic year 2020 impressively demonstrated that data protection is a cross-cutting issue that now extends into all areas of public and private life. Digitization has been given an enormous boost by the current crisis. Technical developments are opening up possibilities for communication and information that were unthinkable just a few decades ago. Digitization connects people with each other, makes the world accessible even from the limited local perspective of the home office, and ensures permanent individual participation and co-creation in both professional and private matters. This gives rise to technical, ethical and legal challenges. Some of them are completely new, while other familiar problems are pushing their way onto the agenda. The range of data protection-specific issues extends from video communication systems in schools and universities to the collection of health data by employers, collection of contact data of visitors to public institutions and events, and the possibilities of tracking or tracing infected persons as well as working in a home office in accordance with data protection.

The difficult task of finding an appropriate balance between the requirements of health protection and the rights and freedoms of citizens affects numerous fundamental rights - including the fundamental right to informational self-determination. It is part of the DNA of the rule of law to avoid all-or-nothing solutions and instead to strike a careful balance between conflicting legal positions. Contrary to popular opinion, this is not about abstract priority relationships between "data protection or health protection" or “data protection vs. the right to education”, but about sounding out how in concrete cases of collision both legal interests can be taken into account as good as possible. It is clear that the goal of combating the pandemic justifies significant restrictions of civil liberties and thus also of the right to informational self-determination. It is equally clear that a transparent and rational discussion on this issue cannot succeed without information, openness and fairness.

Better communication is required not only in the context of public discussions, but also between public bodies and supervisory authorities, which not only control and instruct, but also have to advise them. Consultation prior to important decisions by public bodies bearing privacy implications is by no means a mere formality. Advice has a preventive function and can help to avoid undesirable developments as early as possible. The current activity report shows that there is clearly room for improvement in some areas.

Commenting on the 29th activity report now presented, Johannes Caspar, Hamburg Commissioner for Data Protection and Freedom of Information, said: "This report is the last in my maximum 12-year term of office, which is stipulated by the constitution and ends in June. This is an occasion to look back on the past years and, at the same time, to look forward. In addition to thoroughly positive developments, there are unfortunately some worrying ones."

Among the things that have developed positively, the first thing to mention is the significant increase in demand and interest in data protection assistance and advice from citizens. In 2020, the number of complaints and submissions again rose to an all-time high. What is alarming, on the other hand, is the

The Hamburg Commissioner for Data Protection and Freedom of Information
Ludwig-Erhard-Str. 22, 20459 Hamburg
Phone: 040/42854-4040 | Fax: 040/42854-4000
E-mail: mailbox@datenschutz.hamburg.de | Internet: www.datenschutz-hamburg.de

Hamburg

number of serious cases of sexually motivated shootings in Hamburg, to which children and women in particular fall victim. However, these developments, as well as additional audits, investigations and fining proceedings, currently exceed the authority's personnel resources and are now leading to delays in the task of helping people exercise their rights that are questionable in terms of the rule of law.

Johannes Caspar: "Data protection is a fundamental right and a right of ordinary people. The right to the protection of personal data 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, data subjects therefore have a right to support from the data protection supervisory authorities as fully independent bodies. In order to fulfil the tasks assigned to them by law, the supervisory authorities must be adequately equipped by the member states. Unfortunately, this has not been done to the necessary extent in Hamburg in recent years. The activity report therefore contains concrete proposals for a future procedure that helps to better enforce the right to complete independence and the corresponding equipment of the supervisory authority in the budgetary procedure as well.

Against the background of these shortcomings, it may come as a surprise that the economic balance of the authority has developed positively over the entire last decade. For example, due to a major administrative fine in the reporting period, it can be determined that the authority has not only been able to retroactively cover the costs for all personnel, room rent and all material expenses since 2010. In addition, the HmbBfDI has paid an average of another 1.4 million euros to the Hamburg budget every year since 2010.

Johannes Caspar comments: "For good reason, data protection supervisory authorities are not profit-oriented and are politically and economically independent. Nevertheless, it is good news for taxpayers that the results of the data protection supervisory authority in Hamburg since 2010 have been positive overall. Against this backdrop, too, it should be assumed that politics will in future provide the support that a modern and forward-looking data protection authority needs for its work to protect citizens' digital rights."

Data has become a central economic resource with a high degree of covetousness. Unfortunately, enforcement of the EU General Data Protection Regulation for cross-border data processing at the European level has so far proven to be less than effective. Especially the large Internet services and platforms that process data globally and have their EU headquarters in a few member states have been largely spared in enforcement so far. The reasons for this include bureaucratic and cumbersome procedures for applying the law, which now mean that EU supervisory authorities are largely in a self-referral mode.

Johannes Caspar commented: "Effective law enforcement is not only required for the rights and freedoms of those affected in the EU, it is also a key prerequisite for fair competition in the digital single market. The European legislator must abandon its passivity and in the future ensure procedural rules that genuinely guarantee harmonized enforcement and do not reward locational advantages. At the same time, the central issue of effective and efficient enforcement should play a much stronger role than before and be prioritized in the European Data Protection Board."

Finally, let's take a look at the future of digitization in Hamburg, a task that is particularly relevant from a data protection perspective: Beyond the important digitization of concrete administrative procedures, which is being driven forward by many individual projects in the FHH, this topic is primarily about a fundamental strategic positioning.

Johannes Caspar comments: "Hamburg's path into the digital future is already being decided today. The 2020 coalition agreement on digitization contains a clear commitment to the use of open source software in public administration and the associated transparency. The digital sovereignty of

Hamburg's administration is to be explicitly strengthened. This is also associated with considerable opportunities for data protection. The neighbouring state of Schleswig-Holstein has already taken a bold step in this direction. It is not only for Hamburg that the dependence on big tech, especially in the use of software products in the public sector, should be resolved in the future. Digital sovereignty determines an autonomous future also beyond digital developments. Only if we determine the rules for handling our communication on our playing field we 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."

The electronic version of the data protection activity report is available at https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF.

Individual focal topics, pandemic-related and general issues of the past year are presented in the following appendix (in German).

Press contact:
Martin Schemm
Phone: 0049/4042854-4044
Mail: presse@datenschutz.hamburg.de

Hamburg

Nachstehend ausgewählte Themen des 29. Tätigkeitsberichts des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit:

Datenschutzfragen rund um Corona (S. 34 ff.):

Corona-Warn-App: Mit der Entwicklung der Corona-Warn-App (CWA) ist die Bundesregierung neue Wege gegangen, sowohl bei ihrem Entwicklungsmodell als auch ihrer Funktionsweise. Nach anfänglichen Diskussionen über unterschiedliche Konzepte wurde ein begrüßenswert transparenter Weg gewählt. Die App beruht auf den Prinzipien Freiwilligkeit, Dezentralität und Quelloffenheit. Dies hat das öffentliche Vertrauen in die CWA gestärkt und ist der Grund für die mittlerweile mehr als 25 Millionen Downloads. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat ihr Entstehen kritisch begleitet und begrüßt insbesondere die technische Weiterentwicklung um mehrere neue Funktionen.

Kontaktdatenerfassung: Seit dem 13.5.2020 verpflichtet die Hamburgische SARS-CoV-2-Eindämmungsverordnung Betriebsinhaber, zur Nachverfolgbarkeit von Infektionsketten die Namen und Kontaktdaten aller Gäste zu erfassen. Infolgedessen erreichten den HmbBfDI nahezu täglich Beschwerden von Bürgerinnen und Bürgern über Gaststätten mit offenen, frei zugänglichen Kontaktlisten. Zudem haben Anfragen von Gaststätten gezeigt, dass vielfach Unsicherheit besteht, wie die Kontaktdatenerhebung praktisch erfolgen kann, ohne die Datenschutzrechte der Besucherinnen und Besucher zu verletzen. Um Gastwirte zu sensibilisieren, hat der HmbBfDI im Juni 2020 stichprobenartig 100 Gewerbe- und Gaststättenbetriebe aufgesucht und die Umsetzung der Kontaktdatenerhebung kontrolliert. Den Schwerpunkt legte der HmbBfDI zunächst auf die Beratung und Sensibilisierung der Verantwortlichen vor Ort bei der Umsetzung der Kontaktdatenverarbeitung nach den Regeln der Datenschutzgrundverordnung. Dabei wurden in einem Drittel der Fälle unzulässige offene Listen vorgefunden. Eine im August durchgeführte Nachkontrolle hat ergeben, dass die weit überwiegende Anzahl der Gaststätten den Hinweisen auf die Rechtslage gefolgt und die Praxis erfolgreich umgestellt hat. In vier Restaurants bestanden jedoch nach wie vor dieselben Missstände. Nachdem die erste Stichprobenaktion primär auf die Beratung und Sensibilisierung im Hinblick auf die neuen rechtlichen Anforderungen gerichtet war, war ein Einschreiten mit aufsichtsbehördlichen Mitteln geboten.

Videokommunikationssysteme: Kontaktbeschränkungen machten es innerhalb kürzester Zeit erforderlich, alternative Kommunikationsformen zu finden, mit denen der gesellschaftliche Austausch aufrechterhalten werden kann. Insbesondere im Bildungsbereich gibt es seit März 2020 vielfältige Bedarfe nach Videokonferenzlösungen, verbunden mit einem erheblichen Anstieg der Beratungsersuchen in diesem Zuständigkeitsbereich. Vielerorts wurde zunächst nach pragmatischen Lösungen gesucht, bei denen die genauere Betrachtung der Belange des Datenschutzes hintenan stehen musste. Um den Verantwortlichen klare Vorgaben zu setzen, wie Videokonferenzsysteme datenschutzkonform betrieben werden können, hat der HmbBfDI sich intensiv auf Ebene der Datenschutzkonferenz bei der Erstellung der Orientierungshilfe zu Videokonferenzsystemen engagiert und zusätzlich federführend eine gemeinsame Checkliste für diesen Bereich erarbeitet. Die erste Resonanz aus dem Kreis der Anwendenden zeigt, dass diese Hilfestellung in der Praxis gut angenommen wird und einen wertvollen Beitrag zur Sicherstellung der Rechte und Freiheiten betroffener Personen leistet. Besondere Schwierigkeiten ergeben sich beim Einsatz von Videokommunikationssystemen im schulischen Bereich. Aufgrund weiterhin bestehender Defizite bei der Performanz des für die hamburgweite Lernsoftware eingesetzten Dienstleisters ist in der Praxis die Nutzung unterschiedlicher Anbieter an der Tagesordnung. Dies ist problematisch, nicht nur, weil diese häufig den rechtlichen Anforderungen nicht genügen, sondern weil bei deren Einsatz und deren Konfiguration mitunter auch die erforderliche Sachkunde vor Ort fehlt. Daraus resultierenden

Gefahren für die personenbezogenen Daten Betroffener sowie die Integrität des Unterrichts durch mögliche Störung von dritter Seite gilt es durch die Schulbehörde zu begegnen. Hier warten wir auf Rückmeldung, um diese zu unterstützen.

H&M Bußgeldverfahren (S. 103 ff.):

Der H&M Online Shop AB & Co. KG wurde ein Bußgeld in Höhe von 35,3 Millionen Euro für Verstöße gegen den Beschäftigtendatenschutz auferlegt. Das Unternehmen hat auf Rechtsmittel verzichtet, sodass der Bescheid rechtskräftig geworden ist. Sanktioniert wurden die umfangreiche Erfassung und Speicherung von Informationen über private Lebensumstände von Mitarbeiterinnen und Mitarbeitern durch Vorgesetze. Dazu zählten beispielsweise Krankheitssymptome, Urlaubserlebnisse und familiäre Streitigkeiten. In einem aufwändigen Ermittlungsverfahren wertete der HmbBfDI einen Datensatz von rund 60 Gigabyte aus und vernahm zahlreiche Zeuginnen und Zeugen. Das Unternehmen zeigte sich einsichtig und nahm zusätzlich zum Bußgeld pauschale und vorbehaltlose Schadenersatzzahlungen an die Beschäftigten vor.

Internationaler Datenverkehr nach Schrems II (S. 89 ff.):

Der Europäische Gerichtshof hat in einem wegweisenden Urteil zu einer Kehrtwende bei der Praxis des internationalen Datenverkehrs aufgefordert. Die bislang für Übermittlungen aus dem EWR heraus überwiegend genutzten Grundlagen Privacy Shield und Standardvertragsklauseln sind nicht mehr wie zuvor nutzbar. Herrscht im Empfängerstaat kein mit dem EU-Standard vergleichbares Datenschutzniveau, sind Zusatzmaßnahmen zu ergreifen, um etwa anlasslose Massenüberwachung durch Sicherheitsbehörden zu unterbinden. Wo solche Zusatzmaßnahmen nicht möglich sind, ist in der Regel auf europäische Dienstleister zu wechseln. Eine bundesweite Task Force setzt unter der Leitung des HmbBfDI die neuen Anforderungen mittels breit angelegter Stichproben durch.

Polizei-Abfragen (S. 109ff):

Polizeibeamtinnen und Polizeibeamte haben aus dienstlichen Gründen Zugriffe auf verschiedene Datenbanken. Es kommt jedoch immer wieder vor, dass Polizistinnen und Polizisten aus persönlichen Motiven auf diese Datenbanken zugreifen. Die Polizei betreibt Stichproben, um die dienstliche Rechtfertigung von Abfragen zu überprüfen. Die vom HmbBfDI verfolgten Taten bezogen sich bislang vor allem auf Abfragen aus dem eigenen persönlichen Umfeld, zum Beispiel über ehemalige Partnerinnen und Partner oder Hilfestellungen für Bekannte, die wissen wollten, ob gegen sie ermittelt wird. Auch Datennutzungen für Flirtversuche mit Anzeigeerstatterinnen hat es gegeben. Abfragen aus dem Bereich „NSU 2.0“ wurden bislang nicht positiv festgestellt. Allerdings ermittelt der HmbBfDI in drei verschiedenen Fällen, in denen ein solcher Bezug zu Polizeiabfragen zum gegenwärtigen Zeitpunkt der Ermittlungen nicht ausgeschlossen werden kann.

Missbräuchliche „private“ Aufnahmen von Dritten (S. 120ff):

Vermehrt werden an den HmbBfDI Fälle herangetragen, in denen Privatpersonen andere Menschen auf der Straße ohne deren Einwilligung heimlich fotografieren oder filmen. Dabei handelt es sich nicht um allgemeine Straßenaufnahmen oder im Rahmen von Streitigkeiten getätigte Aufnahmen. Vielmehr geht es vor allem um sexuell motivierte Aufnahmen von knapp bekleideten Frauen (beim Sonnenbaden im Park) oder um Aufnahmen von fremden Kindern, die häufig in Begleitung ihrer Eltern an öffentlichen Plätzen fotografiert oder gefilmt werden. Auch sog. Upskirting (also das Filmen in den Intimbereich unter dem Rock) in Bussen oder im Park kommt regelmäßig vor. Diese Fälle werden von Polizei oder Staatsanwaltschaft an den HmbBfDI abgegeben, nachdem keine Straftaten erkannt werden konnten (Upskirting ist erst seit Mitte letzten Jahres ein eigenständiger Straftatbestand). Der HmbBfDI ahndet diese Verstöße regelmäßig mit Bußgeldern, die sich an der Schwere des Verstoßes und dem Einkommen der Täter orientieren.