PRESSEMITTEILUNG

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

25. Februar 2021

Digitalisierung, Datenschutz und Pandemie

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit legt den 29. Tätigkeitsbericht Datenschutz für das Berichtsjahr 2020 vor

Das Pandemie-Jahr 2020 hat eindrücklich vor Augen geführt, Datenschutz ist ein Querschnittsthema, das mittlerweile in alle Bereiche des öffentlichen und privaten Lebens hineinreicht. Die Digitalisierung hat durch die derzeitige Krise einen enormen Schub bekommen. Noch vor wenigen Jahrzehnten war es undenkbar, dass die technische Entwicklung derartige Möglichkeiten der Kommunikation und Information eröffnet. Die Digitalisierung verbindet die Menschen miteinander, macht die Welt aus der beschränkten lokalen Perspektive des Homeoffice erreichbar und sichert eine permanente individuelle Teilnahme und Mitgestaltung in beruflichen wie in privaten Belangen. Hieraus erwachsen technische, ethische und rechtliche Herausforderungen. Einige sind gänzlich neu, andere bekannte Problemstellungen drängen mit Macht auf die Tagesordnung. Die Spanne der datenschutzspezifischen Fragestellungen reicht von Videokommunikationssystemen in Schulen und Universitäten zur Erhebung von Gesundheitsdaten durch Arbeitgeber, Kontaktdatenspeicherung von Besucherinnen und Besuchern öffentlicher Einrichtungen bis hin zu den Möglichkeiten des Tracking bzw. Tracing infizierter Personen sowie dem datenschutzgerechten Arbeiten im Homeoffice.

Die schwierige Aufgabe, in der Pandemie einen angemessenen Ausgleich zwischen den Anforderungen des Gesundheitsschutzes und den Rechten und Freiheiten von Bürgerinnen und Bürgern zu finden, betrifft zahlreiche Grundrechte – auch das Grundrecht auf informationelle Selbstbestimmung. Es gehört zur DNA des Rechtsstaats, Alles-oder-Nichts-Lösungen zu vermeiden und stattdessen kollidierende Rechtspositionen zu einem schonenden Ausgleich zu bringen. Entgegen landläufiger Meinung geht es dabei nicht um abstrakte Vorrangrelationen zwischen "Datenschutz oder Gesundheitsschutz" sowie „Datenschutz vs. Recht auf Bildung“, sondern darum, in konkreten Kollisionsfällen auszuloten, wie beide Rechtsgüter möglichst optimal berücksichtigt werden können. Es ist klar, dass das Ziel der Pandemiebekämpfung wesentliche Einschränkungen durch Eingriffe in die Freiheitsrechte und damit auch in das informationelle Selbstbestimmungsrecht rechtfertigt. Es ist gleichsam klar: Eine transparente und rationale gesellschaftliche Diskussion hierüber kann ohne Informiertheit, Offenheit und Fairness nicht gelingen.

Eine bessere Kommunikation ist nicht nur im Kontext öffentlicher Diskussionen gefordert, sondern auch zwischen öffentlichen Stellen und Aufsichtsbehörden, die diese nicht nur kontrollieren und anweisen, sondern auch zu beraten haben. Die Beratung vor wichtigen Entscheidungen mit Auswirkungen auf die Privatsphäre durch senatsunmittelbare Stellen ist keineswegs eine bloße Formalität. Beratung hat eine präventive Funktion und kann dazu beitragen, Fehlentwicklungen möglichst früh zu vermeiden. Der Tätigkeitsbericht zeigt, in einigen Bereichen ist hier deutlich Luft nach oben.

Zum nun vorgelegten 29. Tätigkeitsbericht Johannes Caspar, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit: „Dieser Bericht ist der letzte in meiner durch die Verfassung festgelegten maximal 12-jährigen Amtszeit, die im Juni endet. Dies gibt Anlass, auf die vergangenen

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22, 20459 Hamburg
Tel.: 040/42854-4040 | Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de | Internet: www.datenschutz-hamburg.de

Hamburg

Jahre zurückzublicken und gleichzeitig den Blick nach vorn zu richten. Neben durchaus positiven, sind leider auch bedenkliche Entwicklungen zu konstatieren.“

Unter den Dingen, die sich positiv entwickelt haben, sind zunächst die erheblich gestiegene Nachfrage und das Interesse an datenschutzrechtlicher Hilfe und Beratung durch die Bürgerinnen und Bürger zu nennen. Im Jahr 2020 ist die Anzahl von Beschwerden und Eingaben erneut auf ein Allzeithoch angewachsen. Erschreckend ist hingegen die Zahl gravierender Fälle von sexuell motivierten Aufnahmen in Hamburg, denen insbesondere Kinder und Frauen zum Opfer fallen. All diese Entwicklungen sowie zusätzliche Prüfungen und Bußgeldverfahren übersteigen derzeit jedoch die personellen Ressourcen der Behörde und führen mittlerweile zu rechtsstaatlich bedenklichen Verzögerungen bei der Aufgabe, Menschen bei der Ausübung ihrer Rechte zu helfen.

Hierzu Johannes Caspar: "Datenschutz ist Grundrechtsschutz und ein Recht der kleinen Leute. Das informationelle Selbstbestimmungsrecht ist ein individuelles Grundrecht, das eben nicht von Einzelnen selbst, etwa im Wege der teuren Privatklage, durchgesetzt werden muss. In der EU besteht daher ein Anspruch der Betroffenen auf Unterstützung durch die Datenschutzaufsichtsbehörden als vollständig unabhängige Stellen. Um die ihnen gesetzlich übertragenen Aufgaben erfüllen zu können, müssen die Kontrollstellen von den Mitgliedstaaten angemessen ausgestattet werden. Leider ist dies in den letzten Jahren in Hamburg nicht im erforderlichen Maße erfolgt. Der Tätigkeitsbericht enthält daher konkrete Vorschläge für ein künftiges Verfahren, das das Recht auf vollständige Unabhängigkeit und der damit korrespondierenden Ausstattung der Kontrollstelle auch im Haushaltsverfahren besser zur Durchsetzung verhelfen kann.

Vor dem Hintergrund der Ausstattungsdefizite mag überraschen, dass die wirtschaftliche Bilanz der Behörde sich über die gesamte letzte Dekade positiv entwickelt hat. So lässt sich aufgrund eines größeren Bußgeldverfahrens im Berichtszeitraum feststellen, dass die Behörde seit 2010 rechnerisch die Kosten für das gesamte Personal, die Raummiete und alle sachlichen Ausgaben rückwirkend nicht nur selbst tragen konnte. Darüber hinaus hat der HmbBfDI durchschnittlich seit 2010 in jedem Jahr noch einmal 1,4 Millionen Euro an den Hamburger Haushalt abgeführt.

Hierzu Johannes Caspar: "Datenschutzaufsichtsbehörden sind aus gutem Grund nicht an Profitgrundsätzen orientiert und politisch und wirtschaftlich unabhängig. Dennoch ist es eine gute Nachricht für die Steuerzahler, dass die Datenschutzaufsichtsbehörde im Ergebnis seit 2010 in Hamburg eine insgesamt positive Bilanz ausweist. Auch vor diesem Hintergrund sollte doch angenommen werden, dass die Politik künftig die Unterstützung bietet, die eine zeitgemäße und in die Zukunft gerichtet ausgestattete Datenschutzbehörde für ihre Arbeit zum Schutz digitaler Rechte von Bürgerinnen und Bürgern benötigt.“

Daten sind zu einer zentralen ökonomischen Ressource mit einer hohen Begehrlichkeit geworden. Leider erweist sich der Vollzug der EU-Datenschutzgrundverordnung bei grenzüberschreitender Datenverarbeitung auf der europäischen Ebene bislang als wenig effektiv. Gerade die großen Internetdienste und Plattformen, die global Daten verarbeiten und ihre EU-Hauptniederlassung größtenteils in einigen wenigen Mitgliedstaaten haben, wurden bislang im Vollzug weitgehend verschont. Ursächlich dafür sind u.a. bürokratische und schwerfällige Verfahren der Rechtsanwendung, die mittlerweile dazu führen, dass sich die EU-Aufsichtsbehörden in hohem Maße in einem Selbstbefassungsmodus befinden.

Hierzu Johannes Caspar: „Eine effektive Rechtsdurchsetzung bleibt nicht nur für die Rechte und Freiheiten der Betroffenen in der EU gefordert, sie ist auch eine zentrale Voraussetzung für einen fairen Wettbewerb auf dem digitalen Binnenmarkt. Der europäische Gesetzgeber muss seine Passivität aufgeben und künftig für Verfahrensregelungen sorgen, die einen harmonisierten Vollzug wirklich gewährleisten und keine Standortentscheidungen prämieren. Gleichzeitig sollte im

Europäischen Datenschutzausschuss die zentrale Frage nach einem effektiven und effizienten Vollzug eine viel stärkere Rolle als bisher spielen und priorisiert werden."

Abschließend noch ein Blick auf die Zukunft der Digitalisierung in Hamburg, eine Aufgabe, die gerade unter Datenschutzgesichtspunkten relevant ist: Jenseits der wichtigen Digitalisierung konkreter Verwaltungsverfahren, die durch viele einzelne Projekte in der FHH vorangetrieben wird, geht es bei diesem Thema vor allem auch um eine grundsätzliche strategische Positionierung.

Hierzu Johannes Caspar: "Hamburgs Weg in die digitale Zukunft entscheidet sich bereits heute. Der Koalitionsvertrag von 2020 zum Thema Digitalisierung enthält ein klares Bekenntnis zum Einsatz von Open Source-Software in der öffentlichen Verwaltung und der damit verbundenen Transparenz. Ausdrücklich soll die digitale Souveränität der Hamburger Verwaltung gestärkt werden. Damit sind auch erhebliche Chancen für den Datenschutz verbunden. Das Nachbarland Schleswig-Holstein ist auf diesem Weg bereits mutig vorangegangen. Nicht nur für Hamburg gilt, dass die Abhängigkeit von Big Tech, insbesondere beim Einsatz von Software-Produkten im öffentlichen Sektor, künftig gelöst werden sollte. Die digitale Souveränität entscheidet über eine selbstbestimmte Zukunft auch jenseits digitaler Entwicklungen. Nur wenn wir selbst über die Spielregeln bestimmen, nach denen zukünftig unsere Informationen und unsere Kommunikation gestaltet werden, sind wir in der Lage, uns selbstbestimmt, offen und transparent den schwierigen Herausforderungen und Fragen unserer Zeit zu stellen. Hier besteht erheblicher Handlungsbedarf."

Einzelne Schwerpunktthemen, pandemiebedingte und allgemein Fragestellungen des letzten Jahres werden in der Anlage dargestellt.

Aufgrund der Corona-Pandemie hat der HmbBfDI in diesem Jahr von einer Pressekonferenz zur Vorstellung des Tätigkeitsberichts abgesehen.

Die elektronische Fassung des Datenschutz-Tätigkeitsberichts kann unter https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF abgerufen werden.

Pressekontakt:
Martin Schemm
Telefon: 040/42854-4044
E-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.