

13. Februar 2020

Grundrecht Datenschutz – große Nachfrage, lange Lieferzeit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit legt seinen 28. Tätigkeitsbericht Datenschutz für das Berichtsjahr 2019 vor

Der heute vorgelegte Tätigkeitsbericht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) zum Berichtsjahr 2019 gibt sowohl Anlass zurückzublicken als auch eine Standortbestimmung vorzunehmen, um die künftigen Ziele ins Auge fassen zu können. Im Mai werden es zwei Jahre, in denen die Datenschutzgrundverordnung (DSGVO) gültig ist. Durchsetzung und Umsetzung der neuen Regelungen des Datenschutzrechts nehmen in Hamburg und auch in Deutschland insgesamt an Fahrt auf. Gleichzeitig zeigen sich aber auch zum einen negative Auswirkungen der limitierten Behördenressourcen und zum anderen dramatische Unterschiede im europäischen Vollzug.

Datenschutz vor Ort

Moderner Datenschutz ist multifunktional. Die Öffentlichkeit ist für die Risiken und Rechte im Zusammenhang mit der Verarbeitung von Daten zu sensibilisieren. In Staat und Gesellschaft muss das Bewusstsein geschärft werden, dass angesichts einer immer stärkeren Vernetzung und einer immer größeren Abhängigkeit der Wirtschaft und der Verwaltung von der Verarbeitung von Daten die Rechte der Bürgerinnen und Bürger effektiv zu schützen sind. Gleichzeitig gilt es, insbesondere bei jungen Menschen die Kompetenz für den Schutz der eigenen und den Respekt vor den Daten anderer zu fördern. Hier hat der HmbBfDI eine Initiative zum Datenschutz in der Medienbildung aufgenommen, die aktuell mit einem Projekt der Förderung des Themas an Schulen startet.

Mit Hilfe der aufsichtsbehördlichen Instrumente wiederum muss sichergestellt werden, dass die Rechte Betroffener seitens der Daten verarbeitenden Stellen gewahrt werden. Seit Inkrafttreten der DSGVO ist ein dramatischer Anstieg von Beschwerden durch Bürgerinnen und Bürger zu verzeichnen. Allein im letzten Jahr wuchs das Beschwerdeaufkommen beim HmbBfDI um 25%, nachdem im Jahr des Inkrafttretens der DSGVO bereits eine Verdoppelung der Eingabenzahlen erfolgte. Die personelle Aufstockung der Behörde um lediglich zwei Stellen im aktuellen Haushalt bleibt angesichts dieser Entwicklung deutlich hinter den Erforderlichkeiten zurück.

Hierzu Johannes Caspar, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit: "Das neue Bewusstsein von Bürgerinnen und Bürgern über ihre Datenschutzrechte kann nicht hoch genug veranschlagt werden. Beschwerden geben uns auch wichtige Hinweise auf mögliche strukturelle Datenschutzprobleme. Wenn es jedoch nicht gelingt, mit den derzeitigen Ressourcen die Anfragen in zeitlich halbwegs akzeptablen Zeiträumen zu beantworten, bleibt bei den Betroffenen ein negativer Eindruck beim Thema Datenschutz zurück. Mit zusätzlichem, befristetem Personal ist es zuletzt immerhin gelungen, Eingänge und Ausgänge in etwa in der Waage zu halten. Diese Kräfte müssen verstetigt werden. Zudem machen der stetige Zuwachs von Fällen und die erheblichen Rückstände eine weitere Verstärkung erforderlich."

Datenschutz der zwei Geschwindigkeiten?

Die umfangreichen Sanktionsbefugnisse zur Ahndung von Datenschutzverstößen sind entscheidend für die Durchsetzung von Rechten und Freiheiten Betroffener in einem sich immer schneller

drehenden Karussell der Datenkapitalisierung. Leider werden die europaweit harmonisierten Sanktionsinstrumente sehr uneinheitlich umgesetzt.

Je nach Sitz der verantwortlichen Stelle sind unterschiedliche nationale Behörden bei grenzüberschreitenden Datenverarbeitungen federführend für deren gesamte Aktivitäten zuständig (sog. One-Stop-Shop-Verfahren). Hierbei sind Abstimmungsverfahren unter vielen europäischen Aufsichtsbehörden zu bewältigen, einschließlich der Befassung durch den Europäischen Datenschutzausschuss, einem Gremium aller EU-Aufsichtsbehörden. Dies gestaltet sich schwerfällig, zeitaufwändig und ineffektiv und bleibt im Ergebnis häufig enttäuschend. Rechtsverbindliche Maßnahmen gegen global agierende Internetdienste sind auch nach Beschwerden bislang weitgehend ausgeblieben. Damit verbundene Richtungsentscheidungen zur Auslegung der DSGVO liegen auf Eis.

Die Ziele der DSGVO werden so in ihr Gegenteil verkehrt. Statt eines harmonisierten Rechtsvollzugs entsteht ein höchst unterschiedliches und intransparentes Milieu der Vollzugskulturen. Statt Rechtsschutz für betroffene Personen herzustellen, werden Verfahren hinausgeschoben, bis sie nahezu in Vergessenheit geraten. Statt eines fairen Wettbewerbs auf dem gemeinsamen Markt für digitale Dienstleistungen verfestigen sich nationale Biotope für Digitalkonzerne, die ihre Marktstellung in Europa gegenüber anderen Wettbewerbern sichern und ausbauen. Für die Akzeptanz der Datenschutzregeln ist der Eindruck fatal, gerade die großen Marktteilnehmer stünden jenseits der Vorschriften.

Hierzu Johannes Caspar: „Dass gegen die Mehrzahl der global führenden Internetdienstleister und Plattformen seit Geltung der DSGVO trotz zahlreicher Meldungen über Datenschutzverletzungen in den letzten beiden Jahren keinerlei rechtsverbindliche Maßnahmen erlassen wurden, noch nicht einmal Entscheidungsentwürfe dazu vorliegen, ist ein schlechtes Zeichen im Jahr 2 nach Einführung der DSGVO. Unterschiedliche rechtlich-kulturelle Traditionen im Vollzug, fehlende Korrekturmöglichkeiten für untätige federführende Behörden, unterschiedliche nationale Vorschriften zum Verwaltungsverfahren sowie eine Massierung von Unternehmen in wenigen Mitgliedstaaten, zeigen: Das Konzept des One-Stop-Shop mag gut gedacht sein, ist aber nicht praxistauglich.“

Die Defizite sind strukturell und lassen sich aus meiner Sicht allein auf kooperativer Basis zwischen den Aufsichtsbehörden nicht beheben. Es bedarf der rechtlichen Umsteuerung. Die Hoffnung, der Faktor Zeit werde diese Situation heilen, ist trügerisch und verlängert nur den derzeitigen Zustand. Zeit ist die knappste Ressource im Prozess der Digitalisierung. Der Spielball liegt nun im Feld der EU-Kommission, im Rahmen des Ende Mai vorzulegenden Evaluationsberichts geeignete Vorschläge für Rechtsänderungen zu präsentieren. Ein Zuwarten bis zur nächsten Evaluation wäre fatal, denn diese findet turnusgemäß erst 2024 statt.“

Eine Auswahl von Themen des aktuellen Tätigkeitsberichts findet sich auf den nachfolgenden Seiten.

Die elektronische Fassung des Datenschutz-Tätigkeitsberichts kann unter „https://datenschutz-hamburg.de/assets/pdf/28_Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf“ abgerufen werden.

Pressekontakt:

Martin Schemm

Telefon: 040/42854-4044

E-Mail: presse@datenschutz.hamburg.de

Nachstehend ausgewählte Themen des aktuellen Tätigkeitsberichts:

Digitalfunk Feuerwehr (S. 38ff): Bereits 2016 wurde bekannt, dass die Feuerwehr Hamburg bei der Notfallalarmierung sensible personenbezogene Daten per Funk unverschlüsselt überträgt, obwohl seit langem hierfür Verschlüsselungsverfahren zur Verfügung stehen. Nach vielen Verzögerungen hatte die Feuerwehr Hamburg im Februar überraschen mitgeteilt, dass der für den Jahresbeginn angesetzte Beginn der Einführung auf März 2020 verschoben werden muss, da die Software noch fehlerhaft sei. Das heißt: Auch nach über 3 Jahren werden immer noch sensible Daten der Notfallalarmierung unverschlüsselt übertragen. Aus Sicht des HmbBfDI muss die Feuerwehr Hamburg endlich alles daran setzen, nach der Freigabe des Verfahrens umgehend für eine flächendeckende Ausstattung der Erstversorgungswehren mit der neuen App zu sorgen, um dann die unverschlüsselte Übertragung personenbezogener Daten abzustellen. Dieser Stand macht deutlich, dass die Feuerwehr Hamburg einer datenschutzgerechten Ausgestaltung ihrer Systeme keine ausreichende Priorität einräumt.

Tracking (S. 47ff, S. 57ff, S. 83ff): Nutzer von Internetangeboten werden häufig umfassend beobachtet. Tracking-Dienste verfolgen deren Klicks sowohl innerhalb einzelner Angebote als auch über Anbieter hinweg. Diese vor allem bei Webauftritten der Presse weit verbreitete Praxis macht auch vor sensiblen Bereichen wie etwa dem Online-Banking nicht Halt. Meist geht es um das zielgenaue Einspielen von Werbung und die Optimierung der Angebote. Dies sind berechnete Ziele, die jedoch bei vielen Tracking-Diensten nur mit Einwilligung der Nutzer verfolgt werden können. Der HmbBfDI hat im Berichtszeitraum sowohl bei verschiedenen großen Anbietern als auch auf der Ebene von Verbänden die Einführung entsprechender Einwilligungs-Lösungen eingefordert. Dies entfaltet nur nach und nach Wirkung und muss daher auch im laufenden Jahr fortgesetzt werden.

Videmo (S. 96ff): Im Jahr 2018 hatte der HmbBfDI eine Löschanordnung gegen eine von der Polizei Hamburg anlässlich der Ermittlungen zu den G20-Ausschreitungen eingesetzte automatisierte Gesichtserkennungssoftware gegenüber der Behörde für Inneres und Sport erlassen. Nach Klageerhebung durch die Innenbehörde im Januar 2019 gegen diese Anordnung hat das zuständige Verwaltungsgericht Hamburg im Oktober 2019 nun sein Urteil gefällt. Der Klage der Innenbehörde wurde stattgegeben und die Löschanordnung für rechtswidrig erklärt. Das Urteil des VG Hamburg wirft in datenschutzrechtlicher Hinsicht eine Reihe grundsätzlicher Fragen auf, die neben der Legitimierung solcher Maßnahmen durch Gesetz auch den Umfang der Überprüfungs Kompetenzen des HmbBfDI betreffen. Der HmbBfDI hat daher einen Antrag auf Zulassung der Berufung gestellt.

Novellierung Verfassungsschutzgesetz (S. 116ff): Die Behörde für Inneres und Sport hat im Berichtszeitraum ihren Entwurf zur Novellierung des Hamburgischen Verfassungsschutzgesetzes vorgelegt. Das Regelungswerk beinhaltet erhebliche Änderungen im Bereich des Datenschutzes. Der HmbBfDI hat die Entwürfe trotz sehr kurzer Beteiligungsfristen einer kritischen datenschutzrechtlichen Prüfung unterzogen. Einigen Bedenken des HmbBfDI hat die Behörde für Inneres und Sport bereits innerhalb der Behördenabstimmung Rechnung getragen. Anderen datenschutzrechtlichen Bedenken des HmbBfDI wurde bedauerlicherweise nicht abgeholfen und sie haben nun Eingang in das im Januar 2020 durch die Bürgerschaft angenommene Gesetz gefunden. Besonders kritisch sieht der HmbBfDI weiterhin die konkrete Ausgestaltung der Herabsetzung des Schutzes Minderjähriger sowie neuartige Übermittlungsbefugnisse des Landesamts an öffentliche und auch private externe Stellen.

Datenschutzkompetenzförderung durch den HmbBfDI (S. 154ff): Digitale Kompetenz ist ein Schlüsselthema des 21. Jahrhunderts. Daher gehören die Datenschutzkompetenzförderung und Medienbildung auch zu den Kernaufgaben des HmbBfDI, denn die Fähigkeiten zum Selbstschutz junger Menschen vor möglichen Risiken in der digitalen Welt müssen gestärkt werden. In Workshops an Schulen wird über aktuelle Datenschutzthemen gesprochen und Sensibilisierungsarbeit geleistet. Auch konnten durch intensivierte Kooperation mit Landesmedienanstalten und Bildungseinrichtungen Förderansätze vorangetrieben und neue Projekte initiiert werden. Des Weiteren bietet der HmbBfDI auf seiner Website ein breites Informationsangebot zu Datenschutzkompetenzfragen für Bürgerinnen und Bürger an.

Privates Fotografieren in Kitas und Schulen (S. 133 ff): Hinsichtlich der Frage der Zulässigkeit privater Fotografien in Kitas und Schulen besteht eine erhebliche Unsicherheit, die sich sowohl in der medialen Berichterstattung als auch in zahlreichen Beratungsanfragen beim HmbBfDI widerspiegelt. In der Praxis sind Fotoaufnahmen durch Eltern in datenschutzrechtlicher Hinsicht anders zu beurteilen als Fotoaufnahmen durch die Schule selbst. Sie sind etwa zu rein persönlichen oder familiären Zwecken von der sogenannten Haushaltsausnahme der DSGVO erfasst und damit auch ohne Einholung einer Einwilligung der Abgebildeten zulässig. Anderes kann jedoch für das Teilen derartiger Fotos in sozialen Netzwerken gelten. Ihm sind durch die DSGVO enge Grenzen gesetzt.