PRESSEMITTEILUNG

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

21. Februar 2018

Datenschutz am Beginn einer neuen Zeitrechnung

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit legt seinen 26. Tätigkeitsbericht Datenschutz für die Jahre 2016/2017 vor

Im Vorfeld der ab Mai 2018 europaweit geltenden Datenschutzgrundverordnung (DSGVO) werfen die gesetzlichen Neuerungen längst ihre Schatten voraus. Datenschutzaufsichtsbehörden, aber auch die gesamte öffentliche Verwaltung sowie die Unternehmen in Europa stellen sich intensiv auf diesen Wandel ein. Diese Umstellung und Neujustierung war auch für die Behörde des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) in den letzten beiden Jahren ein bestimmender Faktor.

Dazu Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: „Im Datenschutz bleibt in 2018 kein Stein auf dem anderen. Ob und inwieweit es Unternehmen, aber auch Aufsichtsbehörden gelingt, die neuen Regelungen und die daraus erwachsenden Aufgaben und Pflichten zeitgerecht umzusetzen, wird sich zeigen. In Hamburg bleibt die Situation der Aufsichtsbehörde auch weiterhin sehr angespannt. Nach einem erneuten Anstieg der Eingabenzahlen in 2017 auf ein neues Jahreshoch wird es sehr schwer werden, die mit der DSGVO verbundenen Aufgaben zeitgerecht zu bewältigen. Das alles darf aber nicht von der positiven Tatsache ablenken, dass mit Geltung der neuen Regelungen im Datenschutz auf EU-Ebene eine neue Zeitrechnung beginnt. Datenschutz ist kein Selbstzweck zur Aufblähung von Behördenstrukturen, sondern dient direkt dem Schutz der Privatsphäre von Bürgerinnen und Bürgern. Dass dieser immer schwerere und komplexere Anforderungen stellt, zeigen die vielen Baustellen der letzten beiden Jahre: Die Durchsetzung der Anforderungen der Datensicherheit in den Behörden, die Kontrolle der rechtmäßigen Datenhaltung der Polizei oder zahlreiche gerichtliche Verfahren mit Beteiligung von internationalen Konzernen, die ihren Hauptsitz in der Hansestadt haben – Datenschutz ist längst zu einem Mega-Thema in Staat und Gesellschaft geworden, das unser aller Zukunft betrifft.“

Nicht zuletzt um den neuen Herausforderungen Rechnung zu tragen, wurde auch das Konzept des Tätigkeitsberichts des HmbBfDI erneuert. Der vorliegende 26. Tätigkeitsbericht stellt die Arbeit der Hamburger Datenschutzaufsichtsbehörde nun nach rein output-orientierten Kriterien vor. So bilden Prüfungen, Berichte, rechtsverbindliche Anordnungen und Bußgelder, Beratungen und Datenschutz-kommunikation sowie Informationen zur Behörde (u.a. Statistiken) die Hauptkapitel.

Die elektronische Fassung des 26. Tätigkeitsberichts Datenschutz 2016/2017 kann auf der Website des HmbBfDI unter „www.datenschutz-hamburg.de“ abgerufen werden.

Pressekontakt:
Martin Schemm
Telefon: 040/42854-4044
E-Mail: presse@datenschutz.hamburg.de

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6, 20095 Hamburg
Tel.: 040/42854-4040 | Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de | Internet: www.datenschutz-hamburg.de

Hamburg

Nachstehend einige ausgewählte Themen des aktuellen Tätigkeitsberichts:

Polizei und G20-Gipfel (S. 22ff): Die Überprüfungen von Datenspeicherungen bei der Polizei Hamburg haben ergeben, dass häufig die rechtlichen Anforderungen für die Speicherung personenbezogener Daten nicht erfüllt waren. So musste bei den Speicherungen sowohl in landeseigenen Dateien als auch in Verbunddateien u.a. festgestellt werden, dass es an der Erforderlichkeit bzw. einer notwendigen Negativprognose fehlte, dass nachfolgende Erkenntnisse wie z.B. Strafverfahrensausgänge nicht oder nicht zeitnah berücksichtigt wurden und dass Daten nicht rechtzeitig gelöscht wurden. In einer der geprüften Dateien führte die Löschung von 3.794 Datensätzen bzw. von 87 % des Datenbestandes zu einem datenschutzkonformen Zustand. Die Ankündigung der Polizei Hamburg, den gesamten Datenbestand von ca. 900.000 Datensätzen zu etwa 160.000 Personen zu bereinigen, ist daher zu begrüßen. Auch die aufwendige datenschutzrechtliche Aufarbeitung der polizeilichen Arbeit während des G20-Gipfels ergab, dass es hierbei ebenfalls organisatorischen Mängeln geschuldet war, dass unbefugte Dritte Kenntnis von denjenigen Namen von Journalisten erlangen konnten, die auf einer Liste zwecks Entziehung der Akkreditierung genannt waren. Insgesamt muss die Polizei ihre Anstrengungen verstärken, um in Zukunft die Datenhaltung und den Datenumgang datenschutzkonform auszugestalten.

E-Mail-Verschlüsselung bei Sozialdaten (S. 41 ff.): Eine Prüfung im Jugendamt ergab, dass durchweg Sozialdaten per E-Mail ohne erforderliche Ende-zu-Ende-Verschlüsselung versendet werden, die die Kenntnisnahme der Inhalte durch Unbefugte ausschließt. Es ist zwingend erforderlich, dass den Jugendämtern die Möglichkeit der E-Mail-Kommunikation erhalten bleibt; anderenfalls würde gerade in Krisensituationen, in denen es auf eine schnelle Hilfegewährung ankommt, das Kindeswohl durch Zeitverlust zusätzlich gefährdet. Allerdings muss auch der hohe Schutzbedarf der Sozialdaten angemessen berücksichtigt werden. Ein Bruch der Vertraulichkeit würde insbesondere für die betroffenen Kinder und Jugendlichen zu einer erheblichen Beeinträchtigung ihrer gesellschaftlichen Stellung und ihres Ansehens führen. Eine Transportverschlüsselung reicht hier nicht aus. Die Behörde für Arbeit, Soziales, Familie und Integration wurde gebeten, kurzfristig entsprechende Maßnahmen zu ergreifen, die dem Schutzbedarf der Daten der Kinder und Jugendlichen entsprechen. Zwischenzeitlich wurde mit der Erarbeitung eines erhöhten E-Mail-Schutzes begonnen.

Bußgelder bei unerlaubter Videoüberwachung (S. 71ff): Im Berichtszeitraum wurde ein Bußgeldverfahren gegen das Betreiben mehrerer Video-Kameras in den Gasträumen eines Restaurants verhängt. Das AG Hamburg sieht die Videoüberwachung von Gasträumen ebenso wie die Datenschutzaufsicht grundsätzlich als unzulässig an und folgte unserer Begründung des Bußgeldbescheids im Wesentlichen. Die verantwortliche Stelle wurde wegen vorsätzlich unbefugter Erhebung und Verarbeitung personenbezogener Daten verurteilt. Zu unserem Bedauern – nicht aber zu unserer Überraschung - wurde das Bußgeld trotz einer jahrelangen rechtswidrigen Überwachungspraxis der Gäste und einer komfortablen Einkommenslage des Gastronomieunternehmens von ursprünglich 5000 Euro auf 1000 Euro herabgesetzt. Leider ist dies kein Einzelfall. Mit der ab Mai 2018 geltenden Datenschutzgrundverordnung wird der Bußgeldrahmen bei vorsätzlichen Datenschutzverletzungen von 300.000,- € auf 20 Millionen € (oder 4% des weltweiten Jahreskonzernumsatzes) ganz wesentlich angehoben. Es ist zu erwarten, dass Datenschutzverletzungen künftig nicht mehr als Bagatellvergehen angesehen werden, die mit Bußgeldern belegt werden, von denen keinerlei Abschreckungseffekt ausgeht. Das gilt nicht für die Datenschutzaufsicht, sondern auch für die Gerichte.

Das Verfahren HERAKLES der Kasse.Hamburg (S. 39f): Im Februar 2016 war es rund 6.600 Beschäftigten der Behörden und Ämter möglich, mittels freier Suche im Buchhaltungsprogramm HERAKLES der Stadt Hamburg auf über 2 Millionen Kontenstammdatensätze der Kasse.Hamburg zuzugreifen. Somit waren u.a. personenbezogene Daten wie Name, Anschrift und Kontoverbindungen aufgrund des unzureichenden Zugriffsberechtigungskonzepts frei zugänglich. Bereits 2015 wurde die verantwortliche Finanzbehörde vom HmbBfDI auf die mangelhaften Zugriffsregelungen hingewiesen (vgl. 25. TB, VIII 2.2). Dennoch ist es dem HmbBfDI erst nach fast drei Jahren gelungen, angemessene Zugriffsberechtigungen zu vereinbaren, die jedoch aufgrund fehlender Funktionen wie u.a. Protokollierungen noch immer nicht vollumfänglich zufriedenstellen können.

Verschlüsselung von Funkdaten bei der Feuerwehr (S. 36ff): Das Digitale Alarmierungssystem der Feuerwehren in der Stadt überträgt die Daten unverschlüsselt, wodurch deren Inhalte mitgeschnitten werden können, obwohl seit den 2000er Jahren grundsätzlich die technischen Voraussetzungen für eine Verschlüsselung erfüllt sind. Nachdem wir im September 2016 über diese Missstände informiert worden sind, sah die Feuerwehr keinerlei Handlungsbedarf, ihr System anzupassen. Erst nachdem Angaben zu Einsätzen (z.B. Anschriften, Namen, Diagnosen) im Frühjahr 2017 mehrmals illegal im Internet veröffentlicht wurden, erkannte die Polizei die Problematik und arbeitet seitdem mit den Herstellern der Geräte an einer Lösung. Unter anderem sollen so bis Mitte 2018 neue Geräte beschafft werden, die auch mit dem nachfolgenden Alarmierungssystem TETRA-BOS-Digitalfunk kompatibel sind.

Smart Meter Rollout in Hamburg (S. 107ff): Die Digitalisierung der Energiewende erreicht in den kommenden Jahren jeden Hamburger Haushalt. Mit dem Messstellenbetriebsgesetz hat der Gesetzgeber die Weichen für ein intelligentes Stromnetz gestellt. Ziel ist die Harmonisierung des zunehmenden Anteils erneuerbarer Energien mit der Stromnachfrage. Dazu ersetzen ‚intelligente Messsysteme' und ‚moderne Messeinrichtungen' bis 2032 die derzeit verwendeten analogen Messgeräte. Das Grundrecht auf informationelle Selbstbestimmung wird insbesondere durch die selbstständig kommunizierenden intelligenten Messsysteme auf die Probe gestellt. Denn aus Verbrauchsmenge und -zeitpunkt können Rückschlüsse auf die private Lebensführung gezogen werden. Zwar hat der Gesetzgeber die Gefahren weitgehend erkannt und ein enges Maßnahmenkorsett normiert. Ob dieses ausreichend sein wird, muss in den kommenden Jahren kritisch beobachtet werden. Diesem Auftrag wir der Hamburgische Beauftragte nachkommen.

Digitale Stadt (S. 93ff): Der Senat der FHH treibt Hamburgs Rolle als „Digitale Stadt" voran. Mit diesem Stichwort verbunden sind weitreichende Planungen und Visionen für eine Stadt von morgen, in der Bürger ihre Behördengänge online erledigen oder sich gänzlich ersparen können (antraglose Verwaltung), in der E-Government die Regel und Papier die Ausnahme ist, in der Sensoren im Straßenraum energie- und zeitsparend den automatisierten öffentlichen Verkehr lenken. Solche Visionen sind wichtig und für den Fortschritt unerlässlich. Gleichzeitig werfen sie viele Datenschutzfragen auf, die beantwortet werden müssen, damit solche Vorhaben rechtskonform aufgestellt werden und am Ende auch gelingen können. Wir sind auf verschiedenen Ebenen mit den beteiligten Behörden im Gespräch. Neben vielen praktischen Fragen der technischen Konzeptionierung und Umsetzung zeigt sich, dass auch das Recht weiterentwickelt werden muss, um solche neuen Konzepte möglich zu machen. Gerade hier tut sich Hamburg allerdings schwer. Noch immer wird vom Senat offenbar kein Bedarf gesehen, durch ein E-Government-Gesetz den rechtlichen Rahmen für die Digitalisierung von Verwaltungsverfahren zu schaffen, wie dies im Bund

und in den meisten anderen Ländern bereits erfolgt ist. Wir werden weiter auf entsprechende Regelungen drängen.

Google-Suchergebnisse – „Recht auf Vergessenwerden“ (S. 82): Nach wie vor erreichen uns viele Beschwerden über die Praxis von Google im Zusammenhang mit Anträgen von Betroffenen, Suchergebnisse sperren zu lassen, die bei der Eingabe ihres Namens in die Google-Suchmaschine angezeigt werden. Häufig können wir den Betroffenen zur Durchsetzung ihrer Rechte verhelfen, allerdings besteht auch aus unserer Sicht nach Abwägung der Umstände nicht immer ein Anspruch auf Sperrung der unerwünschten Ergebnisse. In einzelnen Fällen haben sich Betroffene, die mit unserer Entscheidung nicht zufrieden waren, an das Verwaltungsgericht gewandt, um ein entsprechendes Vorgehen gegen Google durch uns zu erzwingen. Dies hat das VG allerdings abgelehnt und Ansprüche der Betroffenen, die über die Entgegennahme, Prüfung und Ergebnismitteilung ihrer Beschwerde hinausgehen, verneint. In zwei Fällen wird sich das Verfahren beim OVG fortsetzen.

Safe Harbor und Privacy Shield (S. 75ff): Nachdem der Europäische Gerichtshof das Safe-Harbor-Abkommen zwischen der EU und den USA für ungültig erklärt hatte, hat der HmbBfDI etliche Unternehmen zunächst darauf aufmerksam gemacht. Damit hatten diese die Gelegenheit, ihre Datenübermittlungen in die USA der veränderten Rechtslage anzupassen. Das überprüfte der HmbBfDI einige Monate später bei mehr als 30 großen Unternehmen. Lediglich in drei Fällen mussten wegen Datenschutzverstößen in diesem Bereich Bußgelder verhängt werden. Nach Inkrafttreten des Privacy Shield prüfte der HmbBfDI gleichzeitig mit 9 anderen Bundesländern die Datenübermittlungen in Drittländer in Hamburg erneut. Hierzu wurden 11 sehr unterschiedliche Unternehmen ausgesucht, die einen Fragenkatalog zu beantworten hatten. Keines der Unternehmen hatte sich datenschutzwidrig verhalten, so dass auf weitere Maßnahmen verzichtet werden konnte.