PRESSEMITTEILUNG

25. Februar 2016

Über dem Limit und im Umbruch

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit zieht in seinem 25. Tätigkeitsbericht Bilanz der Jahre 2014/2015

Der Datenschutz befindet sich derzeit in einer tiefgreifenden Umbruchphase. Auf europäischer Ebene wurde die Diskussion um die EU-Datenschutzgrundverordnung abgeschlossen. Das Datenschutzrecht wird im Wesentlichen vereinheitlicht, eventuell werden Aufgaben abgegeben, in jedem Fall werden im Rahmen des sogenannten One-Stop-Shops und des Kohärenzverfahrens neue Aufgaben hinzukommen. Die Diskussion um ein neues „Safe Harbor"-Abkommen nach der Entscheidung des Europäischen Gerichtshofs, der die alte Rechtsgrundlage für Datenübermittlungen in die USA im Oktober 2015 gekippt hat, befindet sich in vollem Gange. Gleichzeitig haben sich die Aufgaben der Datenschutzbehörden qualitativ und quantitativ verändert: Immer mehr Menschen machen ihre Datenschutzrechte aktiv geltend, die Digitalisierung hat das Leben in allen Bereichen ergriffen. Es stellt daher einen Anachronismus dar, dass die Behörde des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit mit ihren rund 16 Planstellen unter dem Strich nicht einmal so gut ausgestattet ist wie zu Beginn der 2000er Jahre.

Die digitale Entwicklung – das zeigt der heute vorgelegte Tätigkeitsbericht – hat auch im vergangenen Berichtszeitraum die Anforderungen an die Arbeit der Hamburger Datenschutzbehörde weiter erhöht. Neue Entwicklungen, neue Aufgaben und neue Herausforderungen haben die alten Probleme weiter verschärft: Während die digitale Welt sich rasend schnell verändert, ist die Hamburger Aufsichtsbehörde immer weniger in der Lage, die vielfältigen Anforderungen an einen zeitgemäßen Datenschutz technisch und rechtlich zu erfüllen. Das betrifft nicht nur die Ansprüche der Bürgerinnen und Bürger auf ein effizientes Beschwerdemanagement, sondern auch die Erwartungen von privaten und öffentlichen Stellen an Beratungen und Begleitungen von Verfahren.

In einem Tätigkeitsbericht lässt sich nicht umfassend darstellen, welche Aufgaben ungelöst und welche Datenschutzverstöße ungeahndet geblieben sind. Es wurde dem Bericht daher ein Anhang beigefügt, der bestehende Ausstattungsdefizite und deren Auswirkungen bei der täglichen Arbeit aufzeigt. Aber schon die Masse und Bandbreite der Themen des Tätigkeitsberichts macht deutlich, dass sich der Hamburgische Datenschutzbeauftragte am Rande des noch Machbaren bewegt.

Dazu Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: „Der Tätigkeitsbericht der letzten beiden Jahre zeigt: Der Datenschutz in Hamburg ist über dem Limit. Wird er nicht personell besser aufgestellt, wird es nicht gelingen, den vielfältigen Herausforderungen gerecht zu werden, die mit der neuen europaweit geltenden Datenschutzgrundverordnung künftig verbunden sind und die sich täglich aus zahlreichen Eingaben und Beratungsanfragen ergeben. Insoweit freue ich mich auf den Fortgang der Diskussion über die rechtliche Stärkung und Verbesserung der Ausstattung, die in den nächsten Monaten zu führen sein wird, und hoffe, dass am Ende ein tragfähiges Ergebnis stehen wird, das dem effizienten Schutz der digitalen Grundrechte für die Zukunft angemessen Rechnung trägt."

Eine Auswahl der Themen des 25. Tätigkeitsberichts ist dieser Pressemitteilung beigefügt.

Pressekontakt:

Arne Gerhards

Tel.: 040/42854-4153

E-Mail: presse@datenschutz.hamburg.de

Ausgewählte Themen des 25. Tätigkeitsberichts des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (Anhang zur Pressemitteilung)

Datensicherheit im Netz der Freien und Hansestadt Hamburg (FHH)? Interne und externe Verschlüsselung von E-Mails (25.TB VI 1.4)

Die Prüfung des Hamburgischen Datenschutzbeauftragten hat gezeigt, dass sich Administratoren der Stadt mit wenigen Klicks Zugriff auf jede E-Mail verschaffen könnten. Die Wahrscheinlichkeit, dass ein solcher Missbrauch aufgedeckt würde, ist minimal. Dadurch ist die Vertraulichkeit von sensiblen Daten, beispielsweise im Jugendamt oder bei der Polizei, stark gefährdet. Nach Jahren der Diskussion mit der Finanzbehörde konnten wir immerhin erreichen, dass alle Rechner der FHH mit einem Verschlüsselungs-Modul ausgestattet werden sollen, mit dem eine Verschlüsselung von E-Mails, die innerhalb des FHH versandt werden, mit nur zwei zusätzlichen Klicks möglich wäre. Aber auch fast zwei Jahre nach der Zusage sind immer noch nicht alle Rechner nachgerüstet. Die Polizei hat zudem erklärt, dass sie diese Vorgabe nicht umsetzen wird. Auch gibt es immer noch nicht die von uns eingeforderte Richtlinie, die alle Mitarbeiterinnen und Mitarbeiter verpflichtet, dieses Verschlüsselungs-Modul zu nutzen, wenn eine E-Mail sensible Daten enthält.

Bei der E-Mail-Kommunikation mit Externen hält die FHH den Stand der Technik nicht ein, obwohl dies nach § 8 Abs. 1 Hamburgisches Datenschutzgesetz erforderlich ist. Zum Stand der Technik gehört, dass eine Transportverschlüsselung zwischen Mail-Servern, die sog. TLS-Verschlüsselung, aktiviert ist. Diese übliche Basis für eine sichere interne Verbindung wird aber bei einer Kommunikation zwischen Bürger und Verwaltung durch die FHH nach wie vor nicht erreicht. Dabei hat die Finanzbehörde dem Hamburgischen Datenschutzbeauftragten seit April 2014 mittlerweile fünf Termine genannt, zu denen die Transportverschlüsselung für E-Mails an oder von Externen umgesetzt werden sollte. Diese Termine sind alle verstrichen, ohne dass der gravierende Mangel behoben wurde. Ein neuer Umsetzungstermin wurde für März 2016 angekündigt. Wir sind gespannt, ob es die Finanzbehörde nun schaffen wird, ihn einzuhalten?

Das Projekt Herakles – kein Herkules des Datenschutzes (25.TB VIII2.2)

Es erfordert wahrlich große Kräfte, das Projekt HERAKLES der Finanzbehörde, mit dem eine soweit wie möglich automatisierte und papierlose Rechnungsbearbeitung mit Buchungen für die FHH realisiert werden soll, zu stemmen. Aber die Kraft, mit der die Finanzbehörde die Aufgabe angeht, das Verfahren datenschutzgerecht zu betreiben, wird einem Herkules nicht gerecht.

Anfang 2015 wurden wir durch Hinweise von Beschäftigten darauf aufmerksam gemacht, dass über 5.000 interne Nutzer der FHH in einem riesigen Datenbestand mit über 2 Millionen Datensätzen suchen konnten. Alleine der Name einer Person reicht aus, um diese Suche zu starten. Da hierfür kein dienstlicher Anlass abgefragt wird, sind dem Missbrauch Tür und Tor geöffnet. So kann auf diese Weise nach privaten Adressen und Bankdaten von Kolleginnen und Kollegen, von Senatsmitgliedern, von Verwandten oder Freunden gesucht werden. Nach sehr zähen Gesprächen mit der Finanzbehörde konnte der Datenschutzbeauftragte erreichen, dass das IT-Verfahren nun bis zum April 2016 geändert werden soll. Zukünftig müssen u.a. immer das Aktenzeichen oder die Rechnungsnummer als Anlass der Suche eingegeben werden. Eine technisch kleine Korrektur, die allerdings erst nach über einem Jahr zugesagt wurde.

Das Smarte Hamburg – digitale Agenda der FHH (25. TB VI 1.7, 2.1, 2.2 und 2.4)

Die Digitalisierung aller Lebensbereiche ist eine Herausforderung, der sich die FHH mit besonderem Interesse widmet. Dass nach dem Willen des Senats ausdrücklich auch der Datenschutz ein Projektbestandteil werden soll, ist erfreulich. Datensparsamkeit, Zweckbindung, Verschlüsselung und Transparenz sind nur einige der Prinzipien, die bei der Umsetzung datenschutzrechtlicher

Anforderungen praktische Relevanz erhalten. Sicherlich können technische Möglichkeiten und eine zunehmende Vernetzung in verschiedenen Zusammenhängen sinnvolle und erprobenswerte Neuerungen mit sich bringen sowie durch den Aufbau von E-Governance und städtischer Infrastruktur Innovationsräume schaffen. Entscheidend ist aber, dass die Projekte sich in den bestehenden Rechtsrahmen einordnen und das informationelle Selbstbestimmungsrecht der Betroffenen gewahrt wird, auch wenn es sich zunächst nur um Pilotprojekte handelt. Während jedes einzelne Projekt selbst für den Datenschutz und die Datensicherheit verantwortlich ist, hat der Hamburgische Datenschutzbeauftragte als Mitglied der eigens eingerichteten Lenkungsgruppe sowie einer entsprechenden Koordinierungsrunde die Gelegenheit, datenschutzrechtliche Aspekte bereits zentral einzubringen. Bisher wurde er in folgende konkrete Projekte eingebunden:

Beim **„Intelligenten Bürgerservice“** kann in einer räumlich abgeschlossenen, nicht einsehbaren Box, die in einem Einkaufszentrum aufgestellt wird, mittels geschützter Fernkommunikation ein Kita-Gutschein beantragt werden. Hier sind technische Sicherheitsaspekte ebenso zu beachten wie der Schutzbedarf der verarbeiteten personenbezogenen Daten und die Frage, inwieweit zur Realisierung des informationellen Selbstbestimmungsrechtes die Einwilligung der Bürgerinnen und Bürger eingeholt werden kann.

Der Hafen spielt für Hamburg eine sehr wichtige Rolle. Hier bietet der technische Fortschritt besonderes Potential, wie sich auch an der Vielzahl der dortigen Projekte zeigt. Der Bereich **smartPORT logistics** dient u.a. der Erstellung einer intelligenten Infrastruktur für einen reibungslosen Ablauf der Verkehrs- und Warenströme. Da hierbei jedoch Techniken wie Bluetooth, WLAN und mobile Endgeräte genutzt werden sollen, kommt es auch zur Verarbeitung personenbezogener Daten. Die Hamburg Port Authority hat eine Reihe von datenschutzrechtlichen Hinweisen durch die Datenschutzbehörde erhalten, die beispielsweise auch den Einsatz von Videotechniken und die Beachtung des Mitarbeiterdatenschutzes betreffen.

Bei dem Projekt der **Reisezeiterfassung** auf der A7 soll den Verkehrsteilnehmerinnen und Verkehrsteilnehmern während des Ausbaus der A7 optimale Alternativrouten per App angeboten werden. Dazu sollen auch aktuelle Daten über weitere Verkehrsstörungen, zum Beispiel bei Überlastung einer der Alternativrouten, einbezogen werden. Um das zu erreichen, werden an mehreren Messpunkten die MAC-Adressen von allen bluetooth-fähigen und entsprechend aktivierten Geräten, die sich in vorbeifahrenden Fahrzeugen befinden, ausgelesen und verarbeitet. Da dieses Verfahren die Zuordnung der erhobenen Daten am nächsten Messpunkt erfordert, hat der Hamburgische Datenschutzbeauftragte unter anderem empfohlen, die erfassten MAC-Adressen zu kürzen und zu verschleiern. Die Möglichkeit zur Profilbildung muss in jedem Fall ausgeschlossen werden.

Hamburger Health Studie – so gesund ist die Stadt (25. TB II 1.3)

Das UKE startet mit der Hamburg City Health Studie eines seiner größten Forschungsprojekte: Die Daten und Proben von 45.000 Bürgerinnen und Bürger sollen erfasst, untersucht und ausgewertet werden, um neue Erkenntnisse zu den häufigsten Volksleiden wie z.B. Herz-Kreislauf-Erkrankungen, Schlaganfall, Demenz und Krebserkrankungen zu erhalten. Selbstverständlich müssen Datenschutz und Datensicherheit dabei einen hohen Stellenwert haben. Wenn die Bürgerinnen und Bürger ihre Gesundheitsdaten der Forschung überlassen und sich auch mit genetischer Forschung einverstanden erklären, dann muss sichergestellt sein, dass all diese sensiblen personenbezogenen Daten auch bestmöglich geschützt werden.

Über einen Zeitraum von mehr als zwei Jahren hat der Hamburgische Datenschutzbeauftragte die datenschutzrechtlichen Planungen des UKE begleitet. Schließlich wurde ein Studiendesign entwickelt, das sowohl den datenschutzrechtlichen Belangen als auch den Forschungsinteressen genügt. Das UKE muss die im Datenschutzkonzept niedergeschriebenen Anforderungen und

Regelungen umsetzen. Obwohl es in Anbetracht des hohen Schutzbedarfes der hier verarbeiteten personenbezogenen Daten dringend erforderlich ist, die praktische Einhaltung des Datenschutzes vor Ort zu kontrollieren, wird dies dem Hamburgischen Datenschutzbeauftragten aber mangels ausreichender personeller Kapazitäten voraussichtlich weder bei der Hamburg City Health Studie noch bei irgendeinem der vielen weiteren Forschungsprojekte möglich sein.

Polizei und Datenschutz – zwischen verdeckten Ermittlern, Gefahrengebieten und Bodycams (25. TB IV 1.2, 1.3 und 1.5)

Die Verarbeitung personenbezogener Daten durch Sicherheitsbehörden steht immer wieder im Fokus der Datenschutzaufsicht. Dies gilt insbesondere deshalb, weil die hoheitliche Datenerhebung und -verarbeitung in diesen Bereichen häufig ohne Kenntnis der Betroffenen in Betracht kommt und auch erfolgt. Die unbestrittene Bedeutung einer effektiven Gefahrenabwehr und Strafverfolgung befreit nicht von der Bindung an verfassungsrechtliche Grundlagen, wie das Recht auf informationelle Selbstbestimmung der Betroffenen. So sehen die gesetzlichen Regelungen unter bestimmten formellen und materiellen Voraussetzungen auch die Möglichkeit einer **verdeckten Ermittlung** durch die Polizei vor. Der langjährig praktizierte Einsatz von sogenannten Beobachtern für Lagebeurteilungen, die gerade in Abgrenzung zu einem verdeckten Ermittler eingesetzt wurden, genügte hingegen den hohen verfassungsrechtlichen Anforderungen nicht. Da das durch die Beobachtungen erfolgte Erheben und das anschließende Speichern personenbezogener Daten in Berichten in das informationelle Selbstbestimmungsrecht der Betroffenen eingriff, ohne dass hierfür – insbesondere im Hinblick auf die verdeckt erfolgte Datenverarbeitung – eine gesetzliche Grundlage bestand, war es folgerichtig, dass die Polizei zukünftig auf den Einsatz von Beobachtern für Lagebeurteilungen verzichtet. Die umfangreichen Prüfungen des Hamburgischen Datenschutzbeauftragten zum Thema verdeckte Ermittler müssen aber dennoch intensiv weitergeführt werden, damit die Berücksichtigung datenschutzrechtlicher Anforderungen auch bei diesem gesetzlich zugelassenen Ermittlungsinstrument geklärt ist.

Vergleichbares gilt auch für sogenannte **Gefahrengebiete**. Die Verarbeitung personenbezogener Daten in ausgewiesenen Gefahrengebieten durch die Polizei ist insbesondere nur dann rechtmäßig, wenn sie verhältnismäßig und verfassungskonform erfolgt. Hier hat das Oberverwaltungsgericht Hamburg die Sicht der Datenschutzaufsichtsbehörde bestätigt: Die einschlägige gesetzliche Grundlage (§ 4 Abs. 2 S. 1 PolDVG) dürfte verfassungsrechtlichen Anforderungen nicht genügen. Soweit die Polizei an diesem Instrument zur Verhütung von Straftaten weiterhin festhalten will, ist eine verfassungskonforme Änderung der gesetzlichen Regelung nun rechtsstaatlich dringend geboten.

Der Hamburgische Datenschutzbeauftragte war außerdem in die gesetzliche Einführung der **Bodycams** bei der Polizei eingebunden. Der Großteil unserer Anregungen wurde vom Gesetzgeber aufgegriffen, unsere Bedenken hinsichtlich der schrankenlosen Verankerung der „technischen Mittel“ im Gesetzestext, der Erforderlichkeit von Tonaufnahmen oder der den Interessen der Betroffenen entgegenstehenden kurzen Speicherfrist der Aufzeichnungen leider nicht. Wichtig ist nun, dass die Geeignetheit von Bodycams im praktischen Einsatz evaluiert wird.

Google Privatsphärebestimmungen – Was lange währt... Teil 1 (25. TB V 1.2)

Seit über drei Jahren befasst sich der Hamburgische Datenschutzbeauftragte gemeinsam mit verschiedenen anderen europäischen Aufsichtsbehörden mit den Datenschutzbestimmungen bei Google. Diese gelten für alle Nutzer, egal ob sie ein Nutzerkonto bei dem Unternehmen haben oder ob sie beispielsweise – und aus ihrer Sicht anonym – googeln. Google möchte in jedem Fall Nutzungsprofile erstellen, um sie dann für Werbung oder die Weiterentwicklung ihrer Produkte verwenden zu können. Aufgrund der Kritik, dass dafür keine Rechtsgrundlage besteht, hat das Unternehmen nun auf ein bekanntes Instrument im Datenschutz zurückgegriffen: die Einwilligung.

Die meisten Nutzerinnen und Nutzer dürften die entsprechenden Hinweise bereits gesehen und die Erklärungen vermutlich auch abgegeben haben. Trotz dieser vom Grundsatz her positiven Entwicklung kann der Hamburgische Datenschutzbeauftragte aktuell noch keinen Schlussstrich unter die Anordnung ziehen, die er in diesem Zusammenhang gegenüber Google erlassen hat. Denn ein solches Einwilligungsmodell darf keine „Alles-oder-nichts-Situation“ sein. Nutzerinnen und Nutzer müssen vielmehr über Einstellungsmöglichkeiten verfügen, die den Umfang der Profilbildung effektiv beeinflussen. Ob dies im erforderlichen Maß der Fall ist, wird zurzeit noch geprüft. Zudem hat Google bereits gegen die Anordnung geklagt, so dass auch die gerichtliche Ebene noch eine Rolle spielen wird.

Facebook – Klarnamenpflicht unter Micky Mäusen (25. TB V 2.2)

Aufgrund der Beschwerde einer Facebook-Nutzerin über die Sperrung ihres Kontos hat der Hamburgische Datenschutzbeauftragte angeordnet, dass das soziale Netzwerk den Zugriff wieder eröffnen muss. Dies gilt auch dann, wenn die Nutzerin weiterhin nicht ihren echten Namen, sondern ein selbst gewähltes Pseudonym für dieses Konto verwendet. Die sogenannte Klarnamenpflicht ist ein Prinzip, das Facebook unter seinen Nutzern konsequent durchsetzen möchte. Wer aber Facebook-Nutzer mit Varianten des Namens „Micky Mouse“ sucht, merkt schnell, dass dies in der Praxis nicht wirklich gelingt. Eine solche Pflicht widerspricht dem im Telemediengesetz zugesicherten Anspruch des Nutzers, Telemedien unter Pseudonym nutzen zu können, wenn dies technisch möglich und dem Anbieter zumutbar ist. Da in dem konkreten Fall beide Kriterien erfüllt sind, wurde Facebook aufgefordert, das Telemediengesetz umgehend entsprechend umzusetzen. Gegen die sofortige Vollziehbarkeit der Anordnung hat Facebook das Verwaltungsgericht Hamburg angerufen. Dort liegt die Sache nun seit nahezu einem halben Jahr. Während dieser langen Zeit wartet die Nutzerin weiterhin darauf, ihr Facebook-Konto unter dem gewünschten Profilnamen fortführen zu können.

Fußballinformationsportal: Fair Play gilt auch beim Datenschutz (25. TB V 10.)

Der organisierte Fußball hat in Deutschland einen besonderen Stellenwert. Profis und Amateure sind in zahllosen Vereinen und Ligen engagiert. Entsprechend groß ist das Interesse der Öffentlichkeit an Informationen über Spiele und Daten von Spielern. Durch eine Beschwerde wurde der Hamburgische Datenschutzbeauftragte auf ein bekanntes Informationsportal in Hamburg aufmerksam gemacht, das solche Daten in großem Umfang zum Abruf bereitstellt.
Dem nachvollziehbaren öffentlichen Interesse steht dabei der Persönlichkeitsschutz des einzelnen Spielers entgegen. Beide Interessen müssen in Ausgleich gebracht werden. Dies war bei dem Portal insbesondere in Hinblick auf minderjährige Spieler und auch auf Gesundheitsdaten nicht der Fall. Den betroffenen Sportlern muss zudem mehr Mitsprache in Form von Einwilligungen oder Widerspruchsrechten eingeräumt werden. Dies gilt gerade gegenüber Amateursportlern.

Online-Kredite für die Welt – aber ohne deutschen Datenschutz (25. TB VIII 1.6)

Ein Startup-Konzern mit Hamburger Holding vergibt Kleinkredite über Online-Portale an Kunden im Ausland. Die Kreditentscheidung erfolgt automatisiert durch Scoring-Algorithmen, die Daten in unverhältnismäßigem Umfang erhalten. So fließt beispielsweise das Verhalten der Antragsteller auf verschiedenen Internetseiten ein. Zudem werden sie aufgefordert, in eine Auswertung ihrer Facebook-Timeline einzuwilligen, wodurch auch Daten Dritter einbezogen werden. Ein Löschkonzept existiert dabei nicht. Dieses dem nationalen Datenschutz zuwiderlaufende Geschäftskonzept ist möglich durch die Ausgestaltung der Konzernstruktur, die alle Verantwortlichkeit auf ausländische Tochterunternehmen verlagert. Die Holding in Hamburg entzieht sich so weitgehend der Kontrolle der nationalen Datenschutzaufsicht, sodass lediglich Verbesserungen der Datensicherheit erreicht werden konnten. Gegen die Datenverarbeitung selbst

können jedoch nur die Aufsichtsbehörden in den Ländern der Tochterunternehmen vorgehen, die über die Missstände informiert wurden.

Warndatei im Versandhandel – Was lange währt… Teil 2 (25. TB VIII 1.4)

Ein Großverfahren gegen einen Hamburger Versandhauskonzern wurde nach vielen Jahren zu einem guten Ergebnis gebracht. Hintergrund waren insgesamt 33 Kundendateien der einzelnen Konzernunternehmen. Im Rahmen der Neukundenkreditprüfung nahmen die jeweiligen Unternehmen Abrufe in den Datenbanken anderer vor. Diese Praxis ist wegen des Interesses der Versandhändler, Waren ohne Vorkasse nur an zuverlässige Kunden auszuliefern, nicht grundsätzlich ausgeschlossen. Das Verfahren muss sich jedoch an den strengen Regelungen des Bundesdatenschutzgesetzes für Auskunfteien orientieren, die bei dem Konzern nicht implementiert waren. In Kooperation mit den Aufsichtsbehörden anderer betroffener Bundesländer konnte erreicht werden, dass der Konzern das System regulär als Auskunftei bei uns angemeldet hat und nun die gesetzlichen Voraussetzungen für den Datenaustausch umsetzt.

Safe Harbor – Der Hafen, der nie sicher war (25. TB X 1.)

Personenbezogene Daten dürfen nur dann in Drittstaaten außerhalb der EU übermittelt werden, wenn dort ein angemessenes Datenschutzniveau sichergestellt ist. Dies war nach einer Entscheidung der EU-Kommission aus dem Jahr 2000 in den USA der Fall, wenn sich US-Unternehmen selbst zertifizierten, dass sie die Safe Harbor-Standards einhalten. Nachdem sich zeigte, dass nur wenige dieser Unternehmen die Standards tatsächlich umsetzten und zudem die anlasslose Massenüberwachung durch US-Geheimdienste bekannt wurde, hat der Europäische Gerichtshof am 6.10.2015 die Kommissionsentscheidung zu Safe Harbor für ungültig erklärt. Infolge dieses Urteils müssen deutsche Unternehmen nun Alternativen für Ihren transatlantischen Datenverkehr etablieren oder darauf verzichten. Der Cloud-Dienstleister Dropbox hat beispielsweise angekündigt, Speicherkapazitäten nach Deutschland zu verlagern. Der Hamburgische Datenschutzbeauftragte hat Prüfungen von 35 Hamburger Unternehmen begonnen, die bislang von der nun ungültigen Safe Harbor-Entscheidung Gebrauch gemacht haben. Viele haben die Grundlage ihres Datenverkehrs inzwischen auf die Standardvertragsklauseln der EU-Kommission umgestellt. Wo dies nicht geschehen ist, werden zurzeit aufsichtsbehördliche Maßnahmen eingeleitet.