PRESSEMITTEILUNG

20. Februar 2014

Datenschutz made in Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hat der Bürgerschaft seinen Tätigkeitsbericht 2012/2013 vorgelegt.

Die Enthüllungen des Whistleblowers Edward Snowden haben im vergangenen Jahr die öffentlichen Diskussionen zum Thema Datenschutz beherrscht und reißen nicht ab. In bisher ungeahnter Dimension wurden und werden Bürgerinnen und Bürger von Geheimdiensten ausgespäht. Angesichts immer umfassenderer Überwachungsprogramme müssen wir uns fragen: Haben wir überhaupt die vollständige Kontrolle über unsere Daten? Nein, wir verlieren sie jeden Tag mehr und mehr. Daraus ergibt sich: Datenschutz erfordert globales Denken und gleichzeitig lokales Handeln.

Daher gilt es, vor Ort – also mit Blick auf die Daten verarbeitenden Stellen in Hamburg – eine informationelle Fremdbestimmung zu verhindern und einen sorgsamen Umgang mit unseren Daten einzufordern. Datenschutz ist wie kaum ein anderes Sachgebiet ein Querschnittsthema der Informationsgesellschaft. Ihn auf allen Gebieten des sozialen Lebens gegenüber privaten Akteuren wie auch gegenüber öffentlichen Stellen durchzusetzen, ist beschwerlich und oft das sprichwörtliche „Bohren dicker Bretter“.

Der aktuelle Tätigkeitsbericht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit beleuchtet die Arbeit der vergangenen zwei Jahre auf über 270 Seiten in all ihren Facetten. Exemplarisch sind hier zu nennen:

- Wesentlich für die modernen Herausforderungen des Datenschutzes ist eine sichere Infrastruktur der Datenverarbeitung. Die Freie und Hansestadt Hamburg hat eine neue Telefontechnologie eingeführt (Next Generation Network, NGN), die auf der **Internettelefonie** (VoIP) basiert. Alle entsprechenden Telefongespräche der Behördenmitarbeiter und -mitarbeiterinnen werden dabei über die gleiche Infrastruktur wie die behördeninternen Datenverbindungen abgewickelt. Die FHH hat dabei aus Kostengründen entgegen unserer Forderung auf eine Verschlüsselung der Datenströme verzichtet. Das Risiko, dass Gesprächsinhalte unberechtigt abgehört werden, wird dabei in Kauf genommen. Dies betrifft die Privatsphäre der Beschäftigten ebenso wie die der Bürger, sofern deren personenbezogene Daten Gegenstand von Telefonaten innerhalb der FHH werden.
- Die **sozialen Netzwerke** haben unsere Kommunikation von Grund auf revolutioniert, sie haben aber auch unsere Privatsphäre wesentlich verletzlicher gemacht. Dass öffentliche Stellen zusehends soziale Netzwerke nutzen wollen, ist ein nachvollziehbares Anliegen, das zu diskutieren und zu prüfen ist.
  - ➔ Darf die Polizei ihre Öffentlichkeitsfahndung über soziale Netzwerke betreiben? Wenn ja, unter welchen Voraussetzungen und Bedingungen? Hier muss verhindert werden, dass Dritte die Öffentlichkeitsfahndung als Aufruf zur Selbstjustiz und zu Hetzjagden im

Internet missbrauchen. Im Übrigen sind die weiteren rechtlichen Voraussetzungen sehr genau zu prüfen.

➔ Schulen werden künftig für die tägliche Kommunikation zwischen Lehrern und Schülern soziale Netzwerke nutzen oder selbst anbieten. Deren datenschutzrechtliche Risiken müssen erkannt und minimiert werden. So ist auszuschließen, dass Dritte schul- und jahrgangsübergreifende Bildungsprofile einzelner Schülerinnen und Schüler erstellen. Jugendliche dürfen nicht gezwungen werden, unbewusst erhebliche Risiken der Kommunikationstechnologie einzugehen.

- Das Verhalten im Internet und der Einsatz der eigenen Daten muss erlernt werden wie das Verhalten im Straßenverkehr. Der Hamburgische Datenschutzbeauftragte hat sich deshalb – neben seiner Initiative „Meine Daten kriegt ihr nicht“ – an dem Projekt „**Hamburger Medienpass**“ der Schulbehörde beteiligt und 2013 das Modul „Datenschutz und soziale Netzwerke“ erstellt. Lehrerinnen und Lehrer erhalten hierin für die 5. bis 8. Jahrgangsstufe umfangreiches Unterrichtsmaterial zur Medien- und Datenschutzkompetenz insbesondere im Umgang mit sozialen Netzwerken.
- Zur Aufklärung und **Gefahrenabwehr** haben alle Polizeikräfte Zugriff auf umfangreiche Dateien. Der Hamburgische Datenschutzbeauftragte hat erreicht, dass die Stichprobenkontrollen der Zugriffs-Protokolle in Zukunft nachvollziehbar dokumentiert und damit erstmals einer Überprüfung zugänglich werden.

  Nicht durchsetzen konnte er sich dagegen bislang mit der Forderung, auf die vorsorgliche Sicherheitsüberprüfung aller Mitarbeiter staatlich beauftragter Abschleppunternehmer zu verzichten, was Kosten für eine ständige Bewachung einer Kfz-Verwahrstelle einsparen soll.
- Verschiedene **Datenschutzpannen in Krankenhäusern und Arztpraxen** zeigen, dass der Schutz der Patientendaten immer wieder neu gesichert werden muss. So hatte beispielsweise eine Hamburger Klinik bei der Entsorgung von Altakten weder hinreichende Regelungen mit den Entsorgern getroffen noch den Zugang zu den Patienten- und Personaldaten ausreichend gesichert.
- Zahnärzte drängten auch Kassenpatienten schon vor dem ersten Arztkontakt zur Einwilligung zu **Bonitätsabfragen**. Schließlich wurden auch Arztbriefe aufgrund fehlerhafter Eingabe der Faxnummer an falsche und damit unberechtigte Dritte übermittelt, denen dann hoch sensible Gesundheitsdaten des Patienten bekannt wurden.
- **Google** räumt sich mit neuen Privatsphärebestimmungen das Recht ein, alle Daten zu verknüpfen, die von den Nutzern bei den verschiedenen Diensten anfallen, ob Suchmaschine, Youtube oder Gmail. Im Rahmen einer europäischen Taskforce hat die Hamburgische Datenschutzaufsicht ein Verwaltungsverfahren dagegen angestrengt.
- Der Hamburgische Datenschutzbeauftragte hat sich außerdem für eine Verbesserung der Kontrollmöglichkeiten der Nutzerinnen und Nutzer bei der Verarbeitung sensibler personenbezogener Daten durch Soziale Netzwerkbetreiber insbesondere **Facebook** stark gemacht. Beispielsweise ist nach Auffassung der Datenschutzaufsicht die Verarbeitung biometrischer Daten im Wege der Gesichtserkennung nur mit einer informierten, freiwilligen und aktiven Einwilligung der Betroffenen zulässig. Am Ende eines langwierigen Verfahrens und umfangreicher Verhandlungen mit Facebook zog es das Unternehmen vor, eher die Gesichtserkennungsfunktion zu deaktivieren als die geforderte Einwilligung zu implementieren.

- In Hamburg ist Wohnraum ein knappes Gut. **Wohnungssuchende** müssen oftmals schon weit vor Vertragsabschluss eine Vielzahl persönlicher Angaben machen, um überhaupt als Mieter in Betracht zu kommen. Damit die Wohnungssuche nicht zu einer umfassenden Selbstoffenbarung wird, hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit eine Informationsschrift entwickelt. Sie klärt darüber auf, ob und zu welchem Zeitpunkt welche Daten der Mietinteressenten erhoben werden dürfen.
- Die Anzahl der von Unternehmen und Privatpersonen eingesetzten **Videoüberwachung** nimmt stetig zu. Hamburger und Hamburgerinnen werden nicht nur in öffentlichen Verkehrsmitteln und auf der Straße, sondern auch in Einkaufszentren, in Cafés und in Hotels in großem Umfang überwacht. Jede Beschwerde, die der Datenschutzbeauftragte von Bürgerinnen und Bürgern zu einer Videoüberwachungsanlage erhält, muss im Einzelnen geprüft werden. Das ist derzeit aus Kapazitätsgründen kaum noch möglich.

„Die atemberaubende digitale Entwicklung der letzten 10 Jahre hat die Arbeit der Datenschutzbehörden wesentlich komplexer gemacht. Qualität und Quantität der modernen Herausforderungen des Datenschutzes setzen angemessen ausgestattete Aufsichtsbehörden voraus, die den technischen und rechtlichen Anforderungen auf der Höhe der Zeit begegnen können. Datenschutz und Datensicherheit erfordern ein Konzept der intelligenten Steuerung, das neben der Aufgabe des Rechtsvollzugs einen Schwerpunkt auf die Aufklärung der Betroffenen und die Beratung von verantwortlichen Stellen setzt. Dies gilt gerade an einem Medienstandort wie Hamburg. Vor diesem Hintergrund muss die Ausstattung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit künftig diesen modernen Herausforderungen angepasst werden“, so Johannes Caspar, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit.

Der Tätigkeitsbericht kann beim Hamburgischen Datenschutzbeauftragten kostenlos angefordert werden und steht unter www.datenschutz-hamburg.de als Download zur Verfügung.

Pressekontakt/ Rückfragen:
Arne Gerhards, Tel. 040/42854-4153