REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ BKA-817.362/0002-DSR/2010
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An
Herrn Bundeskanzler
Werner Faymann

In Kopie an
Herrn Staatssekretär
Dr. Josef Ostermayer

Betrifft: **Ermittlung und Verarbeitung von Daten zu WLAN-Netzwerken sowie Nutzdaten aus offen zugänglichen WLAN-Netzwerken Stellungnahme des Datenschutzrates**

Der **Datenschutzrat** hat in seiner 196. Sitzung am 25. Mai 2010 **einstimmig beschlossen**, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Vorbemerkungen

Der Datenschutzrat hat bereits in seiner Stellungnahme vom 15. Juli 2009 zur Veröffentlichung von Geodaten und Aufnahmen von Straßenzügen im Internet festgestellt, dass für die Aufnahme und Veröffentlichung von Fotografien von Straßenzügen durch verschiedene Diensteanbieter eine Rechtsgrundlage geschaffen werden sollte, um klarzustellen, wie Anbieter vorzugehen haben, und weiters die Bevölkerung vor ausufernden Aktivitäten der Anbieter zu schützen. Grundsätzlich sollte sichergestellt werden, dass die Daten nicht ins Ausland übermittelt werden, solange diese nicht anonymisiert worden sind. Die Veröffentlichung von Aufnahmen soll ausschließlich ohne Personenbezug erfolgen.
Weiters hat der Datenschutzrat in seiner Stellungnahme vom 15. Juli 2009 folgende Empfehlungen/ Forderungen aus datenschutzrechtlicher Sicht beschlossen:

- Da für die Aufnahme und Speicherung von Bildern von Straßenzügen mit Personen, deren Identität bestimmt oder bestimmbar ist, und bei denen auch sensible Daten wie etwa Behinderungen anfallen, eine gesetzliche Grundlage fehlt (und eine solche wohl auch nicht mit einem „wichtigen öffentlichen Interesse“ zu rechtfertigen wäre), sind technische Maßnahmen zu

- Dementsprechend muss auch jede Identifizierbarkeit von gefilmten Personen im Internet ausgeschlossen sein (allenfalls ist eine manuelle Nachkontrolle/Nachbearbeitung notwendig).
- Anlässlich der Ermittlung (Filmen in bestimmten Stadtteilen dgl.) soll im Voraus eine Information der potentiell Betroffenen in geeigneter Form (jedenfalls durch breite mediale Berichterstattung unter Angabe der Ortsteile bzw. Straßenzüge, wo gefilmt werden soll) erfolgen; damit soll den Betroffenen die Möglichkeit gegeben werden, den Filmaufnahmen auszuweichen. Weiters muss klar sein, wo derartige Filmaufnahmen eingesehen werden können. Der Betroffene ist in geeigneter Form über das Bestehen eines Widerspruchsrechts zu informieren.
- Sollte ein Betroffener der Meinung sein, dass er erkennbar ist, soll er sein Widerspruchsrecht auf einfache Weise geltend machen können.
- Wenn der Auftraggeber nicht im Gebiet der Europäischen Union niedergelassen ist, muss er einen in Österreich ansässigen Vertreter benennen, der unbeschadet der Möglichkeit eines Vorgehens gegen den Auftraggeber selbst namens des Auftraggebers verantwortlich gemacht werden kann.
- Sensible Bereiche wie z.B. Kirchen, Gebetshäuser, Krankenhäuser sollten tunlichst schon im Vorfeld bei den Panoramaaufnahmen von Straßenzügen ausgenommen werden.

II. Geschäftsfelder von Google Inc.

Die Geschäftsstrategie von Google Inc. zeichnet sich seit der Gründung im Jahr 1998 durch zahlreiche Akquisitionen von Firmen mit zum Teil sehr unterschiedlichen und speziellen Geschäftsbereichen aus, die weit über den Zweck einer bloßen Suchmaschine hinausgehen. Die Produkte der übernommenen Firmen wurden in der Folge zumeist in bereits bestehende Google Anwendungen integriert oder für neue Google Anwendungen verwendet.
Insbesondere bietet Google – neben oder integriert in die hauseigenen Internet-Suchmaschine – folgende Dienste an:

Google Maps (Kartendienst)
Google Earth (virtueller Globus)
Google News (Nachrichtensuche)
Google Books (Suche nach bzw. in elektronisch erfassten Büchern)
Google Calendar (Webkalender)
Google Groups (Usenet-Suche)
Google Reader (Nachrichten und Blogs)
Google Sites (Erstellung von Webseiten)
Google Picasa (Fotobearbeitung und –datenbank)
Gmail (E-Mail-Services)
Google Analytics (Analysierung von Zugriffen auf Webseiten)
Google Translator (Übersetzer)
Google Wave (Internet-basiertes System zur Kommunikation und Zusammenarbeit in Echtzeit)
Google AdSense (semantische Bedeutung von Webseiten)
Google Desktop Search (Desktop-Suchprogramm)
Google Latitude (soziales Netzwerk mit der Möglichkeit der Standortbestimmung von Freunden; für die Standortbestimmung werden Wi-Fi-Netzwerke bzw. GPS genutzt)
Google Android (Betriebssystem, insb. für Mobiltelefone)
Google Docs (Internet-basierendes Office-Programm)
Google SketchUp (3d-Software für Google Earth)
YouTube (Internet-Videoportal)
Panoramio (Verbreitung geolokaler Digitalfotos, z.B. auch eingebunden in Google Earth und Google Maps)
Google Checkout (Bezahlsystem)
Google Visualization API (Visualisierungsschnittstelle zur Anwendungs-programmierung)
Google Voice (Telefondienstleistungen)
Google Health (elektronische Patientenakten; Google Health wird bislang nur in englischer Sprache und mit englischsprachigen Gesundheitsdienstleistern angeboten)
Google Chrome (Internet-Browser)

Google Fusion Tables (Online-Verwaltung von großen Datensammlungen in Form von Tabellen)
Interest Based Ads (interessenbasierte Anzeigen)
Google Squared (Suchergebnisse im Tabellenformat)
Google Chrome OS (Betriebssystem; noch in Entwicklung)

Darüber hinaus ist Google Inc. ua. im Besitz folgender Firmen/Unternehmungen bzw. Anteilen davon:

Postini (IT-Sicherheitsdienstleister)
Teracent (Bannerwerbung)
DoubleClick Inc. (Online-Werbenetzwerk)
AdMob (mobile Werbung)
Marratech (Videokonferenz)
Endoxon (Kartenunternehmen)
Neven Vision (Biometrische Gesichts- und Objekterkennung)
GeoEye-1 (von Google gesponserter Satelliten für hochauflösende Satellitenfotos für Google Earth und Google Maps)
ReCaptcha (Digitalisierung von Handschriften und Büchern)

Zudem produziert Google ein eigenes Mobiltelefon („Nexus One“) und plant demnächst auch E-Books zu verkaufen.

II. Ermittlung von Daten zu WLAN-Netzwerken

Unter einem WLAN (Wireless Local Area Network; auch WiFi) wird ein lokales Funknetz verstanden. Mit einem WLAN-Router können Geräte mit einer entsprechenden Netzwerkkarte (insb. mobile Geräte, wie Laptops oder Netbooks) innerhalb der Reichweite des WLAN-Routers am Netzwerk teilnehmen bzw. über den WLAN-Router und ein Modem ins Internet gelangen. In den letzten Jahren finden WLAN-Router aufgrund fallender Preise und einfacherer Einstellungsmöglichkeiten vermehrt vor allem auch im privaten Bereich Anwendung.
Grundsätzlich sendet ein WLAN-Router folgende Daten aus (wobei diese abhängig sind von der Konfiguration des Routers und durch den Betreiber allenfalls auch „versteckt“ werden können):

- MAC-Adresse des Gerätes (Media-Access-Control-Adresse)
- Verschlüsselungsstatus
- Liste unterstützter Übertragungsraten
- SSID (Service Set Identifier; Namen des Netzwerkes)

Darüber hinaus könnten – wenngleich der Router selbst keine Standortdaten aussendet – dem Router über das gemessene WLAN-Signal (mehr oder weniger exakt) GPS-Koordinaten zugeordnet werden.

Bei den Fahrten für die Aufnahmen von Straßenzügen durch Google (Google Street View) werden laut Medienberichten auch – zum Teil privat betriebene – WLAN-Funknetzwerke ermittelt. Neben Google werden laut Medienberichten auch vom Fraunhofer-Institut für Integrierte Schaltungen oder dem US-Unternehmen Skyhook WLAN-Daten gesammelt.

Die Ermittlung von WLAN-Netzen dient beim Fraunhofer-Institut der Entwicklung eines WLAN-basierten Ortungssystems. Das Fraunhofer-Institut gibt dazu an, dass für die Entwicklung eines WLAN-basierten Ortungssystems an Referenzpunkten Messwerte aufgenommen werden, welche alle empfangenen WLAN-Basisstationen und die dazugehörigen Empfangsinformationen enthalten. Die Empfangsinformationen beinhalten dabei lediglich die gemessenen Signalstärken der vorhandenen WLAN-Basisstationen an dem Referenzpunkt. Dieser Abdruck der Empfangsinformationen an Referenzpunkten wird vom Fraunhofer-Institut in einer Datenbank hinterlegt und auf dem mobilen Endgerät als Basis für die eigene Positionsbestimmung genutzt. Zur technischen Unterscheidung der gemessenen Signalstärken der WLAN-Stationen wird beim Fraunhofer-Institut die MAC-Adresse herangezogen. Auch gibt das Fraunhofer-Institut bekannt, dass ein Datenaustausch mit der WLAN-Station nicht durchgeführt wird und die Position der WLAN-Sender nicht ermittelt wird. Ebenso wenig wird die SSID oder der Verschlüsselungsstatus ermittelt oder gespeichert (dies wohl deswegen, weil sowohl der SSID-Name des WLAN-Routers als auch der Verschlüsselungsstatus leicht vom Nutzer über die Konfiguration des Routers verändert werden können und daher zur Identifikation eines Netzwerkes nur bedingt geeignet sind).

Auch Google und Skyhook nutzen Daten von WLAN-Routern zur Standortbestimmung. Skyhook hat die ermittelten Standorte von WLAN-Netzen –

unter anderem auch in Ballungsräumen in Österreich – im Internet in einer Landkarte bereits veröffentlicht, wobei jedoch anzumerken ist, dass hierbei nicht im Detail in die Karte hineingezoomt werden kann und somit nur eine grobe Verteilung der WLAN-Netze zu erkennen ist.

Google hat (im Gegensatz zum Fraunhofer-Institut) bislang noch nicht im Detail dazu Stellung genommen, welche der von WLAN-Routern ausgestrahlten Daten tatsächlich ermittelt bzw. verwendet werden. In der gemeinsame Presseerklärung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 22.4.2010 wird dazu ausgeführt, dass nach gegenwärtigen Erkenntnissen davon auszugehen ist, „dass neben der örtlichen Erfassung, dem Verschlüsselungsstatus der Geräte, der weltweit eindeutigen MAC-Adresse auch der vom Betreiber vergebene Name (sog. SSID) gespeichert wurde."

Aktuell gab Google laut Medienberichten zu, dass jahrelang im Rahmen des Street-View-Projekts auch „versehentlich" Nutzdaten aus offen zugänglichen WLAN-Funknetzen gespeichert wurden. Diese Daten enthalten auch Fragmente verschickter E-Mails oder abgerufener Web-Seiten.

III. Grundlegendes zur MAC-Adresse

Die MAC-Adresse (Media-Access-Control-Adresse) ist die Hardware-Adresse eines Netzwerkadapters (z.B. eines Routers oder einer Netzwerkkarte). Die MAC-Adresse wird dabei in hexadezimaler Kennung geschrieben (z.B. 00:07:e9:ab:fd:5a).

Grundsätzlich sollte jeder Netzwerkadapter eine weltweit einzigartige MAC-Adresse erhalten (sohin sollte es jede MAC-Adresse jeweils nur einmal weltweit geben), es gibt jedoch auch Ausnahmen von dieser Grundregel, insbesondere bei fehlerhafter Produktion von Netzwerkkarten. Zudem kann die MAC-Adresse ausgelesen bzw. in der Folge von entsprechend versierten Personen auf unterschiedliche Art und Weise verändert werden (MAC-Spoofing), um etwa Zugang zu einem auf bestimmte MAC-Adressen beschränkten Netzwerk zu bekommen.

IV. Personenbezug von MAC-Adressen

Personenbezogen sind nach § 4 Z 1 DSG 2000 Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen" sind Daten

für einen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.
Vorweg ist zu bemerken, dass kein allgemeines Verzeichnis aller MAC-Adressen mit einer Zuordnung zu bestimmten oder bestimmbaren Personen bekannt ist. Allenfalls kann aufgrund der Vergabe von MAC-Adressen-Bereichen festgestellt werden, welches Unternehmen einen Netzwerkadapter erzeugt hat (z.B. 00-07-E9-xx-xx-xx für Intel oder 00-60-2F-xx-xx-xx für Cisco).
In folgenden Fällen kann eine Zuordnung von MAC-Adressen zu bestimmten oder bestimmbaren Personen jedoch nicht ausgeschlossen werden:

a) MAC Adress Filtering

MAC-Adressen können – je nach Konfiguration – innerhalb eines Netzwerkes auch einer bestimmten Person zugeordnet werden, dies vor allem um den Zugang zu Netzwerken mit einem MAC-Filter (ähnlich einem „Adressbuch“) auf bestimmte Personen bzw. auf in deren Besitz stehende Netzwerkgeräte zu beschränken. In größerem Rahmen können auch Private von einem MAC-Filter betroffen sein, etwa dann, wenn ein (Internet)-Provider zur Vermeidung von missbräuchlicher Verwendung seines Netzwerkes den Zugang zum Netzwerk nur konkreten Kunden und diesen Kunden zugewiesenen Netzwerkgeräten (z.B. Netzwerkkarten oder „Modems“) erlauben will. Wenngleich damit MAC-Adressen konkreten Personen zugeordnet werden können, sind davon in erster Linie die MAC-Adressen von Modems oder Netzwerkkarten von Mitarbeitern oder Kunden, nicht jedoch WLAN-Router betroffen. Denkbar wäre jedoch, dass bei (A)DSL-Routern (eine Kombination aus (A)DSL-Modem und (WLAN-)Router in einem Gerät) die MAC-Adresse des Gerätes (jeweils eine MAC-Adresse für das Modem und den Router) dem Provider bekannt ist (da z.B. ein Gerät des Providers verwendet werden muss) und damit auch der Besitzer des (A)DSL-Routers samt WLAN-Netzwerk dem Provider namentlich bekannt ist.

b) WLAN-Netzwerke im ländlichen Raum

In bestimmten Fällen – so etwa im ländlichen Raum, wenn aufgrund der geringen Bebauungsdichte und der geringen Dichte an WLAN-Netzwerken der Standort eines

WLAN-Routers einem einzelnen Einfamilienhaus zugeordnet werden kann – kann damit unter Umständen auch die MAC-Adresse dem Eigentümer des Hauses (der allenfalls über das Telefonbuch oder Grundbuch bestimmbar ist) zugeordnet werden und stellt dann – wie auch die Postadresse – ein personenbezogenes Datum dar.

c) SSID mit Vor- und Familiennamen

Personenbezogen ist die MAC-Adresse auch dann, wenn sie gemeinsam mit der SSID verarbeitet wird und das Netzwerk über den (frei wählbaren) SSID-Namen einem konkreten Betreiber zugeordnet werden kann. Dies ist vor allem dann der Fall, wenn der Betreiber seinen Vor- und Familiennamen als SSID des Netzwerkes eingibt.

Auch wenn das Netzwerk (bzw. die SSID) vom Betreiber nach seinem Namen benannt wird, kann in der Regel nicht davon ausgegangen werden, dass es sich dabei um „veröffentlichte“ Daten handelt, da die vom WLAN-Router ausgesendete Daten technisch nur in einem geografisch sehr beschränkten Umkreis (je nach Modell und verwendetem Standard unterschiedlich, so etwa bei aktuellen Heimgeräten mit dem IEEE-Standard 802.11n im Freien bis etwa 250 Metern) empfangen werden können, kann nicht ohne weiters von einer „allgemeinen Verfügbarkeit“ dieser Daten ausgegangen werden. Darüber hinaus dienen die vom WLAN-Router ausgesendeten Daten primär dazu, dass sich vom Betreiber „zugelassene“ Netzwerkgeräte mit dem Router verbinden, nicht jedoch zur Verwendung in einer Datenbank zum Zweck der Standortbestimmung.

d) Kundendatenbanken und Registrierungen

Die MAC-Adresse kann auch dann einen Personenbezug herstellen, wenn sie von Herstellern mit Kundendaten verknüpft gespeichert wird. Wenngleich dies beim Verkauf von Hardware wohl nicht der Fall sein wird, kann eine Verknüpfung von MAC-Adressen und Kundendaten insbesondere in bestimmten Wartungsfällen (z.B. Garantiearbeiten an Netzwerkgeräten) nicht vorweg ausgeschlossen werden. Ebenfalls nicht ausgeschlossen werden kann, dass die MAC-Adresse (allenfalls auch verknüpft mit der IP-Adresse) im Zuge der Aktivierung von kopiergeschützter Software übers Internet als Teil des „Fingerprints“ des PCs mitübertragen bzw. ausgelesen wird. Soweit im Zuge dessen auch eine Registrierung des Nutzers mit

dem Namen bzw. der E-Mail-Adresse (z.B. im Hinblick auf die Mitteilung von Updates oder Patches zur Software) beim Softwarehersteller stattfindet, könnte auch in diesem Bereich eine Zuordnung der MAC-Adresse zu bestimmten oder bestimmbaren Personen stattfinden.

e) Erhebung von „Nutzdaten“

Nach aktuellen Medienberichten hat Google im Rahmen der Erfassung von offenen WLAN-Funknetzwerken auch sogenannte Nutzdaten („payload data“) gespeichert. Dabei handelt es sich auch um Fragmente von E-Mails oder Inhalte von abgerufenen Webseiten.

Abhängig von den jeweils erhobenen Nutzdaten könnte damit unter Umständen auch die Identität des Betreibers des WLAN-Netzes oder darüber hinaus auch die Identität von Familienangehörigen bzw. Empfängern von E-Mails bestimmt werden. Auch könnten diese Nutzdaten (bspw. bei E-Mails mit gesundheitsbezogenen Inhalten oder aufgerufenen Webseiten mit religiösen oder politischen Inhalten) auch sensible Daten enthalten.

Soweit diese durch Google erfassten Nutzdaten auch personenbezogene Daten enthalten, ist einer derartige Erhebung aus datenschutzrechtlicher Sicht in jedem Fall als unzulässig anzusehen.

V. Aktueller Gesetzesantrag der Freien und Hansestadt Hamburg

Ein Gesetzesantrag der Freien und Hansestadt Hamburg (Nr. 259/10) vom 28. April 2010 an den deutschen Bundesrat sieht vor, dass die systematische und georeferenzierte Übermittlung digital gespeicherter fotografischer oder filmischer Straßenansichten, insbesondere ihre Bereitstellung im Internet, nur zulässig ist, wenn die verantwortliche Stelle wiedergegebene Gesichter und Fahrzeugkennzeichen vor der Übermittlung unkenntlich macht. Nach Veränderung der Datensätze ist die verantwortliche Stelle verpflichtet, die unveränderten Rohdatensätze innerhalb eines Monats nach ihrer Übermittlung, insbesondere ihrer Bereitstellung im Internet, zu löschen. Ein Widerspruchsrecht soll zudem Hauseigentümern und Mietern ermöglichen, der Abbildung des Gebäudes im Internet uneingeschränkt zu widersprechen. Gleichermaßen können aufgenommene Personen eine vollständige Unkenntlichmachung ihres Abbildes verlangen. Der verantwortlichen Stelle wird in

dem neu aufgenommenen § 33a BDSG die Pflicht zur öffentlichen Mitteilung des Vorhabens und der Benachrichtigung der zuständigen Aufsichtsbehörde auferlegt. Ein Verstoß gegen die genannten Verpflichtungen soll nach § 43 BDSG bestraft werden.

Der Gesetzesantrag der Freien und Hansestadt Hamburg verfolgt damit grundsätzlich das Ziel (ebenso wie der Datenschutzrat bereits in seiner Stellungnahme vom 15. Juli 2009 gefordert hat), dass eine Rechtsgrundlage für die Veröffentlichung von Geodaten und Aufnahmen von Straßenzügen im Internet geschaffen wird.

Im Detail unterscheidet sich der vorliegende Gesetzesantrag jedoch von der Stellungnahme des Datenschutzrates insofern, als der Datenschutzrat gefordert hat, dass sichergestellt wird, dass die **Daten nicht ins Ausland übermittelt werden, solange diese nicht anonymisiert worden sind**. Auch sollten **sensible Bereiche** wie z.B. Kirchen, Gebetshäuser, Krankenhäuser tunlichst schon im Vorfeld bei den Panoramaaufnahmen von Straßenzügen ausgenommen werden.

VI. Schlussfolgerungen

Der **Datenschutzrat wiederholt** seine bereits in der Stellungnahme vom 15. Juli 2009 **zur Veröffentlichung von Geodaten und Aufnahmen von Straßenzügen im Internet aufgestellte Empfehlung**, dass für die Aufnahme und Veröffentlichung von Fotografien von Straßenzügen durch verschiedene Diensteanbieter eine **(europäische) Rechtsgrundlage geschaffen werden sollte**, um klarzustellen, wie Anbieter vorzugehen haben, und weiters die Bevölkerung vor ausufernden Aktivitäten der Anbieter zu schützen. Grundsätzlich sollte auch sichergestellt werden, dass die **Daten nicht ins Ausland übermittelt werden**, solange diese nicht anonymisiert worden sind. Die **Veröffentlichung von Aufnahmen** soll **ausschließlich ohne Personenbezug** erfolgen.

Darüber hinaus **betont der Datenschutzrat** aufgrund der bekannt gewordenen Entwicklungen, dass das **Erfassen und in weiterer Folge das Verwenden von personenbezogenen Daten von WLAN-Netzen bzw. darin verwendeten Nutzdaten** aus datenschutzrechtlicher Sicht **unzulässig ist** und **im Rahmen einer noch zu schaffenden Rechtsgrundlage ausdrücklich untersagt werden sollte**.

Nach Angaben der **Datenschutzkommission** wurde die Datenschutzkommission erst im Zuge der aktuellen Entwicklungen von Google informiert, dass Google Daten zu WLAN-Netzen bzw. Nutzdaten aus WLAN-Netzen erfasst hat. Die Datenschutzkommission hat Google aufgetragen, dass **rechtsgrundlos ermittelte personenbezogenen Daten umgehend zu löschen** sind und die Datenschutzkommission **vom Vollzug der Löschung zu benachrichtigen ist**.

Der Datenschutzrat weist darauf hin, dass er sich in seiner nächsten Sitzung neuerlich mit Fragen zur Registrierung von Google in Österreich, zur Durchsetzung von Sanktionen in Drittstaaten und insbesondere mit der datenschutzrechtlichen Relevanz der bestehenden strafrechtlichen Bestimmungen im DSG 2000 und StGB befassen wird.

27. Mai 2010
Für den Datenschutzrat:
Der Vorsitzende:
MAIER

Elektronisch gefertigt