Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Postfach 1468, 53004 Bonn

Deutsche Telekom AG
Group Privacy
Herrn
53262 Bonn

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-813
TELEFAX (0228) 997799-550
E-MAIL ref8@bfdi.bund.de
BEARBEITET VON Ekkehard Valta
INTERNET www.datenschutz.bund.de

DATUM Bonn, 29.01.2015
GESCHÄFTSZ. **VIII-193-1/002#2133**

**Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anonymisierungsverfahren bei Motionlogic**
BEZUG Ihr Schreiben vom 09.05.2014

Sehr geehrter Herr

vielen Dank für Ihr Schreiben. Die Beantwortung hat sich leider verzögert, da im Rahmen des Projektes grundsätzliche datenschutzrechtliche Fragestellungen intensiv geprüft werden mussten.

Bei dem von Ihnen beschriebenen Verfahren werden Daten gespeichert, die nach Ablauf des Tages als anonymisiert eingestuft werden können, jedoch mit weiterem Vorwissen in manchen Fällen wieder einer bestimmbaren natürlichen Person zugeordnet werden könnten. Daher kann nur dann von einer ausreichenden Anonymisierung, die den Voraussetzungen des § 3 Abs. 6 BDSG entspricht, ausgegangen werden, wenn sichergestellt ist, dass die faktisch anonymisierten Daten nicht mit anderen Datenbeständen zusammengeführt werden, die eine Re-Identifizierung von Betroffenen mit einem verhältnissmäßigen Aufwand an Zeit, Kosten und Arbeitskraft ermöglichen. Dies ist nach meinem Verständnis des von Ihnen vorgelegten Konzepts gegeben, da nicht einzelne Datensätze, sondern nur aggregierte Daten an Dritte übermittelt werden sollen. Da dies für meine Bewertung Ihres Anonymisierungsverfahrens eine zentrale Bedeutung hat, muss auch zukünftig eine solche Zusammenführung bei Änderungen des Konzepts ausgeschlossen werden. Aus diesem Grund



ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

müssen Sie vor allem die Aggregations- und Filterverfahren und -einstellungen fortlaufend unter Berücksichtigung des Stands der Technik überprüfen, um sicherzustellen, dass insbesondere im Kontext des jeweiligen Nutzungszwecks ein Rückschluss auf einzelne Personen für die Empfänger der aggregierten Daten – etwa durch eine Kombination verschiedener Abfragen und der Nutzung von Hintergrundwissen – praktisch nicht durchführbar ist. Weiterhin gehe ich davon aus, dass sich meine Kontrollbefugnis auch auf die Einhaltung dieser Voraussetzungen erstreckt. Insofern bitte ich darum, mich über entsprechende Änderungen des Verfahrens zu unterrichten.

Ich bitte ferner noch zu prüfen, inwieweit die „Bewegungsspuren" über 24 Stunden voneinander unabhängig sind. Es sollte vermieden werden, dass – etwa durch das nach einer exakten Zeitspanne (etwa genau 6 Stunden) erfolgende Periodic Location Update in derselben Funkzelle – die Daten verschiedener Tage mit hoher statistischer Sicherheit in Zusammenhang gebracht werden können. Über das Ergebnis bitte ich mich zu unterrichten.

Im Rahmen unserer Besprechung am 15.12.2014 hatten Sie angekündigt, dass Ihre Kunden über das Verfahren informiert werden und die Möglichkeit erhalten sollen, der Verarbeitung ihrer Standortdaten zu widersprechen. Dies begrüße ich ausdrücklich und bitte sicherzustellen, dass diese Möglichkeit unmittelbar zu Beginn des Verfahrens besteht; für eine entsprechende Unterrichtung wäre ich dankbar.

Falls die noch offenen Fragen positiv geklärt werden, habe ich keine Einwände gegen die Einführung dieses Verfahrens. Bitte informieren Sie mich, sobald das Verfahren im Regelbetrieb aktiv ist, damit ich im Rahmen einer Kontrolle das Verfahren prüfen kann.

Mit freundlichen Grüßen
Im Auftrag

Müller

Anlg

**VIII-193-1/012#1696**

Bonn, den 02.07.2014

Bearbeiter: RD Valta

Hausruf: 813

Betr.: Nutzung von pseudonymisierten/anonymisierten Standortdaten durch Mobilfunkanbieter für Big-Data-Anwendungen

hier: Anfragen von und der Telekom

Bezug: E-Mail von vom 5.6.14
Schreiben der DTAG vom 9.5.14, Az.: VIII-193-1/2#2133
Vermerk vom 28.11.2013, Az.: I-100/28#47
Vermerk vom 7.10.13
Vermerk vom 9.7.13
Vermerk vom 4.7.13

Anlg.: Auszug aus dem 22. TB
Sammlung von Pressemeldungen von 2012 (Spiegel, Zeit)

1) Vermerk

Standortdaten von Mobilfunkteilnehmern können über die Bewegung von Menschen Auskunft geben. Diese Informationen können in anonymisierter Form auch wirtschaftlich im Rahmen von Big-Data- Anwendungen (z.B. für Stauprognosen, zur infrastrukturellen Planung, Reichweitenmessung über Kundenströme im Einzelhandel, etc.) genutzt werden. Bei den TK-Unternehmen ist ein Trend, entsprechende Angebote zu entwickeln klar erkennbar.

Aus deren Sicht ist allerdings problematisch, dass eine „echte" Anonymisierung dazu führen kann, dass die erwünschten Erkenntnisse nicht mehr die gewünschte und eventuell sogar erforderliche Aussagekraft haben. Informationen über Bewegungen können nur durch die Kombination mehrerer Ereignisse (Kontakte des Handys mit dem Netz) eines Teilnehmers gewonnen werden. So müssen einerseits für eine „gute" Anonymisierung Verfahren genutzt werden, die die Personenbeziehbarkeit eines Bewegungsprofils nur über eine sehr kurze Zeitspanne ermöglicht, was andererseits aber dazu führen kann, dass nicht alle relevanten Bewegungsströme erfasst werden können, oder die Aussagekraft der erfassten Bewegungsströme für den gewünschten Zweck unzureichend ist.

Ein vom BfDI akzeptiertes Verfahren war die Gewinnung von Informationen zum Straßenverkehr aus Mobilfunkverkehrsdaten durch für (und später anderen Anbietern). Dies wurde im 22. TB erläutert, siehe Anlage. Hier wurde aus einem personenbezogenen Datum (z. B. IMEI) ein Pseudonym gebildet, wobei die Regel für die Bildung des Pseudonyms innerhalb einer kurzen Zeit (z. B. 90 Minuten) geändert wurde. Dadurch wird verhindert, dass ein einzelner Teilnehmer anhand typischer Bewegungsmuster wiedererkannt werden kann. Der Zeitraum ist allerdings ausreichend, um die Geschwindigkeit und Bewegungsrichtung eines Teilnehmers zu bestimmen. Anhand einer großen Zahl von Teilnehmern kann etwa erkannt werden, ob auf einer Autobahn Stau herrscht.

Für die Anwendungen, die Telekom und anbieten wollen, sind allerdings aussagekräftigere Daten erforderlich, die eine Zuordnung über einen längeren Zeitraum erforderlich machen. Hierzu sind zwei Maßnahmen geplant:

- Die Änderung der Pseudonymisierungsregel soll alle 24 Stunden erfolgen.
- Jedem Pseudonym sollen weitere Angaben (Alter, Geschlecht, Wohnort, ggf. Arbeitsort) hinzugefügt werden.

. Auch die Telekom hat um die Beurteilung eines ähnlichen Verfahrens gebeten.

Sofern die Verfahren so wie beschrieben durchgeführt werden, sind **hinsichtlich der Ergebnisse der Verarbeitungsprozesse** keine datenschutzrechtlichen Bedenken angebracht. Sofern man die Generierung der Daten und die gespeicherten Daten betrachtet, können jedoch Bedenken aufkommen:

- Bei beiden Verfahren werden Bewegungsprofile eines anonymen bzw. pseudonymen Nutzers für 24 Stunden gespeichert. Wenn bestimmte Informationen bekannt sind und es sich um außergewöhnliche Kombinationen handelt[1], könnte auf eine Person geschlossen werden. Die anonymen bzw. pseudonymen Daten sollen langfristig gespeichert werden. Die Genauigkeit der Standortangaben hängt von der Größe der Funkzellen ab. In belebten Innenstadtlagen versorgen Funkzellen nur wenige hundert Meter, in ländlichen Bereichen können Funkzellen auch über 10 km groß sein.

[1] Beispiel: Bekannt ist nachts Wohnung in Bonn, morgens Dienststelle in Bonn, mittags Einschalten des Handys in Tegel, nachmittags Verbindungbüro Berlin. Erkennbar würde, wo der Handynutzer den Abend verbringt.

- Bei dem Verfahren der Telekom werden Altersklasse, Geschlecht und ggf. Postleitzahl der Adresse mitgespeichert, so dass eine Identifizierung des Nutzers erleichtert werden kann. Ebenso wird eine Zusammenführung der Daten mehrerer Tage erleichtert. Bei streng formaler Betrachtung ist zweifelhaft, ob für eine pseudonyme Nutzung der Bestandsdaten zur Generierung der Zusatzinformationen eine Ermächtigungsgrundlage vorliegt.
-

- Die Beantwortung der Frage, ob es sich bei den vorliegenden Verfahren – solange eine Zuordnung noch möglich ist, also 24 Stunden bei der Telekom - bereits um eine Anonymisierung oder noch um eine Pseudonymisierung handelt, hängt im Wesentlichen davon ab, welche Anforderungen an das Unverhältnismäßigkeitsmerkmal des § 3 Abs. 6 BDSG gestellt werden.

Die Beschreibungen der Verfahren können , und dem Schreiben der Telekom entnommen werden.

Es sollte noch darauf hingewiesen werden, dass eine – eigentlich für Aktionäre gedachte Meldung – 2012 ein erhebliches Presseecho hervorgerufen und daraufhin veranlasst hatte, die Pläne nicht weiter zu verfolgen. Insofern ist auch künftig mit einem Medienecho zu rechnen.

**VIII-193-1/002#2133**

Bonn, den 09.12.2014
Bearbeiter: RD Valta

Hausruf: 813

Betr.: Vorbereitung auf die Besprechung mit der Telekom am 15.12.2014

Vermerk

Vorbemerkung: In dem Schreiben der Telekom vom 03.12.2014 geht etwas unter, dass das im Februar 2014 hier in der Dienststelle präsentierte Verfahren und das im Mai schriftlich vorgestellte Verfahren einen aus Datenschutzüberlegungen entscheidenden Unterschied aufweisen. Der Wechsel der Kennung sollte ursprünglich alle 90 Minuten stattfinden, analog zu dem Verfahren zur Stauerkennung für Navigationsgeräte. Damit sind Bewegungsprofile kaum herstellbar. Erst in dem Mitte Mai eingegangenen Schreiben wird darüber informiert, dass die Kennungen (durch ) nur alle 24 Stunden geändert werden soll. Dies erfordert eine erneute datenschutzrechtliche Bewertung.

Bei der Besprechung mit der Telekom ist davon auszugehen, dass die – ggf. aktualisierte – Beschreibung aus dem Schreiben vom 09.05.2014 vorgestellt wird. Hier gibt es m. E. einen zentralen Punkt, der datenschutzrechtlich und vor allem datenschutzpolitisch zu bewerten ist:

Die Standortdaten werden mit einer Kennung, die täglich geändert wird, gespeichert. Dies führt zu Bewegungsprofilen für jeweils einen Tag, die in manchen Fällen mit Zusatzwissen einer Person zugeordnet werden könnten. Insofern ist die folgende Aggregierung ein erforderlicher Teil der Anonymisierung. Die Datenbank mit den Standortdaten soll Dritten nicht direkt zugänglich gemacht werden.

werden hier die zusätzlichen Attribute (Altersklasse, Geschlecht, PLZ Wohnort) zusammen mit den Standortdaten gespeichert, so dass die Identifikation aufgrund des Bewegungsprofils noch erleichtert wird. Die PLZ des Wohnorts wird aus den Bestandsdaten gebildet und bei auffälligen Profilen gekürzt.
Kritik könnte erfolgen, da diese Bewegungsprofile für einen langen Zeitraum gespeichert werden sollen. Diese Daten sollen zwar nur für die Aggegierung genutzt werden, sind aber vorhanden.

Die gemeinsame Speicherung der Standortdaten mit den Attributen erleichtert zwar die Profilbildung, .. Somit ist auch theoretisch keine eindeutige Reidentifizierung anhand von gespeicherten Schlüsseln möglich.

VIII-193-1/012#1696

Bonn, den 03.09.2014
Bearbeiter: RD Valta

Hausruf: 813

Betr.: Nutzung von pseudonymisierten/anonymisierten Standortdaten durch Mobilfunkanbieter für Big-Data-Anwendungen

hier: Anfragen von der Telekom

Bezug: Vermerk vom 02.07.2014

Vermerk

Bei der Mitzeichnung des Vermerks vom 02.07.2014[1] wurde Ref. VIII um eine Beurteilung bzw. Einschätzung zum Verfahren – wie von der Telekom im Schreiben vom 09.05.14 – gebeten.

Bei dem Ansatz der Telekom wird nicht berücksichtigt, dass es keine „ein bisschen personenbezogene" Daten gibt – so wie man auch nicht ein bisschen schwanger sein kann. Es sollen Bewegungsprofile für einen Tag, angereichert mit weiteren Daten wie z. B. Altersklasse, Geschlecht und Wohnort gespeichert werden. Diese können mit Vorwissen für einen Teil der Nutzer einer bestimmten Person zugeordnet werden. Praktisch soll dies durch organisatorische Maßnahmen verhindert werden. Die grundsätzliche Fragestellung ist jedoch, ob man die Daten als faktisch anonymisiert ansieht.

Sofern man in beiden Fällen eine faktische Anonymisierung bejaht, wäre lediglich noch eine Prüfung von Details erforderlich, die auf Fachebene zusammen mit den

[1] Der Vermerk vom 02.07.2014 einschließlich im Bezug genannten Vermerke und Schreiben im Original ist derzeit nicht auffindbar, ein erneuter Ausdruck wurde erstellt.

Unternehmen möglich ist. Grundsätzlich wären die Verfahren unter dieser Voraussetzung nicht zu beanstanden.