universität wien

MASTER-THESIS

MOBIL GEORTET – DATEN GEHORTET

Verwendung ortsbezogener Daten von Mobilfunkgeräten in Big Data Anwendungen

Verfasserin

Mag. Roswitha Lelleck-Zanetti

angestrebter akademischer Grad

Master of Laws (LL.M.)

Wien, Jänner 2015

Universitätslehrgang:	Informations- und Medienrecht
Studienkennzahl lt. Studienblatt:	A 992 942
Betreuer:	ao. Univ. Prof. Dr. Dietmar Jahnel

INHALTSVERZEICHNIS

I. EINLEITUNG

Die öffentlichen Verkehrsbetriebe in Zaragoza[1] starten gemeinsam mit dem spanischen Telekommunikationsunternehmen Telefónica ein Projekt zur besseren Planung des öffentlichen Verkehrsnetzes im Raum Zaragoza anhand der Mobilfunkdaten der Kunden von Telefónica. Im Rahmen der Nutzung von Mobiltelefonen werden laufend Ortsdaten generiert, die Telefónica anonymisiert und zu einem Bewegungsstrom aggregiert den Verkehrsbetrieben übermittelt. Mit Telefónicas Produkt „Smart Steps" können die Verkehrsbetriebe die Einsetzung der Verkehrsmittel bestmöglich planen[2]. In der Nutzung ortsbezogener Mobilfunkdaten sehen jedoch viele neben den großen wirtschaftlichen und innovativen Möglichkeiten auch eine große Gefahr für den Datenschutz.

So gut wie jeder Mensch trägt heute stets ein Mobiltelefon bei sich, durch welches – schon alleine um die Erreichbarkeit zu gewährleisten - ständig ortsbezogene Daten erfasst werden. Mittlerweile sind die Kosten für Speicherplatz derart gering, dass erfasste Daten häufig „für alle Fälle" gespeichert werden[3]. Aus den anfallenden Daten können nach entsprechender Auswertung und Analyse wichtige Einsichten gewonnen werden. Da es sich um riesige Datenmengen handelt, lassen sich daraus Wahrscheinlichkeiten mit hoher statistischer Qualität berechnen und aus diesen Wahrscheinlichkeiten Vorhersagen treffen. Das Treffen von Vorhersagen aus großen Datenmengen fällt unter den Begriff „Big Data"[4].

Die Grundsätze jeder Datenverwendung werden in § 6 Abs 1 DSG[5] festgehalten, wonach Daten nur nach Treu und Glauben und beschränkt auf das für den festgelegten Zweck Notwendige und Richtige verwendet werden dürfen[6].

Werden bereits gesammelte Daten zu einem anderen als den ursprünglich festgelegten Zweck verwendet oder ist die Datenverwendung mit dem ursprünglich festgelegten Zweck

---

[1] Consorcio de Transportes del área de Zaragoza.
[2] "Una aplicación tecnológica analizará el tráfico metropolitan", El Periódico, 29/9/2014 <www.elperiodicodearagon.com/m/noticias/aragon/aplicacion-tecnologica-analizara-trafico-metropolitano_973535.html>.
[3] *Feiler/Fina*, Datenschutzrechtliche Schranken für Big Data, MR 2013, 303.
[4] *Mayer-Schönberger/Cukier*, Big Data. Die Revolution, die unser Leben verändern wird (2013) 12ff.
[5] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), BGBl. I 165/1999 idF I 83/2013.
[6] *Graf*, Datenschutzrecht im Überblick² (2010) 14f.

nicht vereinbar, wird gegen den datenschutzrechtlichen Grundsatz der Zweckbindung verstoßen[7]. Bei Big Data Anwendungen werden verschiedene Daten und Informationen zusammengeführt, um daraus Erkenntnisse zu erzielen. Jede Zusammenführung ist eine Datenverwendung, die an geltende datenschutzrechtliche Grenzen stoßen kann. Nachfolgend soll mit „Smart Steps" ein konkretes Beispiel einer Big Data Anwendung im Mobilfunkbereich näher dargestellt werden.

A. SMART STEPS

Der Telekommunikationskonzern Telefónica gründete die Gesellschaft Telefónica Dynamics Insights, die aus der Verwertung riesiger Datenmengen neue Produkte entwickeln sollte. Durch Big Data Anwendungen sollen neue Einnahmequellen geschaffen werden basierend auf den (nachfolgend anonymisierten) Daten der Mobilfunkkunden von Telefónica, welche notwendigerweise mit der Erbringung der Telekommunikationsdienstleistung anfallen.

Bei der Entwicklung neuer Angebote arbeitet Telefónica mit dem deutschen Marktforschungsinstitut GfK zusammen. Das erste gemeinsame Produkt „Smart Steps"[8] gibt die Bewegungsdaten der Mobilfunkkunden in anonymisierter und aggregierter Form wieder. Smart Steps macht sichtbar, wo sich Menschenmengen aufhalten bzw. wohin sie sich bewegen, und kann damit z.B. darstellen, ob sich am Samstagabend mehr Personen in der Einkaufspassage aufhalten oder im Fußballstadion. Anhand der Bewegungsströme der Mobilfunkkunden können Unternehmen strategische Entscheidungen treffen, wie beispielsweise, wo eine neue Verkaufsstelle eröffnet werden soll oder wann und wo sich „Late night shopping" auszahlt, wie viel Personal in welcher Filiale einzusetzen ist usw. Mithilfe dieser analytischen Einsichten könnten Unternehmen effektiver werden. Die Tatsache, dass Telefónica aktuell der größte Mobilfunkanbieter in Deutschland ist, lässt erahnen, welch hohe Aussagekraft eine Analyse der Bewegungsströme ihrer Kunden aufweisen könnte. Aus dem Bewegungsstrom lässt sich der Aufenthaltsort einzelner Personen nicht erkennen, da die ortsbezogenen Daten, die für Smart Steps verwendet werden, anonymisiert und aggregiert sind. Werden allerdings die Bewegungsströme mit anderen

[7] *Feiler/Fina*, Datenschutzrechtliche Schranken für Big Data, MR 2013, 303.
[8] <dynamicinsights.telefonica.com/488/smart-steps>.

Datensätzen angereichert, kann mit guter Genauigkeit der Aufenthalt gewisser Personengruppen (zum Beispiel ausgewählt nach Alter und Geschlecht) gezeigt werden[9]. Datensätze, die mit anderen Datensätzen kombiniert werden, erhöhen die Attraktivität für Unternehmen deutlich, da sie genauer auf die jeweilige Zielgruppe abgestimmt sind.

Die Daten, die Smart Steps für die Erstellung der Bewegungsströme verwendet, fallen im Zusammenhang mit der Erbringung des Kommunikationsdienstes an und werden somit nicht zusätzlich erhoben. Eine ausdrückliche Zustimmung des einzelnen Mobilfunkkunden für die Verwendung seiner Daten im Zusammenhang mit Smart Steps wird nicht eingeholt.

Erstmalig wurde Smart Steps in Großbritannien angeboten. Die britische Datenschutzbehörde, Information Commissioner's Office (ICO), hielt fest, dass die datenschutzrechtlichen Bestimmungen in Zusammenhang mit anonymisierten Daten keine Anwendung finden, solange sichergestellt ist, dass diese Daten den einzelnen Personen nicht zugeordnet werden können. Kann der Personenbezug nicht hergestellt werden, bedarf das Verarbeiten anonymisierter Standortdaten auch keiner Zustimmung des Einzelnen[10].

Als der internationale Telekommunikationskonzern ankündigte, diese Big Data Auswertung auch in Deutschland anzubieten, sprach sich das für Telekommunikation zuständige Wirtschaftsministerium klar gegen einen Handel mit Standortdaten deutscher Mobilfunkkunden aus, auch wenn es sich dabei um anonymisierte Daten handelt[11]. Die heftige Kritik, dass eine solche Anwendung einen Eingriff in das Grundrecht auf Datenschutz darstelle, veranlasste Telefónica, von der Analyse der Bewegungsdaten ihrer Kunden in Deutschland abzusehen[12]. Grundsätzlich muss aber angemerkt werden, dass – wie beim eingangs vorgestellten Beispiel - ortsbezogene, anonymisierte Daten in vielen Ländern Europas sehr wohl benutzt werden. Mehrere Telekommunikationsanbieter verkaufen die von

---

[9] <dynamicinsights.telefonica.com/1158/a-smart-step-ahead-for-morrisons>; <www.bbc.com/news/technology-19882647>; <www.spiegel.de/netzwelt/gadgets/telefonica-keine-auswertung-von-bewegungsdaten-in-deutschland-a-864772.html>; <www.out-law.com/articles/2012/october/telefonica-to-sell-insights-gleaned-from-anonymised-mobile-phone-location-data>.

[10] *Information Commissioner's Office*, Big data and data protection, <ico.org.uk/news/latest_news/-2014/~/media/documents/library/Data_Protection/Practical_application/big-data-and-data-protection.pdf>.

[11] www.handelsblatt.com/unternehmen/it-medien/ortungsprogramm-bundesregierung-verbietet-o2-handel-mit-bewegungsdaten/7328904.html.

[12] *Mantz*, Standortdaten und Bewegungsprofile, K&R, 1/2013, 7.

ihnen erfassten Daten in anonymisierter Form an Unternehmen - zum Beispiel zur Erstellung von Stauprognosen und/oder Wegzeitplanung. Fraglich ist nun, ob diese Art der Datenverwendung in Österreich datenschutzrechtlich erlaubt ist.

B. DATENSCHUTZ UND BIG DATA

Nach dem Grundrecht auf Datenschutz in § 1 Abs 1 DSG hat jedermann das Recht auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Geheimhaltungsinteresse daran besteht. Das Grundrecht schützt den Betroffenen vor Ermittlung und Weitergabe seiner Daten. Eine Datenanwendung[13], also die Summe logisch verbundener Verwendungsschritte zur Erreichung eines inhaltlich bestimmten Ereignisses, ist grundsätzlich nicht erlaubt. Auch einfachgesetzlich ergibt sich aus § 7 Abs 1 DSG, dass grundsätzlich Daten nicht verarbeitet werden dürfen. Eine Ausnahme besteht demnach nur, soweit *Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen*[14]. Voraussetzung für die Zulässigkeit einer Datenverwendung ist gemäß § 7 Abs 3 DSG weiters, dass der Eingriff in das Grundrecht nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgt und dass die in § 6 festgehaltenen Grundsätze des Datenschutzrechts eingehalten werden[15]. Bei der Prüfung der Zulässigkeit einer Datenanwendung sind die in § 6 DSG enthaltenen wesentlichen Grundsätze zu beachten. Diese geben die schon in der Datenschutzkonvention des Europarates in Art 5 („Qualität der Daten“) festgeschriebenen Qualitätsgrundsätze der Fairness und Rechtmäßigkeit, der strikten Zweckbindung, der Begrenzung des Datenumfangs auf das Wesentliche, der Richtigkeit und Aktualität und der zeitlichen Begrenzung, also dem Grundsatz der Datenlöschung, sobald diese für den Verarbeitungszweck nicht mehr benötigt werden, wieder[16].

---

[13] Unter Datenanwendung versteht man gem § 4 Z 7 DSG: "die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung)“.

[14] § 7 (1) DSG.

[15] *Jahnel,* Datenschutzrecht, in Jahnel /Mader/Staudegger (Hrsg), IT-Recht³ (2012) 432f.

[16] *Pollirer/Weiss/Knyrim*, DSG² § 6 Anm 3 (2014).

Big Data steht für große Datenmengen und gleichzeitig für Methoden, diese großen Datenmengen auszuwerten. Mithilfe von Algorithmen werden riesige Datenmengen analysiert, mit dem Ziel, Einsichten daraus zu gewinnen. Big Data Anwendungen basieren im Allgemeinen auf der Verknüpfung bereits bestehender Datensätze. Oft ist die Verknüpfung bereits vorhandener Daten mit anderen Daten mit dem ursprünglichen Zweck der Datenerfassung nicht vereinbar und verstößt gegen den datenschutzrechtlichen Grundsatz der strikten Zweckbindung, den Wesentlichkeitsgrundsatz und den der zeitlichen Begrenzung[17].

Im oben beschriebenen Fall bietet der Telekommunikationsanbieter Telefónica ortsbezogene Daten seiner Kunden, die im Rahmen der Erbringung des Telekommunikationsdienstes erfasst werden, zusammengefasst zu einem Bewegungsstrom an. Diese Bewegungsdaten sollen durch weitere Angaben, wie beispielsweise Alter und Geschlecht der Kunden, ergänzt werden, um so die Attraktivität und Nutzbarkeit der erhaltenen Bewegungsströme weiter zu steigern. Die Nachfrage nach so zusammengeführten Daten ist sehr groß, da diese vielfältig angewendet werden können. Auch die Telekommunikationsanbieter selbst sehen viele Möglichkeiten diese Daten zu nutzen. Ein riesiges Potential stellt dabei mobile Werbung dar, welche den Providern ermöglichen würde, ihre Kunden- und Standortdaten über externe Werbeangebote zu monetarisieren. Allerdings stellt jede Zusammenführung von Informationen eine eigene Datenanwendung dar, deren Zulässigkeit im Einzelfall zu prüfen ist.

Zur Prüfung der datenschutzrechtlichen Zulässigkeit einer Big Data Anwendung ist diese in einzelne Verarbeitungsschritte aufzuteilen und jeder einzelne Schritt gesondert zu betrachten. Vorausgesetzt es werden dabei personenbezogene Daten verwendet, muss zunächst das Ermitteln der Daten zulässig sein, weiters muss die sammelnde Stelle berechtigt sein, die Daten zu speichern und im Sinne der Big Data Auswertung weiter zu verwenden und mit anderen vorhandenen Daten zu kombinieren. Dabei ist auch zu berücksichtigen, ob gesetzliche Privilegien für die Weiterverwendung bestehen, wie beispielsweise für

[17] *Feiler/Fina*, Datenschutzrechtliche Schranken für Big Data, MR 2013, 303.

Forschende oder für Statistikbehörden. Jede Datenverwendung ist bei einer Big Data Analyse einzeln und in Kombination mit anderen Datensätzen auf Zulässigkeit zu prüfen[18].

Viele Datenschutzexperten warnen vor Big Data Anwendungen und äußern Bedenken, wenn solche Datenmengen völlig herausgelöst aus dem ursprünglichen Erhebungskontext ausgewertet werden. Das geltende Datenschutzrecht kann bei der Verwendung dieser Massen an Daten den geforderten Schutz nicht immer gewährleisten, sondern wird oft durch die anfallenden Datenmengen faktisch ausgehebelt. Auch wenn Datenansammlungen nur aus anonymisierten Daten bestehen, kann durch die Kombination mit anderen Datensätzen die Identität einzelner Personen festgestellt werden. Big Data Anwendungen mit Handy-Standortdaten sind besonders problematisch, da die Daten eines Mobiltelefons viel über die Gewohnheiten der Mobilfunkkunden aussagen können. Auch in anonymisierter Form können sie verwendet werden, um Menschen zu kategorisieren[19].

---

[18] *Weichert*, Big Data und Datenschutz <www.datenschutzzentrum.de/bigdata/20130318-bigdata-und-datenschutz.pdf>.

[19] *Biermann Kai*, „Telefonica will Handy-Bewegungsdaten an Werber verkaufen“, in: Zeit Online, 3/10/2012 <www.zeit.de/digital/datenschutz/2012-10/telefonica-smart-steps-vorratsdaten>; *Art-29-Datenschutzgruppe*, Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten, WP 185, 881/11/DE, <www.cnpd.public.lu/de/publications/groupe-art29/wp185_de.pdf>.

II. TECHNISCHE GRUNDLAGEN

Um nun schrittweise festzustellen, ob beziehungsweise inwiefern die Vermarktung ortsbezogener Mobilfunkdaten rechtmäßig ist, soll zunächst angeführt werden, um welche Daten es sich hierbei handelt.

Für die Erbringung einer mobilen Telekommunikationsdienstleistung muss die Zelle, in der sich der Kommunikationspartner befindet, identifiziert werden. Das GSM-Netz des Mobilfunknetzbetreibers ist hierarchisch sternartig strukturiert. Das funktechnisch abgedeckte Gebiet ist in Funkzellen untergliedert, die Basisstationen zugeordnet werden. Mehrere Basisstationen sind einem Aufenthaltsbereich (Location Area, LA) zugeordnet und Aufenthaltsbereiche werden von einem Base Station Controller („BSC“) verwaltet. Diese Base Station Controller wiederum werden von je einer Mobilvermittlungsstelle (Mobile Switching Center, MSC) kontrolliert. Die Basisstationen sind gemeinsam mit den Mobile Switching Center letztendlich verantwortlich, dass die Nachricht dem Empfänger zugestellt wird. Das gewählte Endgerät muss also lokalisiert werden.

Die Cell-ID, die eindeutig einer Funkzelle zugeordnet ist, identifiziert gemeinsam mit dem Location Area Code (LAC), den Standort des angerufenen Endgerätes. Während der LAC eine Gruppe von Funkzellen zusammenfasst, in denen sich das angerufene mobile Endgerät befindet, identifiziert die Cell-ID die genaue Funkzelle des Empfängers.

Mobiltelefone im empfangsbereiten Zustand melden sich in kurzen Abständen bei der Basisstation des Mobilfunknetzes an, der sie gerade zugehören. Bei dieser ständigen Positionsangabe werden an die Basisstation unter anderem die Kartennummer (IMSI[20]) und die Gerätenummer (IMEI[21]) des Mobiltelefons gesendet. Ein eingehender Anruf oder eine

[20] IMSI= International Mobile Subscriber Identity. Die IMSI ist eine internationale Registrierungsnummer auf der SIM-Karte. Die IMSI dient der eindeutigen Identifizierung des jeweiligen Nutzers. Eine IMSI-Nummer wird weltweit einmalig pro Teilnehmer von den Mobilfunknetzbetreibern vergeben.

[21] IMEI= International Mobile Equipment Identity. Diese Nummer des Geräts wird ebenso nur einmal vergeben und ist allen Netzbetreibern bekannt.

eingehende Kurzmitteilung kann somit durch Lokalisierung des Standortes des Mobiltelefons durch den Mobilfunknetzbetreiber dem Empfänger zugestellt werden[22].

Jedem Mobilfunkteilnehmer wird eine MSISDN (Mobile Station Integrated Services Digital Network Number), eine internationale Teilnehmerrufnummer, zugewiesen. Netzintern wird an jeden Mobilfunkteilnehmer auch eine IMSI (International Mobile Subscriber Identity) vergeben. Mit Hilfe der IMSI kann der Betreiber auf Teilnehmerdaten in den Mobilfunknetz-datenbanken zugreifen. Die IMSI ist auf der SIM-Karte gespeichert, dadurch kann ein Mobiltelefon einem Teilnehmer zugeordnet werden. Die IMSI wird nur beim Einbuchen zur Identifizierung verwendet und wird dann durch eine temporäre Teilnehmer-Kennung TMSI (Temporary Mobile Subscriber Identity), die vom lokalen Besucherverzeichnis VLR[23] vergeben wird, ersetzt. Dadurch bleibt der Teilnehmer bei einer bestehenden Kommunikationsverbindung anonym. Sowohl in den Datenbanken des Netzes als auch auf der SIM-Karte des Teilnehmers wird die aktuelle TMSI gespeichert, die bei erneutem Einbuchen in das Netz im VLR der IMSI zugeordnet werden kann.

Die Nutzer von Mobiltelefonen bewegen sich innerhalb der Funkzellen sowie von Funkzelle zu Funkzelle. Über eine Funkverbindung mit der Basisstation erhält also der Nutzer mit seinem mobilen Endgerät Zugang zum Mobilfunknetz und kann mittels einer Mobilvermittlungsstelle mit mobilen Teilnehmern innerhalb des gleichen Netzes oder auch anderer Netze kommunizieren[24]. Ändert sich der aktuelle Aufenthaltsbereich (Location Area) des Mobiltelefons, ändert sich die von der Basisstation ausgesendete Location Area Identity (LAI) und eine neue Aufenthaltsortsregistrierung wird gestartet[25]. Durch die Aufenthaltsorts-registrierung erhält der Teilnehmer eine neue TMSI vom VLR. Eine Aufenthaltsortsregistrierung wird automatisch durchgeführt, so dass der einzelne Teilnehmer keinen Einfluss darauf hat, wann bzw. in welcher Detaillierung sein Aufenthaltsort gespeichert wird. Die einzige Möglichkeit, die Aufenthaltsortsregistrierung zu verhindern, ist das Ausschalten des Mobiltelefons.

---

[22] <www.itwissen.info/uebersicht/lexikon/Mobilfunknetze.html?page=0>;
<www.elektronik-kompendium.de/sites/kom/1201061.htm>.
[23] VLR = Visitor Location Register.
[24] <www.bsi.bund.de/DE/Publikationen/Studien/anonym/kommunikationgsm.html>.
[25] <de.wikipedia.org/wiki/Location_Area>.

Zusammenfassend kann festgehalten werden, dass im Zusammenhang mit der Mobiltelefonie zur Unterstützung der Teilnehmermobilität und zum Auffinden von Teilnehmern im Mobilfunknetz, für Authentisierungszwecke sowie zur Prüfung von Nutzungsberechtigungen der Teilnehmer viele Daten erfasst werden. Diese werden in den einer Mobilvermittlungsstelle zugeordneten Datenbanken[26] gespeichert.

Aus der Cell-ID kann der ungefähre Aufenthaltsort des Teilnehmers bestimmt werden. Die Genauigkeit der Lokalisierung hängt von der Ausdehnung der Funkzelle ab. Bei kleinen Funkzellen sind bereits ziemlich genaue Standortinformationen ermittelbar. Die Erfassung der Cell-ID ist für eine effiziente Gesprächsvermittlung erforderlich und ist ab dem Zeitpunkt, in dem das Mobiltelefon eingeschaltet wird, fortlaufend sichergestellt. Durch die Laufzeitunterschiede eines Signals zwischen Mobiltelefon und den Basisstationen können auch genauere Standortangaben ermittelt werden.

Die genauesten Standortdaten können mithilfe von satellitengestützter GPS-Technologie (Global Positioning System) erfasst werden[27]. Heutzutage sind bereits bei den meisten Mobiltelefonen Chipsätze mit GPS-Empfängern eingebaut. GPS ist nicht für den Kommunikationsdienst selbst notwendig und kann jederzeit ausgeschaltet werden, darüber hinaus ist die Inanspruchnahme von GPS grundsätzlich nicht auf Speicherung und Übermittlung von Daten angewiesen. Damit ist die Relevanz von GPS für die vorliegende Arbeit nicht gegeben.

---

[26] Heimatregister (Home Location Register, HLR), Besucherregister (Visitor Location Register, VLR), Authentisierungszentrum (Authentication Centre, AC), Geräteidentifizierungsregister (Equipment Identity Register, EIR).

[27] *Kassai*, "Location Based Services" im Gefüge des Datenschutzrechts, MR 2004, 433.

III. DATENSCHUTZRECHTLICHE BESTIMMUNGEN

Durch die zunehmende Verbreitung der elektronischen Datenverarbeitung Anfang der Siebzigerjahre wurde die Verknüpfung verschiedener Datenbestände merklich vereinfacht, was eine neue Gefahr der Privatsphäre darstellte. Die automatisierte Datenverarbeitung führte daher zur Notwendigkeit, dem Einzelnen Schutz seiner Daten zuzusichern und das Datenschutzgesetz 1978 wurde erlassen. Der Zweck des Datenschutzes änderte sich aber bereits in den Achtzigerjahren von einem Abwehrrecht zu einem Gestaltungsrecht, zu einer Garantie einer informationellen Selbstbestimmung, die auch Ziel der europäischen Datenschutzrichtlinie aus dem Jahr 1995 wurde. Für die Verarbeitung und Übermittlung personenbezogener Daten im Bereich der Telekommunikation wurden 2002 mit der Datenschutzrichtlinie für elektronische Kommunikation spezifische Datenschutzbestimmungen vorgesehen. Aufgrund der laufenden technologischen Entwicklung ist auch das Datenschutzrecht laufend anzupassen; zur aktuellsten Anpassung der datenschutzrechtlichen Bestimmungen an den Stand der Technik soll nun eine Verordnung erlassen werden, die die Verarbeitung personenbezogener Daten europaweit einheitlich regeln soll[28].

A. DATENSCHUTZRICHTLINIEN

Auf europäischer Ebene regelt seit 1995 die Richtlinie 95/46/EG[29] die Verwendung personenbezogener Daten. Die Vorgaben dieser Richtlinie sind - teilweise unzureichend - durch das Datenschutzgesetz 2000 in österreichisches Recht umgesetzt worden. In Fällen mangelhafter Umsetzung sind die Bestimmungen der oben angeführten Datenschutzrichtlinie unmittelbar anzuwenden[30]. Nach ständiger Judikatur des EuGH wird aufgrund der

---

[28] *Mayer-Schönberger/Zeger/Kronegger*, Auf dem Weg nach Europa: Zur Novellierung des Datenschutzgesetzes, ÖJZ 1998, 244; *Jahnel,* Datenschutzrecht, in Jahnel /Mader/Staudegger (Hrsg), IT-Recht³ (2012) 419ff.

[29] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31 idF L 2003/284, 1. *Jahnel,* Handbuch Datenschutzrecht (2010) RZ 1/32.

[30] *Jahnel,* Datenschutzrecht, in Jahnel /Mader/Staudegger (Hrsg), IT-Recht³ (2012) 421.

binnenmateriellen Relevanz des freien Verkehrs personenbezogener Daten grundsätzlich der Datenschutzrichtlinie eine vollharmonisierende Wirkung nahe gelegt[31].

Mit Artikel 29 setzt die Richtlinie auch eine eigene Gruppe aus Vertretern der Datenschutzkontrollstellen der einzelnen Mitgliedstaaten für den Schutz von Personen bei der Verarbeitung personenbezogener Daten ein, die auch eine einheitliche Anwendung der Grundsätze der Richtlinie sicherstellen soll.

Die allgemeine Datenschutzrichtlinie wird durch die sektorspezifische Datenschutzrichtlinie für elektronische Kommunikation ergänzt[32]. Für öffentliche Kommunikationsnetze sollen besondere rechtliche und technische Vorschriften gelten zum Schutz der Grundrechte natürlicher Personen[33]. Die allgemeine Datenschutzrichtlinie gilt daher im Bereich der elektronischen Kommunikation vor allem für allgemeine Fragen des Grundrechtsschutzes, die nicht spezifisch von der Datenschutzrichtlinie für elektronische Kommunikation erfasst und geregelt werden und für nicht öffentliche Kommunikationsdienste[34].

Unter Berücksichtigung der raschen Entwicklung der Märkte und Technologien für elektronische Kommunikationsdienste, sowie der zunehmenden Möglichkeiten zur automatischen Datenspeicherung, zielt die Richtlinie 2002/58/EG darauf ab, dass in den Mitgliedstaaten besondere rechtliche und technische Vorschriften zum Schutz der Grundrechte und Grundfreiheiten in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation erlassen werden[35]. Öffentlich zugängliche Kommunikationsdienste in öffentlichen Kommunikationsnetzen eröffnen zwar neue

---

[31] So stellte der EuGH im Urteil in den verbundenen Rechtssachen C-468/10 und C-469/10 fest, dass die Richtlinie 95/46/EG auf eine Vollharmonisierung der Rechte der Mitgliedstaaten abzielt und nicht nur einen Mindeststandard für den Datenschutz schaffen will. (EuGH 24.11.2011, C-468/10, C-469/10 (ASNEF/FECEMD) in *Thiele,* EuGH Urteil vom 24.11.2011, C-468/10, C-469/10 - ASNEF/FECEMD <www.eurolawyer.at/pdf/EuGH-C-468-10.pdf>).

[32] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl L 2002/201, 37 idF L 2009/337, 11.

[33] ErwGr 7 RL 2002/58/EG.

[34] ErwGr 10 RL 2002/58/EG.

[35] ErwGr 7 RL 2002/58/EG.

Möglichkeiten, gefährden jedoch gleichzeitig auch den Schutz personenbezogener Daten der Nutzer[36]. Aufgrund des besonderen Risikos im Bereich der Telekommunikation sollen bereichsspezifische Datenschutzbestimmungen gelten, die eine Detaillierung und Ergänzung der allgemeinen Datenschutzrichtlinie darstellen[37].

B. VORRATSDATENSPEICHERUNGSRICHTLINIE

Die Vorratsdatenspeicherungsrichtlinie[38] legte die Pflichten von Anbietern öffentlicher Kommunikationsdienste zur Vorratsspeicherung bestimmter Daten, die im Zusammenhang mit der Bereitstellung dieser Dienste anfallen, fest. Ziel dieser Richtlinie war es sicherzustellen, dass diese Daten zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen. Die Speicherpflicht bezog sich auf Verkehrs- und Standortdaten, nicht auf den Inhalt elektronischer Nachrichtenübermittlungen[39]. Die Vorratsdatenspeicherungsrichtlinie wurde jedoch vom Europäischen Gerichtshof für ungültig erklärt[40]. Demnach stellt die Vorratsdatenspeicherung einen unverhältnismäßigen Eingriff in die Grundrechte dar, insbesondere in die Grundrechte auf Achtung des Privat- und Familienlebens und auf Schutz personenbezogener Daten, die auch Inhalt der Charta der Grundrechte der Europäischen Union sind.

C. TKG als lex specialis zum DSG

Die nationalen Gesetze spiegeln die europäische Struktur wider und regeln das allgemeine Datenschutzrecht im DSG 2000 und die für den Telekommunikationsbereich spezifischen Datenschutzbestimmungen im TKG 2003[41]. Das DSG bildet die Basis für die sektorspezifischen Regelungen im TKG und findet auch auf im TKG geregelte Sachverhalte

---

[36] ErwGr 6 RL 2002/58/EG.
[37] *Reiter/Wittmann-Tiwald* (Hrsg), Goodbye Privacy (2008) 25.
[38] Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. Nr. L 105 vom 13.4.2006.
[39] *Reiter/Wittmann-Tiwald* (Hrsg), Goodbye Privacy (2008) 26.
[40] EuGH 08.04.2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd und Seitlinger).
[41] Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 - TKG 2003), BGBl I 70/2003 idF I 44/2014.

Anwendung, soweit dieses nicht anderes bestimmt[42]. Die Spezialbestimmungen finden sich in den §§ 92 - 107 des TKG, die leges speciales zum DSG sind und dieses ergänzen[43].

Nach dem Grundrecht auf Datenschutz hat jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Geheimhaltungsinteresse besteht. Das Grundrecht auf Geheimhaltung schützt vor Ermittlung und Übermittlung von Daten, vor zwangsweiser Verpflichtung zur Weitergabe oder Offenlegung von Daten. Grundsätzlich ist die Verwendung von Daten verboten, es sei denn, die Daten unterliegen nicht dem Datenschutz oder es liegt ein Erlaubnistatbestand vor[44].

Die Verarbeitung von Daten, die vom Datenschutz erfasst werden, ist dann zulässig, wenn ihr Zweck und Inhalt durch eine gesetzliche Zuständigkeit oder eine rechtliche Befugnis gedeckt sind, also wenn für die Datenverarbeitung eine Berechtigung des Auftraggebers vorliegt, und wenn dadurch schutzwürdige Interessen der betroffenen Personen nicht verletzt werden[45]. Bei der Beurteilung, ob schutzwürdige Geheimhaltungsinteressen der Betroffenen verletzt werden, ist grundsätzlich zu unterscheiden, ob sensible oder nicht sensible Daten verarbeitet werden[46]. Sofern nicht ein in § 9 DSG enthaltener Ausnahmetatbestand vorliegt, ist die Verwendung sensibler Daten verboten. Handelt es sich hingegen um nicht sensible Daten und liegt keine gesetzliche Ermächtigung, Zustimmung oder ein lebenswichtiges Interesse des Betroffenen vor, wodurch die Verwendung der nicht sensiblen Daten erlaubt wäre, ist in Form einer Interessenabwägung zu prüfen, ob schutzwürdige Geheimhaltungsinteressen verletzt werden. § 8 DSG enthält eine beispielhafte Aufzählung von Verwendungsfällen, die keine Verletzung schutzwürdiger Geheimhaltungsinteressen darstellen[47].

---

[42] § 92 Abs 1 S 2 TKG.
[43] *Brandl/Feiel,* Telekommunikationsrecht, in Jahnel /Mader/Staudegger (Hrsg), IT-Recht³ (2012) 562f.
[44] *Graf*, Datenschutzrecht im Überblick² (2010) 41.
[45] § 7 Abs 1 DSG.
[46] § 4 Z 2 DSG *„sensible Daten" („besonders schutzwürdige Daten"): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben.*
[47] *Pollirer/Weiss/Knyrim*, DSG² § 8 (2014), 45; *Jahnel,* Datenschutzrecht, in Jahnel /Mader/Staudegger (Hrsg), IT-Recht³ (2012) 433ff; *Jahnel*, Handbuch Datenschutzrecht (2010) RZ 4/20; *Knyrim*, Datenschutzrecht: Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm (2012) 75ff; *Graf*, Datenschutzrecht im Überblick² (2010) 43.

Für den spezifischen Bereich der Telekommunikation werden strengere Regelungen für die Verarbeitung personenbezogener Daten vorgesehen. Demnach dürfen Daten nur im Zusammenhang mit der Bereitstellung von Kommunikationsdiensten verwendet werden. Für jede sonstige Verwendung ist die Zustimmung des Betroffenen erforderlich. Ein besonderer Schutz wird für diesen Bereich auch aufgrund der zunehmenden Fähigkeiten zur automatischen Speicherung personenbezogener Daten und der einfachen Verknüpfbarkeit der erfassten Daten vorgesehen. Darüber hinaus können gerade im Bereich der Telekommunikation riesige Datenmengen durch eine Datenschutzverletzung betroffen sein[48].

Da das DSG den Ansatz eines generellen Datenschutzrechts verfolgt, sollen diese allgemeinen Bestimmungen durch die bereichsspezifischen Bestimmungen nur hinsichtlich bereichsspezifischer Besonderheiten ergänzt werden. Der 12. Abschnitt des TKG gilt für die Verwendung der Daten im Zusammenhang mit der Bereitstellung öffentlicher Kommunikationsdienste und bestimmt weiters auch die Zulässigkeit der Speicherung und die Verpflichtung zur Löschung dieser Daten[49]. Dieser Abschnitt sieht einleitend ergänzend zu den allgemeinen Definitionen des § 3 TKG eigene Begriffsbestimmungen für den Datenschutzbereich vor[50].

Abweichend vom allgemeinen Datenschutzrecht, das die zentrale Verantwortlichkeit für die Datenverwendung dem Auftraggeber zuweist, also demjenigen, der die Entscheidung getroffen hat, die Daten zu verwenden[51], richtet sich das bereichsspezifische Datenschutzrecht des TKG vor allem an Anbieter[52]. Dabei versteht man unter „Anbieter“ gemäß § 92 Abs 3 Z 1 Betreiber von öffentlichen Kommunikationsdiensten, also jeden, der einen öffentlichen Kommunikationsdienst anbietet und nicht notwendigerweise alle Funktionen dieses Dienstes kontrolliert. Der Begriff des Anbieters ist daher weiter auszulegen als der des Betreibers eines Kommunikationsdienstes. Der Betreiber eines Kommunikationsnetzes oder –dienstes, auf den

---

[48] vgl. auch *Bauer/Reimer* (Hrsg), Handbuch Datenschutzrecht (2009) 419f.
[49] *Brandl/Feiel,* Telekommunikationsrecht, in Jahnel /Mader/Staudegger (Hrsg), IT-Recht³ (2012) 562ff; *Stratil* (Hrsg), TKG 2003⁴ § 92 Anm 3 (2013).
[50] *Stratil* (Hrsg), TKG 2003⁴ § 92 Anm 5 (2013).
[51] § 4 Z 4 DSG.
[52] *Kassai*, "Location Based Services" im Gefüge des Datenschutzrechts, MR 2004, 433.

grundsätzlich im TKG abgestellt wird, ist in § 3 TKG definiert[53]. Zur Einhaltung der datenschutzrechtlichen Bestimmungen soll jedoch jeder Anbieter unmittelbar gezwungen werden und nicht nur derjenige, der die zur Erbringung des Kommunikationsdienstes notwendigen Funktionen kontrolliert, um so einen besseren Verbraucherschutz zu gewährleisten[54].

1. Anwendung des TKG

Die besonderen datenschutzrechtlichen Bestimmungen des TKG gelten für die Verarbeitung und Übermittlung von personenbezogenen Daten in Verbindung mit der Bereitstellung öffentlicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen[55]. Ein „Kommunikationsdienst" ist gemäß § 3 Z 9 TKG eine gewerbliche Dienstleistung, die in der Übertragung von Signalen über Kommunikationsnetze besteht[56]. Das TKG definiert nicht den Begriff „öffentlicher Kommunikationsdienst", bestimmt aber, dass ein „öffentliches Kommunikationsnetz" zur Bereitstellung öffentlich zugänglicher Kommunikationsdienste dient[57]. Ein Kommunikationsdienst, der nur einer geschlossenen Benutzergruppe zur Verfügung gestellt wird, ist demnach kein öffentlicher Kommunikationsdienst. Hingegen ist der Dienst der Mobiltelefonie, den Telefónica gewerblich der Öffentlichkeit anbietet, auf jeden Fall ein öffentlicher Kommunikationsdienst, und Telefónica gilt als „Anbieter" im Sinne des § 92 Abs 3 Z 1 TKG. Für das Produkt Smart Steps verwendet der Betreiber die Mobilfunkdaten der Kunden, die im Rahmen der Bereitstellung des öffentlichen Mobiltelefoniedienstes anfallen.

Voraussetzung für das Recht auf Datenschutz – sowohl nach dem allgemeinen DSG als auch nach dem TKG – ist die Verwendung personenbezogener Daten. Handelt es sich bei den Mobilfunkdaten der Kunden um personenbezogene Daten, finden nach österreichischem

---

[53] § 3 Z 3 TKG: "Betreiber eines Kommunikationsdienstes" (ist) ein Unternehmen, das die rechtliche Kontrolle über die Gesamtheit der Funktionen, die zur Erbringung des jeweiligen Kommunikationsdienstes notwendig sind ausübt und diese Dienste anderen anbietet.
[54] *Stratil* (Hrsg), TKG 2003[4] § 92 Anm 6 (2013).
[55] § 92 Abs 1 S 1 TKG.
[56] *Bauer/Reimer*, Handbuch Datenschutzrecht (2009) 421.
[57] § 3 Z 17 TKG.

Recht zumindest auf die Verwendung dieser Daten in Verbindung mit der Bereitstellung des Kommunikationsdienstes die datenschutzrechtlichen Spezialbestimmungen des TKG Anwendung[58].

2. § 92 Allgemeines - Verkehrs- und Standortdaten

Zu Beginn des Datenschutzabschnitts des TKG werden auch die dafür relevanten Datenkategorien definiert. Gemäß § 92 Abs 3 Z 6 TKG sind Standortdaten jene Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geographischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben.

Solche Angaben können sich also auf den Standort des Endgeräts nach geographischer Länge, Breite und Höhe beziehen, auf die Übertragungsrichtung, den Grad der Genauigkeit der Standortinformation, die Identifizierung des Netzpunktes, an dem sich das Endgerät zu einem bestimmten Zeitpunkt befindet, und auch auf den Zeitpunkt, zu dem die Standortinformationen erfasst werden[59]. Um den Dienst der mobilen Telefonie oder eines ortsbezogenen Zusatzdienstes überhaupt erbringen zu können, muss der Mobilfunkanbieter die ortsbezogenen Daten auch einem bestimmten Teilnehmer zuordnen können. Wie oben ausgeführt, erfolgt dies mit Hilfe der MSISDN und IMSI, die jeweils einem bestimmten Teilnehmer zugeordnet ist; die Daten sind dadurch auf jeden Fall personenbezogen. Die Verarbeitung dieser Daten ist eine besonders sensible Angelegenheit, da aus den Standortinformationen der mobilen Endgeräte Rückschlüsse auf Gewohnheiten einzelner

[58] Der OGH (22. 6. 2012, 6 Ob 119/11k) hat grundlegend entschieden, dass die Verwendung personenbezogener Daten iVm der Bereitstellung von Diensten, die keine elektronischen Kommunikationsdienste darstellen, nicht von den §§ 92 ff TKG erfasst wird, ohne dabei auf das Kriterium der „Öffentlichkeit" des Kommunikationsdienstes einzugehen.

[59] ErwGr 14 RL 2002/58/EG.

Personen gezogen werden können[60]. Es sind daher eigene Vorschriften hinsichtlich der Verwendung solcher Standortdaten erlassen worden[61].

Im Zuge der Umsetzung der Richtlinie zur Vorratsdatenspeicherung[62] ist die Verpflichtung zur Führung von historischen Aufzeichnungen über die Standorte von Funkzellen durch die Mobilfunknetzbetreiber mittels Speicherung der Cell-ID eingeführt worden. Dabei wurde auch die Definition der „Cell-ID" in § 92 Abs 3 Z 6a TKG hinzugefügt, nach der die „Standortkennung" die Kennung einer Funkzelle ist, über welche eine Mobilfunkverbindung hergestellt wird[63]. Mit § 90 Abs 8 TKG wurde Artikel 5 Abs 1 lit f Z 2 der Vorratsdatenspeicherungsrichtlinie umgesetzt und sichergestellt, dass die Betreiber jederzeit in der Lage sein müssen, trotz sich ständig ändernder Funkzellen die Zuordnung einer Cell-ID zum tatsächlichen geografischen Standort für jeden Zeitpunkt in den letzten sechs Monaten anzugeben[64].

Die Verpflichtung zur Speicherung der Standortkennung wurde nicht unter den Regelungen der Verarbeitung von Standortdaten festgeschrieben, sondern ist unter den Informationspflichten des § 90 TKG geregelt worden. Die Speicherpflicht der Cell-ID ist dabei bewusst an dieser Stelle festgehalten worden und somit auch nicht im Rahmen der Aufzählung der einzelnen „Vorratsdaten" in § 102a TKG enthalten, um damit klar zu stellen, dass auch durch die Einführung der Vorratsdatenspeicherung die Erfassung von kommunikationsunabhängigen Bewegungsprofilen nicht erlaubt werden sollte. Dennoch wurde gerade die Speicherung der Verkehrs- und Standortdaten an der Vorratsdaten-speicherung besonders kritisiert, da dadurch leicht Bewegungsprofile erstellt werden könnten, was einen massiven Eingriff in das Grundrecht auf Privatsphäre darstellt[65].

---

[60] *Art-29-Datenschutzgruppe*, Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten, WP 185, 881/11/DE, <www.cnpd.public.lu/de/publications/groupe-art29/wp185_de.pdf>.

[61] *Art-29-Datenschutzgruppe,* Stellungnahme 5/2005 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen, WP 115, 2130/05/DE, <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_de.pdf>.

[62] RL 2006/24/EG.

[63] Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 - TKG 2003 geändert wird, BGBl. I Nr. 27/2011.

[64] Regierungsvorlage ErlRV 1074 BlgNR XXIV. GP .

[65] *Baumgartner*, Grundrechte und Datenschutz, AnwBl 2014, 24 (28).

Die Richtlinie über die Vorratsdatenspeicherung ist vom Europäischen Gerichtshof am 8.4.2014 für ungültig erklärt worden[66]. Mit Entscheidung vom 27. Juni 2014[67] hat der Verfassungsgerichtshof die nationalen Bestimmungen der Vorratsdatenspeicherung als verfassungswidrig erklärt. In der entsprechenden Kundmachung über die Aufhebung von Bestimmungen zur Vorratsdatenspeicherung finden sich jedoch weder § 90 Abs 8 TKG noch die Definition der Cell-ID in § 92 Abs 3 Z 6a TKG, weshalb diese Bestimmungen immer noch geltendes Recht sind.

Der Standort des Endgeräts des Absenders oder des Empfängers ist ein „Verkehrsdatum“[68]. Unter „Verkehrsdaten“ fallen alle Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden. Diese Begriffsbestimmung des § 92 Abs 3 Z 4 TKG übernimmt die Definition für Verkehrsdaten in Art 2 lit b der Datenschutzrichtlinie für elektronische Kommunikation. Dabei wurde wörtlich der Zweck der Weiterleitung „an ein“ Kommunikationsnetz übernommen, auch wenn hier wohl Daten erfasst sind, die zum Zweck jeder Weiterleitung einer Nachricht auch „über“ das Kommunikationsnetz verarbeitet werden[69]. So ist es auch in der englischen Fassung der Datenschutzrichtlinie für elektronische Kommunikation definiert, während die französische oder spanische Version klar ausdrücken, dass die Daten der Weiterleitung einer Nachricht über ein Netz dienen[70].

Unter Verkehrsdaten fallen insbesondere auch die aktive und passive Teilnehmernummer, die zu verrechnenden Einheiten, die Art, Datum, Zeitpunkt und Dauer einer Kommunikation, das Netz, von dem die Nachricht ausgeht oder an das sie gesendet wird, und eben der Standort, an dem sich das die Nachricht empfangende oder sendende Endgerät befindet.

---

[66] EuGH 08.04.2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd und Seitlinger).
[67] VfGH 27.06.2014, G 47/2012.
[68] ErwGr 15 RL 2002/58/EG.
[69] *Stratil* (Hrsg), TKG 2003[4] ErläutRV zu § 92 (2013).
[70] Art 2 b RL 2002/58/EG ‘*traffic data’ means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*; anders in der französischen Version, in der Art b) klar bestimmt: "*données relatives au trafic": toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation;* oder *«datos de tráfico»: cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma.*

Standortdaten zählen also zu den Verkehrsdaten, wenn ihre Ermittlung der Weiterleitung einer Nachricht an ein oder über ein Kommunikationsnetz dient. Es können aber auch andere Standortdaten als Verkehrsdaten ermittelt werden. Werden im Mobilfunknetzbereich diese „reinen" Standortdaten mit anderen Daten verknüpft, können Dienste mit Zusatznutzen generiert werden, die man als Location Based Service (LBS) bezeichnet[71].

3. § 93 - Kommunikationsgeheimnis

Verkehrsdaten und Standortdaten, sowie auch Inhaltsdaten, unterliegen dem in § 93 TKG verankerten Kommunikationsgeheimnis, das einfachgesetzlich das Grundrecht des Fernmeldegeheimnisses[72] näher ausführt. Das Fernmeldegeheimnis umfasst Kommunikationsinhalte, die über Fernmeldeanlagen übermittelt werden, und erlaubt Eingriffe nur aufgrund eines richterlichen Befehls. Das Kommunikationsgeheimnis verbietet das Mithören, Abhören, Aufzeichnen, Abfangen und sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten, wenn nicht eine Einwilligung aller beteiligten Benutzer oder eine gesetzliche Ausnahme vorliegt[73]. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit, durch die sie begründet wurde. Verkehrsdaten unterliegen dem Kommunikationsgeheimnis, da anhand dieser geschlossen werden kann, wer mit wem Kontakt hat. Zur Wahrung des Kommunikationsgeheimnisses werden alle Betreiber eines öffentlichen Kommunikationsnetzes oder –dienstes verpflichtet. Ein Verstoß gegen das Kommunikationsgeheimnis ist mit einer Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen, vorausgesetzt die Tat ist nicht schon nach einer anderen Bestimmung mit höherer Strafe bedroht und es liegt ein Antrag des Verletzten vor[74].

Standortdaten werden ebenso vom Kommunikationsgeheimnis erfasst, da diese meistens Verkehrsdaten sind. Es wäre sachlich nicht gerechtfertigt, diese anders zu

---

[71] *Pfarl*, Gefunden! LBS im Mobilfunknetzbereich, ecolex 2005, 569.
[72] Artikel 10a StGG: *Das Fernmeldegeheimnis darf nicht verletzt werden. Ausnahmen von der Bestimmung des vorstehenden Absatzes sind nur auf Grund eines richterlichen Befehles in Gemäßheit bestehender Gesetze zulässig*.
[73] § 93 Abs 3 TKG.
[74] §108 TKG.

behandeln. Andere Standortdaten als Verkehrsdaten sind außerdem besonders schutzwürdig, da anhand von Standortdaten ziemlich genaue Bewegungsprofile der Teilnehmer erstellt werden können[75] und der Aufenthaltsort der Teilnehmer bestimmt werden kann[76].

4. § 96 Datenschutz – Allgemeines

Die §§ 96 ff TKG legen Einschränkungen für die Verwendung der einzelnen Datenkategorien fest. Die allgemeine Datenschutzbestimmung des § 96 Abs 1 TKG hält für alle Datenkategorien fest: *Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten dürfen nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden*.

Das TKG sieht keine besondere Definition für den Begriff „Verarbeiten" vor und nach der allgemeinen Definition im DSG umfasst das „Verarbeiten"[77] das „Ermitteln" ohnehin[78]. Unter „Verarbeiten von Daten" subsumiert das DSG jede Art der Handhabung von Daten mit Ausnahme des Übermittelns. Das Übermitteln von Daten ist die Weitergabe der Daten und umfasst auch die Verwendung der Daten für ein anderes Aufgabengebiet[79]. Gemäß § 96 Abs 2 TKG dürfen die Stamm-, Verkehrs-, Standort- und Inhaltsdaten nur übermittelt werden, soweit das für die Erbringung des Kommunikationsdienstes erforderlich ist. Dahingegen ist die Verarbeitung der Daten bereits zulässig, wenn diese für die Besorgung des Kommunikationsdienstes bloß zweckbezogen ist[80].

Weiters hält § 96 ausdrücklich fest, dass die Verwendung der Daten zum Zweck der Vermarktung von Kommunikationsdiensten oder der Bereitstellung von Diensten mit

---

[75] *Brandl/Feiel,* Telekommunikationsrecht, in Jahnel /Mader/Staudegger (Hrsg), IT-Recht³ (2012) 563ff; *Stratil* (Hrsg), TKG 2003[4] ErläutRV zu § 93 (2013).

[76] *Kassai*, "Location Based Services" im Gefüge des Datenschutzrechts, MR 2004, 433.

[77] § 4 Z 9 DSG: *Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (Z 12) von Daten*;

[78] *Kassai*, "Location Based Services" im Gefüge des Datenschutzrechts, MR 2004, 433.

.[79] § 4 Z 12 DSG; *Jahnel,* Handbuch Datenschutzrecht (2010) RZ 3/124.

[80] *Zib*, Zur Zulässigkeit elektronischer Rechnungspräsentation bei Telekom- und Mobilfunk-Rechnungen, ÖBA 2004, 463 (467); anders Kassai, nach dem „Verarbeiten" wohl die Übermittlung miteinschließt in Anlehnung an das „Verarbeiten" im Sinne der Datenschutzrichtlinie, das im österreichischen Datenschutz als „Verwenden von Daten" umgesetzt wurde, siehe *Kassai,* "Location Based Services" im Gefüge des Datenschutzrechts, MR 2004, 433.

Zusatznutzen sowie sonstige Übermittlungen nur aufgrund einer jederzeit widerrufbaren Zustimmung erfolgen darf. In Absatz 3 wird die Pflicht der Betreiber und Anbieter vorgesehen, die Teilnehmer oder Benutzer klar und umfassend darüber zu informieren, welche personenbezogenen Daten zu welchem Zweck verarbeitet werden.

5. § 99 - Verkehrsdaten

Während § 96 TKG allgemein eine klare Zweckbindung bei der Verwendung der sektorspezifischen Datenkategorien festlegt, regelt § 99 TKG speziell die Verwendung von Verkehrsdaten. Demnach dürfen Verkehrsdaten *außer in den in diesem Gesetz geregelten Fällen nicht gespeichert oder übermittelt werden und sind vom Anbieter nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren*[81]. Die Zulässigkeit einer weiteren Verwendung der Verkehrsdaten, die zu Auskunftszwecken übermittelt werden, richtet sich nach der StPO sowie nach dem SPG, auf die hierin nicht näher eingegangen wird.

§ 99 Abs 1 TKG setzt Art 6 der RL 2002/58/EG um, ist aber formal strenger gefasst, da bereits eine gesetzlich nicht vorgesehene Speicherung untersagt ist. Ziel dieser Bestimmung ist die Vermeidung, einen umfangreichen Datenbestand anzuhäufen, *der auch zu anderen als den gesetzlich vorgesehenen Zwecken genutzt (missbraucht) werden könnte*[82]. Nicht nur im Sinne datenschutzrechtlicher Grundsätze sollten bei der Bereitstellung des Kommunikationsdienstes so wenig personenbezogene Daten wie möglich verwendet werden, sondern auch nach Erwägungsgrund 30 der sektorspezifischen Richtlinie. Demnach soll jede Tätigkeit, die über die Übermittlung einer Nachricht und entsprechender Fakturierung hinausgeht, auf aggregierten Verkehrsdaten basieren, die nicht mit einzelnen Teilnehmern in Verbindung gebracht werden können. Kann die Tätigkeit nicht auf aggregierte Daten gestützt werden, soll sie als Dienst mit Zusatznutzen ausgeführt werden, für welchen eine entsprechende Einwilligung des Teilnehmers erforderlich ist[83].

---

[81] § 99 Abs 1 TKG.
[82] OGH 14.7.2009, 4 Ob 41/09x.
[83] ErwGr 30 RL 2002/58/EG; *Pfarl*, Datenschutz bei LBS im Mobilfunkbereich und im europäischen Notrufsystem <www.it-law.at/uploads/tx_publications/Datenschutz_bei_LBS.pdf>.

Alle zulässigen Fälle, in denen der Anbieter die Verkehrsdaten verwenden darf, werden im TKG geregelt; aus anderen Quellen soll sich nicht implizit eine Berechtigung oder Verpflichtung zur Speicherung oder Übermittlung ableiten lassen. Davon unberührt bleibt die Verwendung der Verkehrsdaten durch die Strafverfolgungsbehörden. § 99 Abs 4 TKG hält fest, dass der Anbieter außer in den im TKG geregelten Fällen die Verkehrsdaten nur mit Zustimmung des Teilnehmers zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen verwenden darf[84]. Eine betriebsnotwendige Speicherung von Verkehrsdaten zur Sicherstellung der Netzqualität wird auch auf jeden Fall vom Zweck der Bereitstellung des Kommunikationsdienstes umfasst. Die Verwendung der Verkehrsdaten zu diesem Zweck wird daher als zulässig erachtet[85] und bedarf keiner zusätzlichen Zustimmung.

Verkehrsdaten sind gemäß § 99 Abs 2 TKG zum Zwecke der Verrechnung zu speichern. Wird nicht innerhalb einer Frist von drei Monaten ein Einspruch gegen die Rechnung erhoben und ist der Bezahlvorgang durchgeführt, sind die Verkehrsdaten zu löschen oder zu anonymisieren.

6. § 102 – Andere Standortdaten als Verkehrsdaten

Gemäß § 102 Abs 1 TKG dürfen andere Standortdaten als Verkehrsdaten nur verarbeitet werden, wenn sie entweder anonymisiert werden oder der Benutzer oder Teilnehmer eine jederzeit widerrufbare Einwilligung gegeben hat[86]. Die Verarbeitung dieser Standortdaten muss sich beschränken auf das für die Bereitstellung eines Dienstes mit Zusatznutzen erforderliche Maß[87]. Der Benutzer oder Teilnehmer muss die Möglichkeit haben, die Verarbeitung seiner Standortdaten jederzeit einfach und kostenlos zu untersagen[88].

[84] *Stratil* (Hrsg), TKG 2003[4] ErläutRV zu § 99 Abs 1 (2013).
[85] *Stratil* (Hrsg), TKG 2003[4] § 99 Anm 1 (2013).
[86] Zur Verwendung der Begriffe Benutzer/Teilnehmer sowie Einwilligung siehe 7.
[87] *Koller/Singer/Steinmaurer*, Datenschutz und Telekommunikation, in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 426.
[88] § 102 Abs 2 TKG; ErwGr 35 RL 2002/58/EG.

Ausgenommen von diesen Bedingungen ist die Verarbeitung anderer Standortdaten als Verkehrsdaten zur Auskunft an Betreiber von Notrufdiensten im Sinne des § 98 TKG[89].

Ein „Dienst mit Zusatznutzen“ ist beispielsweise ein Auskunftsdienst über Sehenswürdigkeiten oder Navigationshilfen, Verkehrsinformationen oder zum Beispiel die Wettervorhersage[90]. Die Einwilligung des Benutzers oder Teilnehmers erfolgt dabei meistens dadurch, dass der Dienst einfach in Anspruch genommen wird. Dadurch muss der Nutzer nicht zusätzlich die Einwilligung widerrufen, sondern gibt diese immer nur für eine spezifische Anfrage ab[91].

Andernfalls, wenn nicht die Einwilligung des Benutzers oder Teilnehmers vorliegt, dürfen gemäß § 102 Abs 1 TKG andere Standortdaten als Verkehrsdaten nur verarbeitet werden, wenn sie anonymisiert werden. Nach § 102 Absatz 3 muss eine Verarbeitung gemäß Absatz 1 (und 2) auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß beschränkt werden[92].

Hält man am Wortlaut des § 102 TKG fest, scheint es also, dass dieser strenge Zweckbindungsgrundsatz auch für anonymisierte Daten gelten soll, dass also auch anonymisierte Standortdaten nur in dem Maße verarbeitet werden sollen, als dies für den Dienst mit Zusatznutzen erforderlich ist. Auch die Datenschutzrichtlinie für elektronische Kommunikation bringt in Artikel 9 zum Ausdruck, dass diese vom Kommunikationsdienst unabhängigen Standortdaten nur im zur Bereitstellung des Dienstes mit Zusatznutzen erforderlichen Maß und nur innerhalb des dafür erforderlichen Zeitraums verarbeitet werden

---

[89] § 98 TKG regelt Auskünfte an Betreiber von Notrufdiensten. Gem § 98 TKG haben Betreiber eines Kommunikationsnetzes oder –dienstes Betreibern von Notrufdiensten auf deren Verlangen Auskünfte über Stammdaten und Standortdaten zu erteilen. In beiden Fällen ist Voraussetzung für die Zulässigkeit der Übermittlung ein Notfall, der nur durch Bekanntgabe dieser Informationen abgewehrt werden kann. Die Zulässigkeit der Übermittlung dieser Daten ergibt sich aus der Interessenabwägung, die zugunsten der Übermittlung ausfällt. Gem § 98 Abs 2 TKG darf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung des gefährdeten Menschen verarbeitet werden, wenn eine aktuelle Standortfeststellung nicht möglich ist. Der Anbieter hat den betroffenen Teilnehmer über eine solche Auskunft zu informieren. Betreiber von Kommunikationsnetzen haben bei der Ermittlung des Standortes der Telekommunikationsendeinrichtung entgeltfrei mitzuwirken.

[90] ErwGr 18 RL 2002/58/EG; *Jahnel*, Spamming, Cookies, Logfiles und Location Based Services im TKG 2003, ÖJZ 2004/21, 336.

[91] *Stratil* (Hrsg), TKG 2003[4] §102 Anm 2 (2013).

[92] § 102 Abs 3 TKG.

dürfen, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben[93]. Allerdings wird auch im Erwägungsgrund 35 auf andere Standortdaten als Verkehrsdaten eingegangen und bestimmt, dass ihre Verarbeitung nur für die Bereitstellung von Diensten mit Zusatznutzen gestattet wird, wenn der Teilnehmer eingewilligt hat. Liegt also keine Einwilligung vor, dürfen nur anonymisierte Standortdaten verarbeitet werden. So hat auch die Datenschutzbehörde § 102 TKG ausgelegt, dass andere Standortdaten als Verkehrsdaten nur verarbeitet werden dürfen, wenn sie anonymisiert oder die Benutzer oder Teilnehmer eine jederzeit widerrufbare Einwilligung gegeben haben[94]. Eine andere Auslegung des § 102 TKG wäre mit dem Datenschutzrecht nicht vereinbar. Auf die Grenzen der Anwendbarkeit des Datenschutzrechts wird in Kapitel IV näher eingegangen.

Dem Wortlaut des § 102 TKG zufolge ist nur das Verarbeiten solcher Standortdaten zweckgebunden. Wie bereits erwähnt, wird das „Verarbeiten von Daten" nur im DSG definiert und umfasst jede Art der Handhabung von Daten mit Ausnahme des Übermittelns[95], das auch die Verwendung für ein anderes Aufgabengebiet umfasst[96]. Das „Verarbeiten" in § 102 TKG wird aber wohl die Übermittlung miteinschließen in Anlehnung an das „Verarbeiten" im Sinne der Datenschutzrichtlinie[97], das im österreichischen Datenschutz als „Verwenden von Daten" umgesetzt wurde[98].

Absatz 3 des § 102 TKG hält ausdrücklich fest, dass die Ermittlung und Verwendung von Standortdaten, die nicht im Zusammenhang mit einem Kommunikationsvorgang stehen, zu Auskunftszwecken unzulässig ist, und soll auch hiermit klar die Ermittlung und Speicherung von Bewegungsprofilen verbieten. Auch im Rahmen der Vorratsdatenspeicherpflicht sollten diese Standortdaten nicht erfasst werden[99].

Auch wenn § 102 TKG nicht ausdrücklich regelt, dass diese Standortdaten nach Erbringung des Dienstes mit Zusatznutzen unverzüglich zu löschen sind, ergibt sich das

---

[93] Art 9 RL 2002/58/EG.
[94] DSK 15.04.2011, K121.659/0007-DSK/2011; DSK 03.08.2012, K121.819/0019-DSK/2012.
[95] § 4 Z 9 DSG.
[96] *Graf,* Datenschutzrecht im Überblick² (2010) 39.
[97] Art 2 lit b RL 95/46/EG.
[98] *Kassai*, "Location Based Services" im Gefüge des Datenschutzrechts, MR 2004, 433.
[99] *Stratil* (Hrsg), TKG 2003⁴ ErläutRV 11 zu § 102 Abs 3 (2013).

sowohl aus der Tatsache, dass diese Daten zu keinem anderen Zweck verwendet werden dürfen, und somit auch danach nicht gespeichert werden dürfen, als auch *per analogiam* zur Löschungspflicht, die für Verkehrsdaten vorgesehen ist[100]. Schließlich dürfen wegen des datenschutzrechtlichen Grundsatzes in § 6 Abs 1 Z 5 DSG ohnedies Daten nur solange in personenbezogener Form aufbewahrt werden, als dies zur Erreichung des Verwendungszwecks notwendig ist[101].

7. Zustimmung

Jede Person hat einen Anspruch auf Geheimhaltung ihrer Daten, kann aber in Ausübung ihres informationellen Selbstbestimmungsrechts durch Zustimmung ihren Geheimhaltungsanspruch aufheben[102].

Festzuhalten ist, dass in den Datenschutzbestimmungen des TKG neben dem Begriff der Zustimmung auch der der Einwilligung gebraucht wird, wobei diese Begriffe als Synonyme verwendet werden[103]. Unterschiedliche Begriffe verwendet das TKG auch bei der Person, die einer Datenverwendung, die nicht der Bereitstellung des Kommunikationsdienstes dient, zustimmen soll. Die allgemeine Bestimmung des § 96 TKG setzt für die Verwendung der Stamm-, Verkehrs-, Standort- und Inhaltsdaten zum Zweck der Vermarktung von Kommunikationsdiensten oder der Bereitstellung von Diensten mit Zusatznutzen sowie für sonstige Übermittlungen eine jederzeit widerrufbare Zustimmung der Betroffenen voraus. Wer „Betroffener" ist, wird im TKG nicht definiert. Gemäß der Begriffsbestimmung des DSG ist „Betroffener" jede vom Auftraggeber verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden[104].

Gemäß der Bestimmung über die Verarbeitung von Verkehrsdaten in § 99 Abs 4 TKG muss *der Teilnehmer* einer Verwendung der Daten zum Zwecke der Vermarktung von

---

[100] *Pfarl*, Datenschutz bei LBS im Mobilfunkbereich und im europäischen Notrufsystem <www.it-law.at/uploads/tx_publications/Datenschutz_bei_LBS.pdf>.
[101] *Knyrim*, Datenschutzrecht: Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm (2012) 81.
[102] *Pollirer/Weiss/Knyrim*, DSG² § 1 Anm 6 (2014).
[103] *Kassai*, "Location Based Services" im Gefüge des Datenschutzrechts, MR 2004, 433.
[104] § 4 Z 3 DSG.

Telekommunikationsdiensten des Anbieters oder zum Zwecke der Bereitstellung von Diensten mit Zusatznutzen zustimmen. „Teilnehmer“ ist im Sinne des TKG *eine natürliche oder juristische Person, die mit einem Betreiber einen Vertrag über die Bereitstellung eines Kommunikationsdienstes geschlossen hat*[105].

§ 102 TKG verlangt die Einwilligung *der Benutzer oder Teilnehmer* zur Verwendung von anderen Standortdaten als Verkehrsdaten. Demnach kann auch jene natürliche Person der Datenverwendung zustimmen, die den öffentlichen Kommunikationsdienst nur nutzt, ohne diesen zwangsläufig abonniert zu haben[106]. Ob die Einwilligung vom Benutzer oder vom Teilnehmer abzugeben ist, hängt von den zu verwendenden Daten und dem Zusatzdienst ab, sowie von der Frage, ob es technisch und vertraglich überhaupt möglich ist, zwischen der einen Kommunikationsdienst in Anspruch nehmenden Person und der an diesem Dienst teilnehmenden zu unterscheiden[107]. Die Einwilligung wird meistens durch die Inanspruchnahme des Dienstes gegeben, was den Vorteil hat, dass die Zustimmung zur Datenverwendung nur für die gewünschte Informationsanforderung gegeben wird. Allerdings könnte der Benutzer durch die Inanspruchnahme des Dienstes der Verwendung der Daten des Teilnehmers zustimmen. Dieser Datenverwendung stimmt aber der Teilnehmer zu, wenn er sein Mobiltelefon einem anderen überlässt.

Die Datenschutzrichtlinie für elektronische Kommunikation schreibt in Art 6 Abs 3 vor, dass *der Teilnehmer oder der Nutzer*, *auf den sich die Daten beziehen,* der Verwendung von Verkehrsdaten zum Zwecke der Vermarktung elektronischer Kommunikationsdienste oder zur Bereitstellung von Diensten mit Zusatznutzen, zustimmen muss. Wie bereits oben ausgeführt, sieht § 99 Abs 4 TKG die alternative Zustimmung des Nutzers zur Verarbeitung der Verkehrsdaten nicht vor und entspricht daher nicht der Richtlinie[108]. „Nutzer“ wird im TKG als Überbegriff verwendet und umfasst gemäß § 3 Z 14 TKG *eine natürliche oder juristische Person, die einen öffentlich zugänglichen Kommunikationsdienst in Anspruch nimmt oder beantragt.* Die spezielle Bestimmung über die Verwendung von Verkehrsdaten

---

[105] § 3 Z 19 TKG.
[106] § 92 Abs 3 Z 2 TKG.
[107] ErwGr 31 RL 2002/58/EG.
[108] *Kassai,* "Location Based Services" im Gefüge des Datenschutzrechts, MR 2004, 433.

sieht also nur die Zustimmung des Vertragspartners vor, aber der allgemeine § 96 TKG verlangt die Zustimmung der Betroffenen für die Verwendung der Daten zum Zweck der Vermarktung von Kommunikationsdiensten oder der Bereitstellung von Diensten mit Zusatznutzen vor und hält somit fest, dass die Zustimmung jener Person notwendig ist, deren Daten verwendet werden.

§ 96 TKG und die spezielleren Normen der §§ 99 und 102 TKG unterscheiden sich auch hinsichtlich des zuzustimmenden Zwecks der Datenverwendung. Während gemäß § 96 Abs 2 TKG die Zustimmung der Betroffenen für die Datenverwendung zum Zweck der Vermarktung von Kommunikationsdiensten, zum Zwecke der Bereitstellung von Diensten mit Zusatznutzen sowie für sonstige Übermittlungen erforderlich ist, erwähnt § 99 TKG die Zustimmung hinsichtlich der Verwendung von Verkehrsdaten für sonstige Übermittlungen nicht und § 102 TKG sieht überhaupt nur die Zustimmung zur Verarbeitung für die Bereitstellung von Diensten mit Zusatznutzen vor. Dies darf aber nicht dahin gehend ausgelegt werden, dass keiner anderen Datenverwendung ausdrücklich zugestimmt werden kann als der gesetzlich erwähnten. Diese Auslegung würde dem generellen Datenschutzrecht widersprechen, das mit ausdrücklicher Zustimmung einen zulässigen Eingriff in das Grundrecht auf Datenschutz vorsieht.

Vielmehr soll hier klar zum Ausdruck gebracht werden, dass der Anbieter die Zustimmung zur Verwendung der Daten der Teilnehmer zu anderen Zwecken als zur Erbringung des Kommunikationsdienstes nicht „erzwingen“ darf, was auch der „Zustimmung“ im Sinne des § 4 Z 14 DSG widersprechen würde[109]. Es wird ausdrücklich festgehalten, dass der Betreiber nicht die Erbringung des Telekommunikationsdienstes von der Zustimmung zur Verwendung der Daten zum Zweck der Vermarktung elektronischer Kommunikationsdienste oder zur Bereitstellung von Diensten mit Zusatznutzen abhängig machen darf[110], wodurch das datenschutzrechtliche Koppelungsverbot normiert und die jederzeitige Widerrufbarkeit der Zustimmung zur Datenverwendung sichergestellt wird.

---

[109] *Jahnel/Siegwart/Fercher* (Hrsg.), Aktuelle Fragen des Datenschutzrechts (2007) 200ff; *Pollirer/Weiss/Knyrim*, DSG² § 4 Anm 14 (2014).
[110] *Stratil* (Hrsg), TKG 2003[4] § 96 Anm 5 (2013).

Die Zustimmung muss auf der Grundlage von klaren und umfassenden Informationen getroffen werden können. Die Information muss auch den Hinweis auf das Recht beinhalten, dass die Zustimmung jederzeit widerrufen werden kann[111]. Art 7 lit a der Datenschutzrichtlinie enthält das Erfordernis, dass der Betroffene *ohne jeden Zweifel* die Einwilligung abzugeben hat. Eine bestimmte Form, in der diese Information zu erteilen ist, ist dabei nicht vorgesehen. Die Einwilligung sollte nur in einer Weise gegeben werden, die eben geeignet ist darzulegen, dass diese sachkundig und in freier Entscheidung erfolgt ist. Dies könnte im Bereich der elektronischen Kommunikation zum Beispiel durch Markieren eines hierfür vorgesehenen Feldes erfolgen[112].

Eine im Rahmen der Annahme der allgemeinen Geschäftsbedingungen erfolgende Zustimmung wird insofern nicht ausreichend sein, als die Zustimmung freiwillig sein muss, und die Betreiber die Bereitstellung der Dienste nicht von einer solchen Zustimmung abhängig machen dürfen[113], welche sich des Weiteren ausdrücklich auf einen konkreten Sachverhalt beziehen muss. Die Datenschutzbehörde hält grundsätzlich die Einbindung datenschutzrechtlicher Zustimmungserklärungen in AGB als unzulässig[114]. Die Artikel 29 – Datenschutzgruppe gibt hinsichtlich der Verwendung von Standortdaten klar vor, dass dieser nicht durch Allgemeine Geschäftsbedingungen zugestimmt werden kann[115].

Die Zustimmung muss sich auf eine konkrete Verwendung beziehen, über die der Betroffene informiert sein muss, da er nur *in Kenntnis der Sachlage für den konkreten Fall* wirksam zustimmen kann[116]. Auch im Sinne der allgemeinen Informationspflichten des TKG

---

[111] OGH 22.04.2010, 2 Ob 1/09z = SZ 2010/41 = jusIT 2010/90, 188 (Thiele).
[112] ErwGr 17 RL 2002/58/EG.
[113] § 96 Abs 2 TKG.
[114] Empfehlung der Datenschutzkommission DSK 13.07.2012, K212.766/0010-DSK/2012; In dieser Empfehlung verweist die Datenschutzbehörde (damals Datenschutzkommission) auf das Rundschreiben des BKA-VD, 810.008/1-V/1a/85 vom 10. August 1985 (zur gleich gelagerten alten Rechtslage), dass eine ausdrückliche Zustimmung des Betroffenen keinesfalls dann vorliegen kann, wenn sie bloß als Bestandteil von Allgemeinen Geschäftsbedingungen vom Betroffenen zur Kenntnis genommen wurde. Damit eine schriftliche Zustimmung ausdrücklich gegeben wird, muss der Betroffene sein Einverständnis zur Datenübermittlung getrennt von etwaigen sonstigen vertraglichen Vereinbarungen geben.
[115] *Art-29-Datenschutzgruppe*, Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten, WP 185, 881/11/DE, < www.cnpd.public.lu/de/publications/groupe-art29/wp185_de.pdf>.
[116] § 4 Z 14 DSG; vgl OGH 27.01.1999, 7 Ob 170/98w.

hat der Anbieter den Teilnehmer darüber zu informieren, welche personenbezogenen Daten verarbeitet werden, auf welcher Rechtsgrundlage und für welchen Zweck dies erfolgt sowie über die Dauer der Speicherung der Daten. Ebenso hat der Anbieter zu informieren, ob die Daten zum Zwecke der Bereitstellung des Zusatzdienstes an einen Dritten weitergegeben werden und bejahendenfalls an wen. Wenn nicht ausdrücklich erwähnt, dürfen Daten nicht an einen kooperierenden Provider zur Vermarktung von Kombinationsangeboten übermittelt werden. Die Zustimmung bezieht sich im Zweifel nur auf Kommunikationsdienste, die vom selben Mobilfunkbetreiber angeboten werden[117].

Der Zweck der Verwendung muss hinreichend bestimmt sein und definiert damit Maßstab und Grenze der Datenverwendung, welche auch auf den dafür erforderlichen Zeitraum zu beschränken ist. Je größer die Tragweite der Erklärung für die Rechte und Freiheiten der betroffenen Person, desto bestimmter soll die Information über die Verwendung sein. Eine Erhebung von Daten für einen allfälligen Bedarf ist also unzulässig, da nur einer konkreten, genau festgelegten Verwendung zugestimmt werden kann. Die Datenverwendung muss möglichst sparsam und transparent erfolgen[118]. Die Artikel 29 – Datenschutzgruppe empfiehlt, den Anwendungsbereich der Einwilligung zeitlich zu begrenzen und die Nutzer diesbezüglich zu erinnern. Da die Zustimmung in Kenntnis der Sachlage für den konkreten Fall abzugeben ist, erfolgt bei Diensten mit Zusatznutzen die Zustimmung oder Einwilligung meistens durch die tatsächliche Inanspruchnahme des Zusatzdienstes. Damit kann sichergestellt werden, dass nur konkret dieser Verwendung zugestimmt wird. Allerdings kann dadurch, wie bereits erwähnt, nicht gewährleistet werden, dass tatsächlich derjenige zustimmt, auf den sich die Daten beziehen.

Zusammenfassend können Verkehrs- und Standortdaten mit ausdrücklicher Zustimmung der Teilnehmer (und der Betroffenen) zur Erstellung von Bewegungsströmen erfasst werden, wenn sichergestellt ist, dass die Zustimmung nicht in Abhängigkeit von der Erbringung des Kommunikationsdienstes eingeholt wird. Die Zustimmung muss also ohne Zwang abgegeben werden und jederzeit einfach und kostenlos widerrufbar sein. Durch die

---

[117] *Stratil* (Hrsg), TKG 2003[4] § 96 Anm 2 (2013); *Jahnel/Siegwart/Fercher* (Hrsg.), Aktuelle Fragen des Datenschutzrechts (2007) 204.

[118] *Kassai,* "Location Based Services" im Gefüge des Datenschutzrechts, MR 2004, 433.

Annahme Allgemeiner Geschäftsbedingungen kann der Verwendung ortsbezogener Daten zu anderen Zwecken als der Erbringung des Kommunikationsdienstes nicht ausdrücklich zugestimmt werden. Ein Mobilfunkbetreiber, der die Mobilfunkdaten seiner Kunden zur Erstellung von Bewegungsströmen verwenden möchte, muss daher eine ausdrückliche Zustimmung der Teilnehmer einholen und ihnen dabei auch eine einfache und kostenlose jederzeitige Widerrufbarkeit ermöglichen.

8. Besondere Verwendung zu Forschungszwecken

Grundsätzlich dürfen Daten nur zu einem festgelegten, eindeutigen und rechtmäßigen Zweck ermittelt werden. Einmal gesammelte Daten dürfen zu keinem anderen Zweck verwendet werden, als für den sie gesammelt wurden. Das allgemeine Datenschutzrecht sieht aber in § 46 DSG Ausnahmen von diesem Zweckbindungsgrundsatz vor für die Weiterverwendung zu wissenschaftlichen oder statistischen Zwecken. In diesen Fällen stellt die Verarbeitung personenbezogener Daten keinen unzulässigen Eingriff in schutzwürdige Geheimhaltungsinteressen des Betroffenen dar[119].

Die allgemeine Datenschutzrichtlinie erkennt eine besondere, privilegierende Stellung von wissenschaftlicher Forschung bei der Verwendung von Daten als sachlich gerechtfertigt an, da nicht ein zu strenger Datenschutz die Wissenschaft und Forschung bremsen soll. Gleichzeitig wird aber auch die Pflicht normiert, auch zu wissenschaftlichen oder statistischen Zwecken, möglichst mit anonymen Daten zu arbeiten.

Die Erlaubnistatbestände des § 46 Abs 1 DSG gelten nur, wenn kein personenbezogenes Ergebnis mit dem konkreten Forschungsprojekt angestrebt wird. Für alle anderen Fälle, die auf personenbezogene Ergebnisse zielen oder keine konkrete Untersuchung darstellen, bedarf es der ausdrücklichen Zustimmung des Betroffenen oder der Genehmigung der Datenschutzbehörde, die die Weiterverwendung der Daten bei überwiegendem öffentlichen Interesse an dieser Verwendung erteilt[120]. Das TKG sieht keine eigenen Bestimmungen zur

[119] *Suda,* Datenverwendung für wissenschaftliche Forschung und Statistik, in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 303.

[120] *Pollirer/Weiss/Knyrim,* DSG² § 46 (2014); *Feiler/Fina*, Datenschutzrechtliche Schranken für Big Data, MR 2013, 303.

Datenverwendung zu Forschungszwecken vor, so dass diesbezüglich das DSG anzuwenden ist.

Die Verarbeitung ortsbezogener Verkehrsdaten für Zwecke der wissenschaftlichen Forschung oder Statistik ist damit privilegiert im Sinne des § 46 Abs 1 DSG, wenn sie kein personenbezogenes Ergebnis zum Ziel hat, und diese Daten für den Auftraggeber der Untersuchung entweder öffentlich zugänglich sind, oder er sie für andere Zwecke zulässigerweise ermittelt hat, oder sie für den Auftraggeber nur indirekt personenbezogen sind[121].

Da Verkehrsdaten nicht öffentlich zugänglich sein dürfen, kommt der erste Erlaubnistatbestand nicht zur Anwendung. Der Mobilfunkanbieter könnte aber die ortsbezogenen Daten, die er zulässigerweise ermittelt hat, zur Erstellung von Bewegungsströmen zu Forschungszwecken verwenden, wenn er auch der Auftraggeber der Untersuchung wäre; andernfalls müssten die Verkehrsdaten in (zumindest) indirekt personenbezogener Form zunächst dem Auftraggeber der Untersuchung übermittelt werden.

Allerdings wird vom Begriff der Untersuchung nur eine punktuelle Auswertung bestehender Datenbestände für andere Zwecke umfasst, nicht hingegen die permanente Überführung eines personenbezogenen Datenbestandes. Ist eine zeitliche Begrenzung nicht möglich, könnte schon aus diesem Grund das Erfassen der Verkehrsdaten zur Bildung von Bewegungsströmen, auch wenn diese zu wissenschaftlichen oder statistischen Zwecken verwendet würden, nicht unter diesen ersten Fall der privilegierten Weiterverwendung fallen. Eine solche Weiterverwendung müsste daher von der Datenschutzbehörde genehmigt werden. Dafür müsste im Einzelfall überwiegendes öffentliches Interesse an der Verwendung der Verkehrsdaten für die Erstellung von Bewegungsströmen vorliegen[122].

Die Verarbeitung ortsbezogener Mobilfunkdaten kann daher nur unter den genannten Voraussetzungen privilegiert sein gemäß § 46 DSG. Auf das Produkt Smart Steps findet § 46 DSG jedenfalls keine Anwendung, da im Rahmen von Smart Steps den Kunden die

---

[121] *Graf*, Datenschutzrecht im Überblick² (2010) 73.
[122] *Feiler/Fina*, Datenschutzrechtliche Schranken für Big Data, MR 2013, 303 (304).

Verkehrsdaten angeboten werden, unabhängig davon, ob diese für ein konkretes Forschungsprojekt verwendet werden sollen oder nicht.

9. Zulässigkeit der Verarbeitung von Verkehrsdaten

Bei den Daten, die Telefónica zur Erstellung von Bewegungsströmen verarbeitet, handelt es sich um Verkehrsdaten iSd § 92 Abs 3 Z 4, da diese Daten zum Zweck der Weiterleitung einer Nachricht an ein Kommunikationsnetz erfasst werden. Sowohl gemäß der allgemeinen sektorspezifischen Datenschutzbestimmung des § 96 TKG als auch der spezielleren Norm des § 99 TKG darf der Anbieter die ortsbezogenen Daten seiner Mobilfunkkunden nur für Zwecke der Besorgung eines Kommunikationsdienstes verwenden. Eine Verwendung der Verkehrsdaten zu einem anderen Zweck darf nur aufgrund einer ausdrücklichen, jederzeit widerrufbaren Zustimmung der Kunden erfolgen. Werden nun die Verkehrsdaten zur Erstellung der Bewegungsströme ohne Zustimmung übermittelt oder länger als gesetzlich vorgesehen gespeichert oder mit anderen Daten verknüpft, liegt eine Weiterverarbeitung der Daten vor, die mit dem ursprünglichen Zweck nicht vereinbar ist, und daher nicht erlaubt ist. Verkehrsdaten sind unverzüglich nach Beendigung der Verbindung zu löschen oder anonymisieren. Werden Verkehrsdaten zunächst durch weitere Informationen angereichert und erst in Folge anonymisiert, liegt bereits eine unzulässige Datenverarbeitung vor.

IV. PERSONENBEZOGENE DATEN

§ 96 TKG schränkt die Verwendung von Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten ein, ohne dabei ausdrücklich anzuführen, dass es sich hierbei um personenbezogene Daten handelt. Ebenso wenig geben die Begriffsbestimmungen von Verkehrs- und Standortdaten, sowie die näheren Ausführungen der §§ 99 und 102 TKG wieder, dass es sich um personenbezogene Daten handelt. Nur zu Beginn des 12. Abschnitts des TKG wird explizit angeführt, dass die Bestimmungen dieses Abschnitts für die Verarbeitung und Übermittlung von personenbezogenen Daten in Verbindung mit der Bereitstellung öffentlicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen gelten sollen[123]. Grundsätzlich ergibt sich allerdings schon aus dem Grundrecht auf Datenschutz in § 1 DSG, dass jedermann ein Recht auf Geheimhaltung seiner personenbezogenen Daten hat und diese nicht uneingeschränkt ermittelt oder weiter gegeben werden sollen[124]. Auch die bereichsspezifischen Datenschutzbestimmungen des TKG schränken daher ebenso wie das allgemeine Datenschutzrecht nur die Verwendung personenbezogener Daten ein.

Der Begriff der „personenbezogenen Daten" wird in § 4 Z 1 DSG definiert, wonach es sich bei „personenbezogenen Daten" um Angaben über Betroffene handelt, deren Identität bestimmt oder bestimmbar ist, während bei „nur indirekt personenbezogenen" Daten der Personenbezug derart ist, dass für einen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmt werden kann.

Gemäß Art 2 lit a der allgemeinen Datenschutzrichtlinie sind personenbezogene Daten *alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind*. Während die Richtlinie

[123] § 92 Abs 1 S 1 TKG.
[124] *Graf*, Datenschutzrecht im Überblick² (2010) 34.

nur natürlichen Personen Schutz bei der Verarbeitung ihrer personenbezogenen Daten gewährt, gewährt das österreichische Datenschutzrecht sowohl natürlichen als auch juristischen Personen diesen Schutz[125].

Im Erwägungsgrund 26 der allgemeinen Datenschutzrichtlinie wird festgehalten, dass die Schutzprinzipien für alle Informationen über eine bestimmte oder bestimmbare Person keine Anwendung finden, wenn sie derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist. Kann aus den Daten die Identität des Betroffenen nicht mehr festgestellt werden, fehlt den Daten datenschutzrechtliche Relevanz[126]. Ob ein Personenbezug vorliegt oder nicht, ist daher ausschlaggebend für die Anwendbarkeit datenschutzrechtlicher Normen. Damit eine Datenverarbeitung keinen Einschränkungen unterliegt, muss ausgeschlossen sein, dass diese Daten personenbezogen sind, was jedoch nicht immer klar feststellbar ist.

A. DEFINITION PERSONENBEZOGENE DATEN

Da die Definition des Begriffs der „personenbezogenen Daten“ im Einzelfall zu gewissen Unsicherheiten führen kann, hat die Artikel 29 - Datenschutzgruppe in ihrer Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ versucht, eine gemeinsame Verständnisgrundlage zu schaffen[127]. Die Datenschutzrichtlinie verfolgt das Ziel, in den Mitgliedstaaten sicherzustellen, dass die Schutzprinzipien für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Nach der Art 29 - Datenschutzgruppe sind „Informationen“ über eine betroffene Person alle Arten von Aussagen über eine Person, sowohl objektive Informationen, als auch subjektive Informationen, wie etwa die Meinung

[125] *Kotschy*, Das Grundrecht auf Geheimhaltung personenbezogener Daten. Rückblick und Ausblick (Teil I: § 1 Abs.1 DSG (1978) bzw. DSG 2000), in Jahnel (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2012 (2012) 27 (31).
[126] *Pollirer/Weiss/Knyrim*, DSG² § 1 Anm 8 (2014).
[127] *Art-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, 01248/07/DE, <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf>.

einer bestimmten Person[128]. Der Begriff der „Informationen“ ist weit auszulegen, unabhängig von der Art, dem Inhalt oder der Form der Information.

Weiters muss es sich um Informationen „über“ eine bestimmte oder bestimmbare Person handeln. Die Daten müssen sich daher auf eine Person beziehen. Auch das ist nicht immer so eindeutig: Die Standortdaten eines Mobiltelefons z.B. beziehen sich eigentlich nur auf das Endgerät selbst. Aufgrund der üblichen räumlichen Nähe des Mobiltelefons zum Teilnehmer, können aus den ortsbezogenen Daten der Mobiltelefone Informationen über ihre Teilnehmer gewonnen werden. Dabei kann es sich sogar um sehr persönliche Details aus dem Privatleben der Teilnehmer handeln. Lassen Daten auf die Interessen und Gewohnheiten einer bestimmten Person schließen, so sind sie als personenbezogen anzusehen.

Bei der Entscheidung, ob eine Person bestimmbar ist, sind alle Mittel zu berücksichtigen, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen[129].

Eine Person wird grundsätzlich anhand spezifischer „Kennzeichen“ direkt oder indirekt bestimmt. Als ein direktes Kennzeichen gilt beispielsweise der Name einer Person, während indirekte Kennzeichen meistens erst in Kombination eine Person identifizierbar machen. Dabei kommt es aber immer auf die Umstände im Einzelfall an. In einer Gruppe weniger Personen kann selbst ein einzelnes Kennzeichen genügen, damit eine Person bestimmbar wird. Es ist daher nicht immer der Name einer Person notwendig, um diese zu identifizieren, auch andere Kennzeichen können eine Person in einer Gruppe singularisieren und somit bestimmbar machen. Eine Handlung, durch die eine Person - auf welche Art auch immer - erkennbar gemacht wird, stellt eine Verarbeitung personenbezogener Daten dar[130].

---

[128] *Art-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, 01248/07/DE, <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf>; *Forgó/Krügel*, Der Personenbezug von Geodaten, MMR 1/2010, 20.

[129] *Forgó/Krügel*, Der Personenbezug von Geodaten, MMR 1/2010, 19.

[130] EuGH 6.11.2003, C-101/01 (Lindqvist) Rz 27; EuGH hielt fest, *dass die Handlung, die darin besteht, auf einer Internetseite auf verschiedene Personen hinzuweisen und diese entweder durch ihren Namen oder auf andere Weise, etwa durch Angabe ihrer Telefonnummer oder durch Informationen über ihr Arbeitsverhältnis oder ihre Freizeitbeschäftigungen, erkennbar zu machen, eine […] Verarbeitung personenbezogener Daten im Sinne von […] Richtlinie 95/46/EG darstellt*.

Gemäß Erwägungsgrund 26 der Datenschutzrichtlinie sind bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel zu berücksichtigen, die vernünftigerweise von einem Dritten zur Identifizierung einer Person eingesetzt werden könnten. Auch diese Mittel sind dem für die Verarbeitung Verantwortlichen zuzurechnen. Ob Daten für einen Dritten personenbezogen, also auf eine bestimmte Person rückführbar sind, hängt vom Kenntnisstand des jeweiligen Dritten ab. Die Datenschutzbehörde führt dazu aus, dass naturgemäß der Wissensstand der Empfänger übermittelter Daten äußerst unterschiedlich sein kann; die verantwortliche Stelle muss von einem durchschnittlich zu erwartenden Informationsstand jenes Empfängerkreises ausgehen, in dem die Information verwendet werden soll. Mittel, auf die ein Dritter legal zugreifen kann und auf die er mit vertretbarem Aufwand zugreifen könnte, hat die verantwortliche Stelle auf jeden Fall zu berücksichtigen. Nicht zu berücksichtigen ist dabei der Informationsstand von Personen, die aus einem besonderen Grund Sonderwissen über den Betroffenen haben[131].

Bei der Beurteilung, welche Mittel vernünftigerweise eingesetzt werden könnten, ist sowohl auf die Kosten der Identifizierung abzustellen, als auch auf den beabsichtigten Zweck, auf die Strukturierung der Verarbeitung, den dadurch erwarteten Vorteil, sowie die auf dem Spiel stehenden Interessen. Dabei ist zu berücksichtigen, dass sich diese Umstände ändern können. Es muss im Einzelfall geprüft werden, ob es nach jeweils aktuellem Standpunkt Mittel gibt, die vernünftigerweise zur Bestimmbarkeit einzelner Personen eingesetzt werden könnten, und ob dies während des Zeitraums der Verfügbarkeit dieser Daten zu erwarten ist. Nur wenn dies ausgeschlossen werden kann, sind die jeweiligen Daten nicht als „personenbezogen“ anzusehen und die Verarbeitung solcher Daten ist somit datenschutzrechtlich nicht relevant.

Der Begriff „personenbezogene Daten“ ist zwar gewollt sehr weit gefasst, aber gleichzeitig wird versucht, den Anwendungsbereich der Datenschutzbestimmungen einzuschränken, damit nicht jede Datenverwendung datenschutzrechtlichen Schranken unterliegt. In gewissen Fällen führen diese zu einer unnötigen Erschwerung der Daten-

[131] DSK 22. 4. 2005, K120.966/0005-DSK/2005; vgl *Haidinger*, Was sind personenbezogene Daten?, Dako 2014/7, 17.

verwendung, was wiederum anderen berechtigten Interessen entgegenstehen könnte[132]. Es ist stets zu berücksichtigen, dass datenschutzrechtliche Regelungen für Situationen einzusetzen sind, in denen die Rechte von Personen bedroht sein könnten und folglich geschützt werden müssen[133].

Es werden ausdrücklich Ausnahmen von der Anwendbarkeit des Datenschutzes in Artikel 3 Abs 2 der Datenschutzrichtlinie vorgesehen, wie beispielsweise hinsichtlich der Verarbeitung personenbezogener Daten als rein familiäre Tätigkeit; die Verarbeitung von Verkehrs- und Standortdaten zur Erfassung von Bewegungsströmen fällt aber unter keine dieser Ausnahmen.

B. DIREKT UND INDIREKT PERSONENBEZOGENE DATEN

Das österreichische Datenschutzgesetz unterscheidet zwischen „direkt personenbezogenen" und nur „indirekt personenbezogenen" Daten. Direkt personenbezogene Daten sind Angaben über eine bestimmte oder bestimmbare Person. Gemäß der Richtlinie liegen personenbezogene Daten bereits vor, wenn sie auch nur künftig durch einen Dritten einer bestimmten Person zugeordnet werden können. Die österreichischen Bestimmungen sehen eine Erleichterung bei der Verwendung von Daten vor, bei denen der Personenbezug derart ist, dass der konkrete Verwender die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann[134]. Für einen Verwender, der auch über alle Kennnummern dieser Daten verfügt, sind diese Daten personenbezogen, während sie dies für einen anderen konkreten Verwender nicht sind[135]. Die Verwendung indirekt personenbezogener Daten unterliegt daher datenschutzrechtlichen Bestimmungen, allerdings werden hierfür nicht so

---

[132] *Kotschy,* Das Grundrecht auf Geheimhaltung personenbezogener Daten. Rückblick und Ausblick (Teil I: § 1 Abs.1 DSG (1978) bzw. DSG 2000), in Jahnel (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2012 (2012) 27 (56).

[133] *Art-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 01248/07/DE, <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf>.

[134] §4 Z 1 DSG; *Kotschy*, Das Grundrecht auf Geheimhaltung personenbezogener Daten. Rückblick und Ausblick (Teil I: § 1 Abs.1 DSG (1978) bzw. DSG 2000), in Jahnel (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2012 (2012) 27 (54).

[135] *Kotschy*, Das Grundrecht auf Geheimhaltung, Jahrbuch Datenschutzrecht und E-Government 2012, 27 (53).

strenge Regelungen vorgesehen[136], da die schutzwürdigen Geheimhaltungsinteressen bei der Verwendung dieser Daten als nicht verletzt gelten [137].

Solche „indirekt personenbezogene Daten“ werden auch oft als „pseudonymisierte Daten“ bezeichnet. Pseudonymisierte Daten sind verschlüsselte Daten, die sich auf Personen beziehen, die durch einen Code gekennzeichnet sind, während der Schlüssel für die Zuordnung des Codes zu den Personen gesondert aufbewahrt wird. Somit sind Mittel vorhanden, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden können, wodurch die Personen bestimmbar sind. Die Verarbeitung dieser Daten unterliegt daher den Datenschutzbestimmungen, sie sind aber weniger schutzwürdig als direkt personenbezogene Daten. Die Verschlüsselung der Daten erlangt zunehmend an Bedeutung, da diese die Verarbeitung personenbezogener Daten datenschutzrechtlich "erträglich" macht[138].

Sind die Codes hingegen nicht eindeutig oder ist die notwendige Zusatzinformation über die Zuordnung der Codes nicht mehr vorhanden und mit vertretbarem Aufwand auch nicht mehr wiederherzustellen, könnten die Informationen als nicht auf bestimmbare Personen bezogen angesehen werden. Die Datenschutzbestimmungen würden auf die Verarbeitung dieser Daten folglich keine Anwendung finden[139].

C. ANONYMISIERTE DATEN

Das österreichische Datenschutzrecht definiert weder den Begriff anonymer Daten selbst noch den des Anonymisierens. Anonyme Daten liegen daher vor, wenn es sich nicht um personenbezogene Daten handelt. Im deutschen BDSG findet sich unter den Legaldefinitionen in § 3 Abs 6 eine Definition für das Anonymisieren: *Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche*

---

[136] *Souhrada-Kirchmayer*, Das Datenschutzgesetz 2000, SozSi 2000, 938.
[137] § 8 Abs 2 DSG.
[138] *Kotschy*, Das Grundrecht auf Geheimhaltung personenbezogener Daten. Rückblick und Ausblick (Teil I: § 1 Abs.1 DSG (1978) bzw. DSG 2000), in Jahnel (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2012 (2012) 27 (55).
[139] *Art-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, 01248/07/DE, < ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf>.

Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Im Umkehrschluss zu dem zum Begriff des Personenbezugs Ausgeführten muss die Zuordnung zu einer bestimmten Person durch das Anonymisieren nicht schlechthin ausgeschlossen werden, es genügt, dass diese Zuordnung einen unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft erfordert. Sind keine Mittel vorhanden, die an diesen Kriterien gemessen vernünftigerweise eingesetzt werden können, um die betreffende Person zu bestimmen[140], sind die Daten als anonym anzusehen. Der Begriff der „anonymen" Daten ist genauso relativ wie der der „personenbezogenen Daten". Es kann daher nicht immer mit Sicherheit die Anonymität gewisser Daten beurteilt werden. Gerade der schnelle technische Fortschritt macht diese Beurteilung noch unsicherer[141].

Ist grundsätzlich eine Deanonymisierung möglich, sind die Daten nicht anonym, sondern als „personenbezogen" zu behandeln. Es kommt dabei nicht auf die Absicht an, die Daten mit den Identifikationsmerkmalen zusammen zu führen, sondern nur auf die Möglichkeit. Ob und inwieweit der anonymisierenden Stelle Zusatzwissen, das ausschließlich Dritten zur Verfügung steht, zugerechnet werden muss, ist im Einzelfall restriktiv auszulegen, um auch die bestehende Verantwortlichkeit einzugrenzen. In der deutschen Literatur wird vielfach vertreten, dass dem für die Verarbeitung Verantwortlichen nur das Zusatzwissen zugerechnet werden kann, über das er selbst verfügt. Dadurch kann aber kein Datenschutz gewährleistet werden; Die verantwortliche Stelle wäre frei, die für sie anonymen Daten z.B. im Internet zu veröffentlichen, wo es durch die Verknüpfbarkeit mit anderen Datenbanken für viele Personen leicht möglich wäre, einen Personenbezug herzustellen. Diesen Umstand hat der für die Datenverwendung Verantwortliche zu berücksichtigen[142].

---

[140] ErwGr 26 RL 95/46/EG.
[141] *Simitis*, Bundesdatenschutzgesetz § 3 RZ 196 (2014).
[142] *Simitis*, Bundesdatenschutzgesetz § 3 RZ 211 (2014).

Das European Privacy Officers Forum (EPOF)[143] hebt die Einschränkung auf vernünftige Mittel, die zur Identifizierung eingesetzt werden könnten, besonders hervor[144]. Diese Einschränkung werde oft überlesen, weswegen das EPOF eine Definition für „anonyme Daten" auch auf europarechtlicher Ebene vorschlägt. Dabei soll die besonders praxisnahe deutsche Definition des „Anonymisierens" als Vorbild dienen. Die Verarbeitung ausreichend anonymer Daten unterliegt nicht dem Datenschutz und bedarf daher auch keiner Zustimmung. Daten sollen, sobald möglich, anonymisiert werden.

In diesem Zusammenhang weist das EPOF auch auf das Problem hin, dass einige Mitgliedstaaten das Anonymisieren selbst als eine Verarbeitung der Daten auslegen, da ja unter „Verarbeitung personenbezogener Daten" jede Art der Handhabung von Daten fällt, somit unter anderem auch das Löschen und Vernichten[145]. Damit müsste auch für das Anonymisieren personenbezogener Daten die Zustimmung des Betroffenen eingeholt werden. Diese Auslegung würde zu weit gehen und gerade das Ziel des Datenschutzes verfehlen, alle personenbezogenen Daten, sobald sie nicht mehr zweckentsprechend gebraucht werden, zu löschen oder anonymisieren. Das „Anonymisieren" sollte daher ausdrücklich vom Begriff der Datenverwendung ausgenommen werden[146].

Die Anonymisierung ist also Voraussetzung für die Weiterverwendung von erfassten Daten, ohne eine zusätzliche Zustimmung der Betroffenen einholen zu müssen. Es gibt verschiedene Methoden der Anonymisierung, von denen meistens mehrere gleichzeitig angewendet werden. Eine Person kann nämlich auch dann bestimmbar sein, wenn alle direkten Identifikationsmerkmale gelöscht sind. Liegen bestimmte Merkmalsausprägungen nur vereinzelt vor, müssen diese entweder gelöscht werden oder durch Merkmalsaggregierung verallgemeinert werden (z.B. „über 65 Jahre"). Dies führt natürlich auch zu einem Informationsverlust. Eine weitere oft zusätzlich verwendete Methode ist das Einbauen von

---

[143] bestehend aus Datenschutzbeauftragten verschiedener multinationaler Unternehmen, gegründet 2001. <www.epof.org>.

[144] *EPOF*, Comments on Review of the EU Data Protection Directive (Directive 95/46/EC), <ec.europa.eu/justice/policies/privacy/docs/lawreport/paper/epof_en.pdf>.

[145] Art 2 lit b RL 95/46/EG.

[146] *EPOF*, Comments on Review of the EU Data Protection Directive (Directive 95/46/EC), <ec.europa.eu/justice/policies/privacy/docs/lawreport/paper/epof_en.pdf>.

„Zufallsfehlern“ in den Datenbestand. Auch dies hat einen gewissen Informationsverlust zur Folge, gewährt aber einen besseren Datenschutz[147].

D. FAZIT

Voraussetzung für die Anwendbarkeit des Datenschutzrechts ist das Vorliegen personenbezogener Daten. Nur wenn Daten weder direkt noch indirekt einer Person zugeordnet werden können, finden weder die besonderen Datenschutzbestimmungen des TKG noch die allgemeinen des DSG Anwendung. Werden daher die Bewegungsströme der Mobiltelefonnutzer ausschließlich aus anonymisierten Daten gebildet, ist ihre Verwendung aus datenschutzrechtlicher Sicht möglich. Es muss sichergestellt sein, dass nicht nur die direkten Identifikationsmerkmale anonymisiert sind, sondern, dass durch die Anonymisierungsverfahren tatsächlich kein Bezug auf einzelne Personen hergestellt werden kann. Auch wenn die Daten eines mobilen Endgerätes so anonymisiert sind, dass der Teilnehmer daraus nicht hervor geht, kann – gerade in dünn besiedelten Gegenden – schon alleine der Standort Aufschluss über die Person geben. Gerade in so einem Fall kann durch Datenaggregierung ein besserer Datenschutz erzielt werden. Darüber hinaus können durch die Kombination verschiedener anonymisierter Datenbestände manchmal mit nur geringem Aufwand einzelne Personen aus diesen bestimmt werden.

Im Rahmen der Studie "Unique in the Crowd" unter der Leitung des MIT (Massachusetts Institute of Technology) konnte gezeigt werden, dass vielfach eine Deanonymisierung möglich ist, und dass damit die Privatsphäre von Handy-Nutzern gefährdet ist. Im Rahmen dieser Studie des MIT wurden die vom Netzbetreiber anonymisiert zur Verfügung gestellten Bewegungsdaten von 1,5 Millionen Nutzern ausgewertet. Mithilfe von komplexen statistischen Analysen war es möglich, einzelne Personen aus der Datenmenge eindeutig zu identifizieren. Zusammenfassend wurde festgestellt, dass 95 Prozent der Nutzer eindeutig identifiziert werden konnten aufgrund von lediglich vier mit Ort und Zeit

[147] *Simitis*, Bundesdatenschutzgesetz § 3 RZ 205ff (2014).

versehenen Datenpunkten. "Unique in the Crowd" veranschaulichte, wie einfach standortbezogene Nutzerdaten zum individuellen Verfolgen Einzelner verwendet werden können[148].

Die Erstellung von Bewegungsströmen mit anonymisierten Mobilfunkdaten ist daher rechtlich gesehen nur möglich, wenn sichergestellt ist, dass eine Identifizierung einzelner Personen aus diesen anonymisierten Bewegungsdaten lediglich mit Mitteln erreicht werden könnte, die mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

[148] *De Montjoye/Hidalgo/Verleysen/Blondel*, Unique in the Crowd: The privacy bounds of human mobility, Scientific Reports³, 2013, 1.

V. ZUSAMMENFASSUNG DER ERGEBNISSE

Allein mit den Verkehrsdaten, die zwangsläufig bei Bereitstellung eines Kommunikationsdienstes anfallen, können Bewegungsprofile erstellt werden, ohne dass dabei auch andere Standortdaten als Verkehrsdaten verarbeitet werden müssten. Der Mobilfunkanbieter erfasst diese Daten, um den öffentlichen Kommunikationsdienst in öffentlichen Kommunikationsnetzen anbieten zu können. Standortbezogene Verkehrsdaten sind jedenfalls personenbezogene Daten, da sie einem bestimmten Teilnehmer zugeordnet werden können. Für die Verarbeitung und Übermittlung dieser personenbezogenen Daten finden die sektorspezifischen Datenschutzbestimmungen des TKG Anwendung. Nur soweit das TKG nicht anderes bestimmt, gelten die Bestimmungen des DSG.

Wie bereits unter „Zulässigkeit der Verarbeitung von Verkehrsdaten“ ab Seite 35 ausgeführt, ist der Mobilfunkanbieter nur berechtigt, Verkehrsdaten für die im TKG abschließend geregelten Fälle zu speichern oder zu übermitteln. Eine Verwendung der Verkehrsdaten zu einem anderen Zweck als der Erbringung des Kommunikationsdienstes bedarf jedenfalls der ausdrücklichen Zustimmung des Teilnehmers, die jederzeit einfach und kostenlos widerrufbar sein muss und nicht Bedingung für die Bereitstellung der Kommunikationsdienste sein darf.

Der Mobilfunkbetreiber müsste eine ausdrückliche Zustimmung jedes einzelnen Teilnehmers für die Verwendung dessen Verkehrsdaten zur Erstellung von Bewegungsströmen einholen und diese auch so verwalten, dass einem möglichen Widerruf eines Betroffenen sofort entsprochen werden kann, was keine praktikable Lösung wäre. Ohne ausdrückliche Zustimmung des Betroffenen hat der Anbieter die Daten nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren[149].

Die Daten sind dabei so zu anonymisieren, dass ein Personenbezug ausgeschlossen ist, eine Rückführbarkeit darf auch für einen Dritten mit Mitteln, die vernünftigerweise zur Identifizierung einer Person eingesetzt werden, nicht mehr möglich sein. Die Verarbeitung

[149] *Stratil* (Hrsg.), TKG 2003[4] ErläutRV 11 zu § 99 Abs 1 (2013).

von nicht personenbezogenen Daten fällt nicht in den Anwendungsbereich des Datenschutzes. Anonymisiert daher der Mobilfunkanbieter die Verkehrsdaten unverzüglich nach Beendigung des Kommunikationsdienstes, können die anonymisierten Bewegungsdaten übermittelt werden. Der für die Verarbeitung Verantwortliche hat aber zu achten, dass auch ohne direkte Identifikationsmerkmale Daten bestimmten Personen zugeordnet werden können. Es reicht somit meist nicht, nur den Namen, die IMSI oder IMEI zu löschen, vielmehr ist zu beachten, dass diese anonymisierten und aggregierten Bewegungsströme auch im Zuge einer späteren Verwendung wieder einen Personenbezug erlangen könnten. Ist durch die Verknüpfung mit anderen Datenbeständen eine Deanonymisierung möglich, dürfen auch anonymisierte Datenströme nicht übermittelt werden. Es muss laufend unter Berücksichtigung der jeweiligen Umstände sichergestellt werden, dass den datenschutzrechtlichen Bestimmungen entsprochen wird. Kann ein Personenbezug ausgeschlossen werden, ist die Datenanwendung zulässig.

In Deutschland wurde die Erhebung von Verkehrs- und Standortdaten für das Produkt „Smart Steps“ heftig kritisiert, da die Verarbeitung von Verkehrs- und Standortdaten für andere Zwecke als die Erbringung des Telekommunikationsdienstes nicht erlaubt ist. Dabei wurde Telefónica insbesondere vorgeworfen, die Bewegungsdaten vor ihrer Anonymisierung mit Bestandsdaten kombiniert zu haben, was datenschutzrechtlich nur mit einer klaren Einwilligung jeder betroffenen Person zu rechtfertigen wäre[150]. Da diese nicht vorlag, war das Vorhaben von Telefónica rechtswidrig[151].

In England ging das Information Commissioner's Office davon aus, dass Telefónica vor einer Anwendung die ortsbezogenen Mobilfunkdaten anonymisiert und aggregiert, und dass nur der aggregierte Bewegungsstrom der Mobilfunkkunden als Ganzes mit anderen Daten aus anderen Quellen kombiniert werde. Unter diesen Voraussetzungen ist die Erstellung eines Bewegungsstromes mittels standortbezogener Mobilfunkdaten zulässig.

---

[150] Auch das deutsche TKG sieht vor, dass Verkehrsdaten über das Ende der Verbindung hinaus nur verwendet werden dürfen, soweit sie zum Aufbau weiterer Verbindungen oder für durch gesetzliche Vorschriften begründete Zwecke erforderlich sind.

[151] *Mantz*, Standortdaten und Bewegungsprofile, K&R, 1/2013, 7.

Das ICO weist auch auf die Gefahr hin, dass in Folge verschiedener Kombinationen vielleicht doch eine bestimmte Person aus dem Bewegungsstrom singularisiert werden könne, dies sollte aber nicht bedeuten, dass eine Anonymisierung kein effektives Mittel darstelle. Unternehmen sollen das Risiko abschätzen und entsprechende Vorkehrungen im Einzelfall treffen, um eine Re-Identifikation unmöglich zu machen[152]. Gemäß dem Vorschlag der europäischen Datenschutzverordnung[153] sollen Unternehmen künftig mehr Eigenverantwortung tragen und geeignete Lösungen finden, die Datenschutzgrundsätze einzuhalten[154]. Im Einklang mit dem Grundsatz der Datenminimierung und Zweckbeschränkung sollen allgemein Daten – nicht nur Verkehrsdaten - gelöscht oder anonymisiert werden, sobald die Notwendigkeit, sie für einen konkreten Zweck zu verwenden, wegfällt.

[152] *Information Commissioner's Office*, Big data and data protection, <ico.org.uk/news/¬latest_news/-2014/~/media/documents/library/Data_Protection/Practical_application/big-data-and-data-protection.pdf>.

[153] Vorschlag für eine Verordnung der Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011-C7-0025/2012-2012/0011(COD)); siehe Kapitel VI.

[154] *Knyrim*, Entwurf der neuen EU-Datenschutz-Grundverordnung, in Scholz/Funk, DGRl Jahrbuch (2012) 30.

VI. AUSBLICK

Seit der Umsetzung der Richtlinie 95/46/EG haben sich verschiedene technische Entwicklungen auf die Anwendbarkeit gewisser geltender datenschutzrechtlicher Bestimmungen ausgewirkt. Die Datenschutzrichtlinie soll daher modernisiert werden. Da die Mitgliedstaaten bei der Umsetzung der Richtlinie einigen Ermessenspielraum hatten und dadurch die angestrebte Vereinheitlichung des Datenschutzes nur bedingt erreicht werden konnte, soll die Richtlinie durch eine Verordnung mit unmittelbarer Anwendbarkeit ersetzt werden. Es soll dadurch ein einheitlicher, hoher und dem Internetzeitalter gerechter Datenschutzstandard in der EU gewährleistet werden.

Die Europäische Kommission hat bereits 2012 einen Vorschlag für eine Datenschutzverordnung vorgelegt. Nach verschiedenen Stellungnahmen zu diesem Vorschlag wurde er vom Europäischen Parlament angenommen. Die Haltung der Mitgliedstaaten gegenüber der Datenschutzgrundverordnung ist nach wie vor uneinheitlich. Während einige der Mitgliedstaaten fürchten ihren hohen Datenschutzstandard zu verschlechtern, kritisieren andere den Vorschlag der EU-Datenschutzgrundverordnung als zu streng.

A. RAHMEN FÜR BIG DATA

Die Datenschutzgrundverordnung soll auch einen einheitlichen Rahmen für Big Data Anwendungen vorgeben; Uneinigkeit herrscht darüber, ob jede Big Data Anwendung, auch wenn ausschließlich anonymisierte Daten verarbeitet werden, dem Datenschutzrecht unterliegen soll, da eine echte Anonymisierung nicht immer gewährleistet werden kann. So ist es möglich, dass durch die Kombination mehrerer Datenprofile die Identität einer Person sehr leicht festgestellt werden kann. Andererseits vertreten gerade Big Data Unternehmen diesen Standpunkt naturgemäß nicht und beharren darauf, dass nicht jede Datenverwendung datenschutzrechtlichen Einschränkungen unterliegen soll. Ein weiteres Argument gegen strenge Datenschutzbestimmungen besteht darin, dass diese die Innovation in Europa bremsen würden, wodurch die europäische Wirtschaft einen Wettbewerbsnachteil erleide.

Die europäische Datenschutzgrundverordnung versucht, sowohl diese Interessen zu berücksichtigen als auch gleichzeitig Datenschutz in einem Big Data Zeitalter zu

gewährleisten, und fordert unter anderem die ausdrückliche Einwilligung der Betroffenen vor Durchführung einer Datenverarbeitung, schreibt Informationspflichten, Transparenz und hohe Sanktionen bei Verletzung der Schutzbestimmungen vor und verwendet zukunftsorientierte Definitionen[155].

1. Ausdrückliche Einwilligung

Der Betroffene muss grundsätzlich einer Verarbeitung und Weitergabe seiner Daten zustimmen. Damit sollen die Möglichkeiten für den Einzelnen verbessert werden, seine Daten zu kontrollieren, allerdings bedeutet dies auch eine Erhöhung des bürokratischen Aufwandes[156].

Gemäß Art 4 Abs 8 des Entwurfs der neuen EU-Datenschutzgrundverordnung[157] muss die Einwilligung ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgen. Die ausdrückliche Willensbekundung ist dabei in Form einer Erklärung oder einer sonstigen eindeutigen Handlung abzugeben. Der Zustimmungsprozess soll sich nach Möglichkeit an standardisierten, leicht verständlichen Symbolen orientieren[158]. Der Widerruf der Einwilligung muss so einfach wie ihre Erteilung sein.

2. Profiling

Unter „Profiling" soll jede Form automatisierter Verarbeitung personenbezogener Daten verstanden werden, die zu dem Zweck vorgenommen wird, bestimmte personenbezogene Aspekte zu bewerten oder insbesondere, um ein Verhalten, bestimmte Vorlieben, den Aufenthaltsort, bestimmte Leistungen oder die wirtschaftliche Situation Betroffener zu

---

[155] *Europagruppe Grüne,* Die europäische Datenschutzgrundverordnung in 10 Punkten < www.gruene-europa.de/die-europaeische-datenschutzgrundverordnung-in-10-punkten-10773.html>.

[156] *Knyrim*, Entwurf der neuen EU-Datenschutz-Grundverordnung, in Scholz/Funk, DGRl Jahrbuch (2012) 25.

[157] Vorschlag für eine Verordnung der Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011-C7-0025/2012-2012/0011(COD)).

[158] *Feiler*, Der Vorschlag der Europäischen Kommission für eine Datenschutz-Grundverordnung der EU, MR-Int, 2011, 127 (128);
Europagruppe Grüne, Die europäische Datenschutzgrundverordnung in 10 Punkten <www.gruene-europa.de/die-europaeische-datenschutzgrundverordnung-in-10-punkten-10773.html>.

analysieren oder vorauszusagen. Dabei spielt aber die Kausalität keine Rolle, es werden nur Korrelationen festgestellt. Wie auch im Erwägungsgrund 58 des Vorschlags der europäischen Datenschutzverordnung festgehalten, soll jede Person das Recht haben, dem Profiling zu widersprechen und über dieses Widerspruchsrecht ist sie auch zu unterrichten. Nicht erlaubt soll eine solche Analyse beziehungsweise Voraussage sein, wenn diese rein automatisiert erfolgt und sich rechtliche Konsequenzen für die betroffene Person ergeben oder maßgeblich ihre Interessen, Rechte oder Freiheiten beeinträchtigt[159].

Die Artikel 29 - Datenschutzgruppe befürwortet die im Entwurf der EU-Datenschutzverordnung enthaltene Bestimmung zum Profiling. Sie bezweifelt jedoch, dass die Bestimmung ausreichend sein wird, den mit der Erstellung und Verwendung von Profilen verbundenen Problemen gerecht zu werden. Es sollte klargestellt werden, dass diese Bestimmung beispielsweise auch das Tracking zur Bewertung des Nutzerverhaltens und das Anlegen von Bewegungsprofilen durch mobile Anwendungen oder die Erstellung von persönlichen Profilen durch soziale Netzwerke betrifft[160].

Bereits die Erzeugung von Profilen sollte geregelt und begrenzt werden. Das Selbstbestimmungsrecht, wie mit persönlichen Daten umgegangen wird, darf nicht mit dem Argument untergehen, dass andernfalls die Vorteile von Big Data Anwendungen nicht erreicht werden könnten; diese gilt es zu erreichen, ohne dass Privatsphäre und Datenschutz beeinträchtigt werden.

3. Folgenabschätzung

Der Rat der Europäischen Union setzt sich für eine Stärkung einer Folgenabschätzung - also einer Risikobewertung - bei der Auferlegung von datenschutzrechtlichen Pflichten ein. Das potentielle Risiko einer Datenverarbeitung vorab festzulegen ist aber gerade im Rahmen von Big Data im Grunde unmöglich.

---

[159] Art. 20 Vorschlag für eine Verordnung der Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011-C7-0025/2012-2012/0011(COD)).

[160] *Art-29–Datenschutzgruppe,* Stellungnahme 01/2012 zu den Reformvorschlägen im Bereich des Datenschutzes, WP 191, 00530/12/DE, <www.cnpd.public.lu/de/publications/groupe-art29/wp191_de.pdf>.

Mit der Auferlegung der Pflicht zur Folgenabschätzung werden die mit der Verarbeitung personenbezogener Daten Verantwortlichen gezwungen, sich über einen höheren Schutz Gedanken zu machen[161].

Der Entwurf der allgemeinen Datenschutzverordnung sieht dabei vor, dass bestimmte Verarbeitungsvorgänge konkrete Risiken beinhalten können, wie beispielsweise die Verarbeitung personenbezogener Daten von mehr als 5000 betroffenen Personen, die Verarbeitung von Standortdaten und Profiling[162]. Bei konkreten Risiken ist eine Datenschutz-Folgenabschätzung vorzunehmen, die sich, wie in Art 33 des Vorschlags der Datenschutzgrundverordnung vorgesehen, auf das gesamte Lebenszyklusmanagement personenbezogener Daten zu beziehen hat, also von der Erhebung über die Verarbeitung bis zur Löschung. Dabei hat eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung in Bezug auf den Zweck zu erfolgen, sowie eine Bewertung auf bestehende Risiken in Bezug auf die Rechte und Freiheiten der Betroffenen. Des Weiteren sind Sicherheitsvorkehrungen, wie zum Beispiel die Pseudonymisierung, zu beschreiben und darzulegen, welche datenschutzfreundlichen Maßnahmen technisch eingesetzt werden. Die Folgenabschätzung muss dokumentiert werden und ein Plan zur Überprüfung der Einhaltung der Datenschutzbestimmungen erstellt werden[163].

Insbesondere zu Big Data Projekten soll eine Folgenabschätzung vorgenommen werden, in der auch die geplanten Verarbeitungsschritte und die geplante Datenverwendung beschrieben wird. Im diesem Zusammenhang kann die Einhaltung datenschutzrechtlicher Bestimmungen nur im jeweiligen Einzelfall für jede einzelne Datenverwendung beurteilt werden. Grundsätzlich lassen sich die Datenschutzprinzipien, die auch in der EU-Datenschutzgrundverordnung zentral gefordert werden, wie unter anderem die

---

[161] *Art-29–Datenschutzgruppe,* Stellungnahme 01/2012 zu den Reformvorschlägen im Bereich des Datenschutzes, WP 191, 00530/12/DE, <www.cnpd.public.lu/de/publications/groupe-art29/wp191_de.pdf>.

[162] Art 32a Vorschlag für eine Verordnung der Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011-C7-0025/2012-2012/0011(COD)).

[163] Art 33a Vorschlag für eine Verordnung der Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011-C7-0025/2012-2012/0011(COD)).

Datensparsamkeit, die Zweckbindung, die ausdrückliche Einwilligung und Interessenabwägung mit Big Data nicht vereinen. Allein schon die Einholung einer Zustimmung jedes Einzelnen unter Berücksichtigung seines jederzeitigen Widerrufsrechts ist aufgrund der vorliegenden riesigen Datenmengen mit Big Data nicht in Einklang zu bringen.

Big Data Anwendungen können daher nur mit Daten vorgenommen werden, die nicht dem Datenschutz unterliegen. Sollen personenbezogene Daten verarbeitet werden, sind diese zu anonymisieren, wobei sicher zu stellen ist, dass auch nach Verarbeitung der Daten diese nicht zu personenbezogenen werden können. Ebenso ist darauf zu achten, dass die Daten, wenn sie zwar selbst nicht personenbezogen sind, aber durch einen nicht erheblich großen Aufwand einzelnen Personen zugeordnet werden können, als personenbezogen anzusehen sind und somit vom Datenschutz erfasst[164].

4. Personenbezogene Daten

Der Entwurf der europäischen Datenschutzverordnung fußt ebenso wie die jetzige Datenschutzrichtlinie auf dem Anknüpfungspunkt der Personenbezogenheit von Daten. Anonymisierte Daten sollen nicht von der Datenschutzgrundverordnung erfasst werden. In diesem Sinne fordern einige Mitgliedstaaten, dass eine klare Definition „anonymisierter Daten“ in die Verordnung aufgenommen werde, was aber der Entwurf nicht vorsieht. Hinsichtlich der Definition „personenbezogene Daten“ hat es mehrere Änderungsvorschläge gegeben, der Entwurf gibt aber die heutige Auffassung des Begriffs wieder. Bei der Beurteilung, ob gewisse Daten personenbezogen sind bzw. ob aus diesen eine Person bestimmbar ist, sind die Mittel zu prüfen, die nach allgemeinem Ermessen aller Voraussicht nach zur Identifizierung oder Herausgreifen einer Person genutzt werden können. „Bestimmbar“ ist gemäß Artikel 4 Abs 2 der vorgeschlagenen Verordnung eine Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer eindeutigen Kennung oder zu einem oder mehreren spezifischen Elementen, die Ausdruck der physischen,

[164] *Dorschel/Nauerth*, Big Data und Datenschutz –ein Überblick über die rechtlichen und technischen Herausforderungen, <www.bartsch-rechtsanwaelte.de/media/docs/JD/Big_Data.pdf>.

physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen, sozialen oder geschlechtlichen Identität dieser Person sind.

Das EPOF fordert eine pragmatische Auslegung des Begriffs „personenbezogene Daten“, der jedenfalls nicht so weit gefasst werden darf, dass eine Anonymisierung unmöglich erscheint. Die verarbeitenden Stellen sollen angehalten werden, die Daten nach ihrer Verwendung zu anonymisieren oder zumindest zu pseudonymisieren oder zu verschlüsseln[165].

In Zeiten von „Big Data“ werden Datensätze zusammengeführt, verknüpft und kombiniert. Da sich ein Personenbezug durch die Auswertung kombinierter anonymisierter Datensätze ebenso wie bei unkritisch erscheinenden Daten als Folge von Änderungen und Entwicklungen technischer Möglichkeiten ergeben kann, soll die europäische Datenschutzverordnung auch diese Gefahren berücksichtigen.

Damit stellt sich die Frage, ob datenschutzrechtliche Bestimmungen auch auf Verarbeitungsprozesse von grundsätzlich nicht personenbezogenen Daten Anwendung finden sollen. Dieser Ansicht wird von Lobbygemeinschaften widersprochen: aufgrund des fehlenden Personenbezugs und somit wegen mangelnder Schutzwürdigkeit sollten anonymisierte, pseudonymisierte und verschlüsselte Daten generell aus dem Geltungsbereich der Datenschutzverordnung herausgenommen werden.

Generell sollten Anonymisierung, Pseudonymisierung und Verschlüsselung eingesetzt werden, um Daten vertraulich zu halten und sollten nicht eine einfache Möglichkeit darstellen, den Datenschutz zu umgehen. Die effizienteste Lösung, auch bei Big Data Anwendungen den Datenschutz zu gewährleisten, ist daher eine Identifizierung der Risiken und Folgenabschätzung im Einzelfall, wie sie auch die EU-Datenschutzgrundverordnung vorschlägt. Sowohl die gegebene Wichtigkeit der Einhaltung des Datenschutzes als auch die Möglichkeiten, die Big Data Anwendungen mit sich bringen können, rechtfertigen den

[165] *EPOF* Comments on the Review of the European Data Protection Framework, February 4, 2011; abrufbar unter: <ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations-_not_registered/european_privacy_officers_forum_en.pdf>.

Aufwand solcher Überprüfungen. Unternehmen sollen ermutigt werden, Lösungen zu finden für ein ausgewogenes Verhältnis zwischen der Einhaltung des Datenschutzes und dem Ermöglichen neuer Anwendungsfelder. Kann mithilfe der richtigen Mittel und Methoden sicher gestellt werden, dass aus den anonymisierten Verkehrsdaten keine Rückschlüsse auf einzelne Personen getroffen werden können, kann so ein Bewegungsstrom zulässigerweise sinnvoll eingesetzt werden, wie zu Beispiel zur besseren Planung des öffentlichen Verkehrsnetzes im Raum Zaragoza.

VII. LITERATUR

Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009)

Baumgartner, Grundrechte und Datenschutz, AnwBl 2014, 24

Brandl/Feiel, Telekommunikationsrecht, in Jahnel /Mader/Staudegger (Hrsg), IT-Recht³ (2012)

De Montjoye/Hidalgo/Verleysen/Blondel, Unique in the Crowd: The privacy bounds of human mobility, Scientific Reports³, 2013

Feiler/Fina, Datenschutzrechtliche Schranken für Big Data, MR 2013, 303

Feiler, Der Vorschlag der Europäischen Kommission für eine Datenschutz-Grundverordnung der EU, MR-Int, 2011, 127

Forgó/Krügel, Der Personenbezug von Geodaten, MMR 1/2010, 20

Graf, Datenschutzrecht im Überblick (2010)

Haidinger, Was sind personenbezogene Daten?, Dako 2014/7, 17

Jahnel, Datenschutzrecht, in Jahnel /Mader/Staudegger (Hrsg), IT-Recht³ (2012)

Jahnel, Handbuch Datenschutzrecht (2010)

Jahnel/Siegwart/Fercher (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007)

Jahnel, Spamming, Cookies, Logfiles und Location Based Services im TKG 2003, ÖJZ 2004/21, 336

Kassai, "Location Based Services" im Gefüge des Datenschutzrechts, MR, 2004, 433

Knyrim, Datenschutzrecht: Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm (2012)

Knyrim, Entwurf der neuen EU-Datenschutz-Grundverordnung, in Scholz/Funk, DGRl Jahrbuch (2012) 25

Kotschy, Das Grundrecht auf Geheimhaltung personenbezogener Daten. Rückblick und Ausblick (Teil I: § 1 Abs.1 DSG (1978) bzw. DSG 2000), in Jahnel (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2012 (2012) 27

Mantz, Standortdaten und Bewegungsprofile, K&R, 1/2013, 7

Mayer-Schönberger/Cukier, Big Data. Die Revolution, die unser Leben verändern wird (2013)

Mayer-Schönberger/Zeger/Kronegger, Auf dem Weg nach Europa: Zur Novellierung des Datenschutzgesetzes, ÖJZ 1998, 244

Pfarl, Gefunden! LBS im Mobilfunknetzbereich, ecolex 2005, 569

Pollirer/Weiss/Knyrim, Datenschutzgesetz 2000 (2013)

Reiter/Wittmann-Tiwald (Hrsg), Goodbye Privacy (2008)

Simitis, Bundesdatenschutzgesetz (2014)

Souhrada-Kirchmayer, Das Datenschutzgesetz 2000, SozSi 2000, 938

Stratil/Polster/Singer/Steinmaurer (Hrsg), TKG - Telekommunikationsgesetz 2003 (2013)

Suda, Datenverwendung für wissenschaftliche Forschung und Statistik, in Bauer/Reimer, Handbuch Datenschutzrecht, (2009), 293

Zib, Zur Zulässigkeit elektronischer Rechnungspräsentation bei Telekom- und Mobilfunk-Rechnungen, ÖBA 2004, 463

A. Online:

Datum der letzten Abfrage: 18.01.2015

Art-29–Datenschutzgruppe, Stellungnahme 01/2012 zu den Reformvorschlägen im Bereich des Datenschutzes, WP 191, 00530/12/DE, < www.cnpd.public.lu/de/publications/groupe-art29/wp191_de.pdf>

Art-29-Datenschutzgruppe, Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten, WP 185, 881/11/DE, <www.cnpd.public.lu/de/publications/groupe-art29/wp185_de.pdf>

Art-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 01248/07/DE, <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf>

Art-29-Datenschutzgruppe, Stellungnahme 5/2005 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen, WP 115, 2130/05/DE, <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_de.pdf>

Bericht der Kommission, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46), KOM (2003) 265 endg., <eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52003DC0265&from=DE>

Biermann, „Telefonica will Handy-Bewegungsdaten an Werber verkaufen", Zeit Online, 3/10/2012 <www.zeit.de/digital/datenschutz/2012-10/telefonica-smart-steps-vorratsdaten>

„Bundesregierung verbietet O2 Handel mit Bewegungsdaten", Handelsblatt, 31/10/2012 <www.handelsblatt.com/unternehmen/it-medien/ortungsprogramm-bundesregierung-verbietet-o2-handel-mit-bewegungsdaten/7328904.html>

Dorschel/Nauerth, Big Data und Datenschutz –ein Überblick über die rechtlichen und technischen Herausforderungen <www.bartsch-rechtsanwaelte.de/media/docs/JD/Big_Data.pdf>

EPOF, Comments on Review of the EU Data Protection Directive (Directive 95/46/EC), online: <ec.europa.eu/justice/policies/privacy/docs/lawreport/paper/epof_en.pdf>

EPOF, Comments on the Review of the European Data Protection Framework <ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations-_not_registered/european_privacy_officers_forum_en.pdf>

Europagruppe Grüne, Die europäische Datenschutzgrundverordnung in 10 Punkten <www.gruene-europa.de/die-europaeische-datenschutzgrundverordnung-in-10-punkten-10773.html>

Information Commissioner's Office, Big data and data protection <ico.org.uk/news/-latest_news/2014/~/media/documents/library/Data_Protection/Practical_application/big-data-and-data-protection.pdf>

Meister, „Big Data vs. Datenschutz: Forscher werten Handydaten von 15 Millionen Menschen über den Zeitraum von einem Jahr aus", Netzpolitik.org, 17/10/2012 <netzpolitik.org/2012/big-data-vs-datenschutz-forscher-werten-handydaten-von-15-millionen-menschen-uber-den-zeitraum-von-einem-jahr-aus>

Pfarl, Datenschutz bei LBS im Mobilfunkbereich und im europäischen Notrufsystem <www.it-law.at/wp-content/uploads/2014/09/Datenschutz-bei-LBS.pdf>

„Smart Step: Telefónica will Bewegungsprofile in Deutschland nicht auswerten", Spiegel Online Netzwelt, 1/11/2012 <www.spiegel.de/netzwelt/gadgets/telefonica-keine-auswertung-von-bewegungsdaten-in-deutschland-a-864772.html>

Telefónica <dynamicinsights.telefonica.com/1158/a-smart-step-ahead-for-morrisons>

Telefónica <dynamicinsights.telefonica.com/488/smart-steps>

“Telefonica hopes 'big data' arm will revive fortunes”, BBC News Technology, 9/10/2012 <www.bbc.com/news/technology-19882647>

“Telefónica to sell 'insights' gleaned from anonymised mobile phone location data”, Out-Law.com, 11/10/2012 <www.out-law.com/articles/2012/october/telefonica-to-sell-insights-gleaned-from-anonymised-mobile-phone-location-data>

Thiele, EuGH Urteil vom 24.11.2011, C-468/10, C-469/10 - ASNEF/FECEMD <www.eurolawyer.at/pdf/EuGH-C-468-10.pdf>

“Una aplicación tecnológica analizará el tráfico metropolitano”, El Periódico, 29/9/2014 <http://www.elperiodicodearagon.com/m/noticias/aragon/aplicacion-tecnologica-analizara-trafico-metropolitano_973535.html>

Weichert, Big Data und Datenschutz <www.datenschutzzentrum.de/bigdata/20130318-bigdata-und-datenschutz.pdf>

B. Judikaturauswahl:

EuGH, C-101/01 vom 6.11.2003 (Lindqvist)

EuGH 08.04.2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd und Seitlinger)

EuGH 24.11.2011, C-468/10, C-469/10 (ASNEF/FECEMD)

OGH 22.04.2010, 2 Ob 1/09z

OGH 14.7.2009, 4 Ob 41/09x

OGH 27.01.1999, 7 Ob 170/98w

OGH 22. 6. 2012, 6 Ob 119/11k

DSK 22. 4. 2005, K120.966/0005-DSK/2005

DSK 15.04.2011, K121.659/0007-DSK/2011

DSK 03.08.2012, K121.819/0019-DSK/2012

DSK 13.07.2012, K212.766/0010-DSK/2012 (Empfehlung)

VIII. Abkürzungen

ABl	Amtsblatt der Europäischen Union
Abs	Absatz
AC	Authentication Centre
AGB	Allgemeine Geschäftsbedingungen
BDSG	deutsches Bundesdatenschutzgesetz
BGBl	Bundes Gesetzblatt
bzw	Beziehungsweise
COM	Europäische Kommission
DSG	Datenschutzgesetz 2000
DSK	Datenschutzkommission
EG	Europäische Gemeinschaften
EIR	Equipment Identity Register
EPOF	European Privacy Officers Forum
ErläutRV	Erläuterungen zur Regierungsvorlage 128 BlgNR 22. GP
ErläutRV 11	Erläuterungen zur Regierungsvorlage 1389 BlgNR 24. GP
ErwGr	Erwägungsgrund
EU	Europäische Union
EU-DSGVO	Europäische Datenschutzgrundverordnung
EuGH	Gerichtshof der Europäischen Union
FN	Fußnote
gem	gemäß
GP	Gesetzgebungsperiode
GPS	Global Positioning System
GSM	Global System of Mobile Communications
HLR	Home Location Register
Hrsg	Herausgeber
idF	In der Fassung
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity

IT	Informationstechnologie
iVm	In Verbindung mit
KOM	Europäische Kommission
LAI	Location Area Identity
LBS	Location Based Service
lit	litera
MS	Mitgliedstaat(en)
MSC	Mobile Switching Center
MSISDN	Mobile Station Integrated Services Digital Network Number
OGH	Oberster Gerichtshof
RL	Richtlinie
Rz	Randzahl
SIM	Subscriber Identity Module
SPG	Sicherheitspolizeigesetz
StGG	Staatsgrundgesetz
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
VLR	Visitor Location Register
VfGH	Verfassungs-Gerichtshof
VO	Verordnung
Z	Ziffer
zB	zum Beispiel

IX. Zusammenfassung

Verwendung ortsbezogener Daten von Mobilfunkgeräten in Big Data Anwendungen

Mobilfunkanbieter erfassen zur Erbringung des Telekommunikationsdienstes ständig ortsbezogene Daten der Endgeräte ihrer Kunden. Bildet man die ortsbezogenen Mobilfunkdaten in anonymisierter und aggregierter Form ab, werden Aufenthaltsorte und Bewegungsmuster der Mobilfunkkunden in ihrer Gesamtheit ersichtlich. Die wirtschaftliche Bedeutung solcher Bewegungsströme ist groß, da auf deren Basis strategische Entscheidungen getroffen werden können. Da aber Standortdaten von Mobilfunkgeräten sehr viel über die einzelnen Nutzer verraten können, werden in der Nutzung dieser Daten nicht nur wirtschaftliche und innovative Möglichkeiten gesehen, sondern auch eine große Gefahr für den Datenschutz. Es stellt sich daher die Frage, ob diese Datenverwendung in Österreich datenschutzrechtlich überhaupt erlaubt ist.

Ortsbezogene Mobilfunkdaten fallen bei der Erbringung öffentlicher Telekommunikationsdienstleistungen an. Bei der Verwendung dieser Daten kommen daher zusätzlich zu den allgemeinen datenschutzrechtlichen Bestimmungen des Datenschutzgesetzes 2000 (DSG) auch die besonderen Bestimmungen des Telekommunikationsgesetzes (TKG) zur Anwendung.

Nach dem TKG sind Verkehrs- und Standortdaten streng an die gesetzlich vorgeschriebenen Verwendungszwecke gebunden. Sobald sie für die Erbringung des Telekommunikationsdienstes nicht mehr benötigt werden, sind sie unverzüglich zu löschen oder zu anonymisieren. Zu anderen Zwecken als der Erbringung des Kommunikationsdienstes dürfen Verkehrsdaten nur verwendet werden, wenn der Teilnehmer einer solchen Verwendung ausdrücklich zugestimmt hat.

Weiters können die ortsbezogenen Mobilfunkdaten zur Erfassung eines Bewegungsstroms verwendet werden, wenn sie so anonymisiert sind, dass ein Personenbezug

nicht mehr möglich ist. Auf nicht personenbezogene Daten findet das Datenschutzrecht keine Anwendung.

Gerade im Zusammenhang mit Big Data Anwendungen kann es aber dazu kommen, dass nicht personenbezogene Daten durch die Verknüpfung mit anderen Datensätzen letztlich doch einer Person zugeordnet werden können. Somit könnte die Verarbeitung gewisser anonymisierter Daten nicht vom Datenschutz umfasst sein, während auf ihr Ergebnis datenschutzrechtliche Bestimmungen Anwendung finden sollten. Es ist daher bei jedem Verarbeitungsschritt zu prüfen, ob ein Personenbezug gegeben ist oder nicht. Werden Mobilfunkdaten unverzüglich nach Beendigung des Kommunikationsdienstes so anonymisiert, dass ein Personenbezug ausgeschlossen ist, können die anonymisierten Bewegungsdaten verarbeitet werden.