Universitätslehrgang
für Informationsrecht und Rechtsinformation
an der Rechtswissenschaftlichen Fakultät der Universität Wien

Datenschutz bei LBS im Mobilfunknetzbereich und im europäischen Notrufsystem

MASTER THESIS

zur Erlangung des akademischen Grades

MASTER OF LAWS (LL.M.)
INFORMATIONSRECHT UND RECHTSINFORMATION

an der Universität Wien

(Universitätslehrgang für Informationsrecht und Rechtsinformation)

vorgelegt von

Mag. Wolfgang Pfarl

begutachtet von

o. Univ.-Prof. Dr. Dietmar Jahnel

im September 2003

Hinweise

Dieses Layout basiert auf der Typoskriptvorlage der Österreichischen Rechtswissenschaftlichen Studien (ÖRSt). Die Verwendung, Bearbeitung und allfällige Veröffentlichung der Bearbeitung erfolgt mit freundlicher Bewilligung des Manz-Verlages. Ansonsten wird auf das UrhG verwiesen.

Vorliegende Arbeit orientiert sich im Wesentlichen an den AZR (*Friedl* (Hrsg), Abkürzungs- und Zitierregeln der österreichischen Rechtssprache und europarechtlicher Rechtsquellen[5] (2000)). Zeitschriftenartikel werden mit der Anfangsseitenzahl zitiert, um eine leichtere Auffindbarkeit in der RDB zu ermöglichen.

Inhaltsverzeichnis

Seite

Abkürzungsverzeichnis

ABGB	=	Allgemeines bürgerliches Gesetzbuch
ABl	=	Amtsblatt der Europäischen Union
Abs	=	Absatz
AGB	=	Allgemeine Geschäftsbedingungen
(N)A-GPS	=	(Network)Assisted Global Positioning System
ASP	=	Application Service Provider
AZR	=	Allgemeine Zitierregeln
BG	=	Bundesgesetz
BGBl	=	Bundesgesetzblatt
BKA-VD	=	Bundeskanzleramt-Verfassungsdienst
BM	=	Bundesministerium
B-VG	=	Bundesverfassungsgesetz 1920 idF von 1929
BMVIT	=	Bundesministerium für Verkehr, Innovation und Technologie
BS	=	Base Station
bzw	=	beziehungsweise´
C	=	communicatio
CC	=	country code
Cell-ID	=	Cell-Identity
dh	=	das heißt
DSG	=	Datenschutzgesetz 2000
DSK	=	Datenschutzkommission
EB	=	Erläuternde Bemerkungen
ECRC	=	Emergency Call Response Centers
ecolex	=	Fachzeitschrift für Wirtschaftsrecht
EG	=	Europäische Gemeinschaft
EG-V	=	Vertrag zur Gründung der Europäischen Gemeinschaft
EK	=	Europäische Kommission
E-OTD	=	Enhanced Observed Time Difference
etc	=	et cetera
EP	=	Europäisches Parlament
EU	=	Europäische Union
EuGH	=	Europäischer Gerichtshof
EU-V	=	Vertrag über die Europäische Union
EWG	=	Europäische Wirtschaftsgemeinschaft
f(f)	=	folgende Seite(n)
FN	=	Fußnote
FS	=	Festschrift
G	=	Gesetz
gem	=	gemäß
GP	=	Gesetzgebungsperiode
GPRS	=	General Packet Radio Services
GPS	=	Global Positioning System
GSM	=	Global System of Mobile Communication

HLR	=	Home Location Register
Hrsg	=	Herausgeber
idF	=	in der Form
ieS	=	im engeren Sinn
IMEI	=	International Mobile Equipement Identifier
iSd	=	im Sinne des, - der
iVm	=	in Verbindung mit
iwS	=	in weiterem Sinn
KOM	=	Europäische Kommission
LAI	=	Location Area Identification
LBS	=	Location Based Services
leg cit	=	legis citatae (der zitierten Vorschrift)
LGBl	=	Landesgesetzblatt
Lit	=	litera
LMU	=	Location Measurement Unit
maW	=	mit anderen Worten
mE	=	meines Erachtens
MS	=	Mitgliedstaaten
MS	=	Mobile Terminal and SIM
MSISDN	=	Mobile Station Integrated Services Digital Network Number
mwN	=	mit weiteren Nachweisen
MVNO	=	Mobile Virtuell Network Operator
NR	=	Nationalrat
NDC	=	national destination number
Oftel	=	Office of Telecommunication
OGH	=	Oberster Gerichtshof
ONP	=	Open Network Provision
OTDOA	=	Observed Time Difference of Arrival
ÖRSt	=	Österreichische Rechtswissenschaftliche Studien
PC	=	Personal Computer
Rdz	=	Randzahl
RL	=	Richtlinie
RV	=	Regierungsvorlage
SIM	=	Subscriber Identity Module
SMLC	=	Serving Mobile Location Centre
SMS	=	Short Message System
SN	=	subscriber number
StGG	=	Staatsgrundgesetz
sog	=	sogenannt, -e, -er, -es
StProt	=	stenographische(s) Protokoll(e)
TA	=	Telekom Austria
TKG	=	Telekommunikationsgesetz 2003
uA	=	unter Anderem
UMTS	=	Universal Mobile Telecommunications Standard
uU	=	unter Umständen

v	=	vom, von
va	=	vor allem
VAS	=	value added services
vgl	=	vergleiche
VO	=	Verordnung
VwGH	=	Verwaltungsgerichtshof
WKO	=	Wirtschaftskammer Österreich
zB	=	zum Beispiel

Literaturverzeichnis

Barta, Wissenschaft und Verantwortlichkeit (1994).

Baumann/Collomb, IST-1999-14093 LOCUS – Enhanced Emergency Call Services (2001).

Baumann/Collomb/Dien/Lopes/Balletta/Casal, IST-1999-14093 LOCUS Deliverable D6 "Final Report" (2001).

Büllesbach, Datenschutz im Telekommunikationsrecht: Deregulierung und Datensicherheit in Europa (1999).

Dammann/Simitis, EG-Datenschutzrichtlinie (1997).

Djuknic/Richton, Geolocation and Assisted-GPS, Bell Laboratories, Lucent Technologies (2001).

Dohr/Weiss/Pollirer, Kommentar Datenschutzrecht – Datenschutzgesetz 2000 samt Europarecht, Nebengesetzen, Verordnungen und Landesdatenschutz mit Prüflisten und Mustern für die Praxis^2 (2002).

Drobesch/Grosinger, Das neue österreichische Datenschutzgesetz – Datenschutzgesetz, Verordnungen, datenschutzrechtliche Bestimmungen, mit ausführlichen Erläuterungen (2000).

Etling-Ernst, Praxiskommentar zum Telekommunikationsgesetz TKG (1999).

European Commission, Directorate B, State of Implementation of the single European emergency call number „112" (2001).

Fallenböck, Der Einsatz von Location Based Services – eine erste Analyse rechtlicher Problemfelder, MR 2002, 182.

Fallenböck/Haberler, Ortsbezogene Dienste für Handys: Droht der gläserne Benutzer?, Die Presse 2002/24/01.

Jahnel, Das Datenschutzgesetz 2000. Wichtige Neuerungen, wbl 2000, 49.

Jahnel, Datenschutz im Internet – Rechtsgrundlagen, Cookies und Web-Logs, ecolex 2001, 84.

Jahnel, Datenschutzrecht in Jahnel/Schramm/Staudegger, Informatikrecht^2 (2003).

Jahnel, Spamming, Cookies, Web-Logs, LBS und die Datenschutzrichtlinie für elektronische Kommunikation, wbl 2003, 108.

Köhler-Ludescher, Location Based Services der Mobilfunkbetreiber im Lichte des neuen Kommunikations-Rechtsrahmens (2000).

Kölmel, Location Based Services: Wünsche und Realität (2002).

Knyrim, Neuerungen im Datenverkehr mit Drittländern, ecolex 2002, 466.

Lechner in Schweighofer/Menzel/Kreuzbauer, IT in Recht und Staat – Aktuelle Fragen der Rechtsinformatik (2002).

Ludden/Pickofrod u.A., Report on implementation issues related to access to location information by emergency services (E112) in the European Union (2002).

Mayer-Schönberger, Information und Recht, Vom Datenschutz bis zum Urheberrecht, Praxisbezogene Perspektiven für Österreich, Deutschland und die Schweiz (2001).

Pfarl, 112 – Emergency Call Systems in Europe, Internal Paper, NetLight (2003).

Pracher, Datenschutz in der Telekommunikation in Forgo/Feldner/Witzmann/Dieplinger, Probleme des Informationsrechts (2003).

Ruhle, Auskunfts- und Verzeichnisdienste im österreichischen und europäischen Telekommunikationsrecht, MuR 2/99.

Schaar, Datenschutz im Internet, Die Grundlagen (2002).

Online:

Dib/Krenn/Leitner, Die bestehenden Möglichkeiten, Benutzer von Mobiltelefonen, GPS und der Bankomatkarte zu kontrollieren, http://www.ifz.tu-graz.ac.at/educate/lv_archiv/krenn_leitner_dib.pdf [Stand 28. Juni 2003].

Fischer, Location Based Service II – Die hohe Kunst der Ortung, online: http://www.networkworld.de/index.cfm?id=81901&pageid=156&type=detail [Stand 2. Juli 2003].

Forum Mobilkommunikation, Die Welt ist im Umbruch, online: http://www.fmk.at/mobilkom/detail.cfm?Textid=5&Kapitelnr=3 [Stand 27 Juni 2003]*Bydlinski P.*, Die Notariatsaktpflicht 1850 und heute, NZ 1990, 289.

Hintergrundpapier – Ortsbezogene Mobilfunkdienste, Location Based Services, http://www.ericsson.de/downloads/pressenews/HintergrundpapierLBS.pdf [Stand 6. Juli 2003].

Huber/Jaenicke/Wallers, GIS und Location Based Services - neue Entwicklungen der Industrie -, online: http://www.gis1.bv.tum.de/Lehre/Vertiefung/GIS-Projekte/Dokumente/Gruppe4.pdf, [Stand 1. Juli 2003].

Hubschneider/Kölmel, Location Based Services – Eine Killerapplikation für UMTS?, online: http://www.e-lba.com/YellowMap_Location%20Based%20Services.pdf [Stand 28. Juni 2003].

Mobile Guide, online: www.a1.net/CDA/article/art_display/0,2756,31-574-html-de,00html [Stand 28. Juni 2003].

Nowak, Location Based Services – Das Telefon-Navigations-Center TelNav, online: http://www.experteam.de/startd/publikationen/Artikel/Ber03_BL.html [Stand 2. Juli 2003].

Oftel, An overview of the fixed telephone emergency services (999/112) – An explanatory document issued by the DG of Telecommunication, 2002, online: http://www.oftel.gov.uk/publications/ind_guidelines/emer1002.htm [Stand 25. Juli 2003].

Sehovic, Location-based, die Herausforderung der Technik die "weiss wo Du bist", online: http://de.gsmbox.com/news/mobile_news/all/20938.gsmbox [Stand 2. Juli 2003].

Tödlicher Wespenstich vor Gericht, Kurier vom 27.8.2003, online http://www.kurier.at/chronik/364136.php [Stand 4. September 2003].

Es gibt Menschen, die gehen in den Wald und finden doch kein Holz.

Tschingis Khan

I. Einleitung

Die Kontrolle über Benutzer-Ortsinformationen innerhalb der Mobilfunknetze macht Netzbetreiber besonders mächtig, auch deshalb, weil die Mehrheit der Anwender den Wunsch hat, diese Informationen exklusiv dem jeweiligen Netzbetreiber zur Verfügung zu stellen.[1] Tatsächlich werden ortsbezogene Dienste, oder Teile davon oft von Dritten (sogenannten Application Service Providern (ASP) oder Content-Providern erbracht.[2] Viele Nutzer möchten wissen, wie persönliche Daten verwendet werden. Sie fragen sich, welche Daten verlangt werden und wer diese zu Gesicht bekommt.[3] Datenschutz schafft Vertrauen und Vertrauen ist wichtig für den Erfolg ortsbezogener Dienste.

Die vorliegenden Arbeit soll praxisnahe juristische Lösungen für datenschutzrechtliche Probleme des modernen Findens und Gefundenwerdens bieten. Es werden ausschließlich die Vorschriften des neuen europäischen Rechtsrahmens und das Datenschutzgesetz 2000 (DSG) und das Telekommunikationsgesetzes 2003 (TKG) diskutiert.

A. Wirtschaftliche Aspekte und Kategorisierung von LBS

Obwohl schon vorhanden, sind ortsbezogene Dienste, sogenannte Location Based Services (LBS), heute meist nur dem Interessierten ein Begriff. Dies wird sich in Österreich und in den meisten anderen europäischen Ländern aus zweierlei Gründen in naher Zukunft ändern. Erstens weist

---

1) 73% der Nutzer und Teilnehmer von LBS sind der Meinung, dass Informationen über den Aufenthaltsort grundsätzlich nur dem Netzbetreiber bekannt sein sollten; Siehe *Kölmel*, Location Based Services: Wünsche und Realität (2002), 5.

2) Aus Gründen der Einfachheit und um Verwechslungen zu vermeiden, wird der Begriff „Location Based Service Provider" („LBS-Provider") für alle Unternehmen die potentiell ortsbezogene Leistungen anbieten verwendet; Dh für klassische Mobilfunkbetreiber, Mobile Virtuell Network Operators (MVNO), Application Service Provider (ASP) und für Content Provider.

3) Laut einer Forrester Studie „Surviving the Privacy Revolution", schätzen über 60% der zukünftigen Nutzer von LBS die Missbrauchsgefahr von persönlichen Daten bei ortsbezogenen Diensten extrem hoch ein; *Fallenböck/Haberler*, Ortsbezogene Dienste für Handys: Droht der gläserne Benutzer?, Die Presse 2002/24/01.

Österreich, sowie die meisten anderen europäischen Länder eine enorm hohe Mobilfunkpenetration auf.[4] Das hat einerseits zur Folge, dass sich Mobilfunknetzprovider und Entwickler insbesondere auf LBS konzentrieren, die als sogenannte „**Killerapplikationen**" bezeichnet werden. Eine Killerapplikation ist eine Anwendung, die sich durch enormes Kundeninteresse und hohe wirtschaftliche Rentabilität ausgezeichnet.[5] Durch das erwartete Kundeninteresse nehmen ortsbezogenen Dienste eine Sonderstellung unter den Value Added Services (VAS) ein. Der zweite Grund für die rasche Etablierung von ortsbezogenen Leistungen liegt wahrscheinlich in der **Dienstevielfalt**. Die untenstehende Aufzählung von LBS steht beispielhaft für die mannigfaltigen Anwendungsgebiete und versucht diese zu kategorisieren. Eine begriffsexakte Unterscheidung zwischen den verschiedenen Arten von LBS ist für datenschutzrechtliche Qualifikationen wichtig.

Grundsätzlich kann man ortsbezogene Dienste in folgende Kategorien einteilen: Erstens, **informationsbezogene Dienste** (Infotainment); Zweitens, **gebührenbezogene Dienste** (location sensitive billing); Drittens **sicherheitsbezogene Dienste (**safety**)**; Viertens, **positionsübermittelnde Dienste** (tracking, positioning).[6] Neben diesen Hauptkategorien gibt es, wie unten gezeigt wird, verschiedenste spezifische Anwendungen die unter einen oder unter mehrerer dieser Begriffe zu subsumieren sind.[7] Weiters wird zwischen „pull-" und „push-" Diensten" unterschieden. Bei „push-" Services wird die Anwendung vom Servicebetreiber an den Nutzer geschickt (zB LB Advertising). Bei „pull-" Diensten wird das Service erst nach Anfrage des Kunden ausgeführt (zB „Find Next-"Dienste).

Unter informationsbezogenen Diensten versteht man hauptsächlich sogenannte „pull-" Services". Standortbezogene Informationen werden von einem Nutzer angefordert und anschließend auf dem Handy des Nutzers abgefragt. Informationen bei sogenannten „Find Next-"Diensten sind beispielsweise der Standort des nächsten Bankomats, der nächstgelegenen Busstation oder, der geographische Standort der nächstgelegenen italienischen

---

4) Forum Mobilkommunikation, Die Welt ist im Umbruch, online: http://www.fmk.at/mobilkom/detail.cfm?Textid=5&Kapitelnr=3 [Stand 27 Juni 2003].

5) *Hubschneider/Kölmel*, Location Based Services – Eine Killerapplikation für UMTS?, 13, online: http://www.e-lba.com/YellowMap_Location%20Based%20Services.pdf [Stand 28. Juni 2003].

6) ibid, 6.

7) Als beliebteste LBS gehen bei einer Online-Umfrage aus dem Jahre 2002 folgende Dienste hervor: „Preisvergleich mit Ortsbezug", „Find Next-"Dienste, „Parkplatz-Finder", „Friend-Finder", „LB Messaging", „City-Guide", „Event-Guide"; Als gute Zahlungsformen werden Pay-per Use (58%), Flat Rate (49%) und Credits/Prepaid (30%) genannt. Außerdem können sich 47% der Befragten vorstellen, einen kostenlosen Dienst gegen Empfang einer Werbung zu nützen; Siehe *Kölmel*, Location Based Services: Wünsche und Realität[1] (2002), 8f. Bezüglich weiterer Anwendungen von ortsbezogenen Diensten (Maut, Kontrolle von Mitarbeitern, Kontrolle von Straftätern) siehe *Lechner* in Schweighofer/Menzel/Kreuzbauer, IT in Recht und Staat – Aktuelle Fragen der Rechtsinformatik (2002), 351ff.

Restaurants.[8] Zu dieser Kategorie gehören auch Services, die nur ein einziges Mal angefordert werden, dann aber im aktuellen Fall unaufgefordert zugesandt werden. Ein Beispiel wäre etwa eine Stauwarnung. Derartige Services sind Beispiele für informationsbezogene Dienste. Die dafür notwendigen Daten werden gewöhnlich von Content-Lieferanten bereitgestellt, auch Mobilfunknetzbetreiber selbst entwickeln Inhalte für LBS.

Beim **location sensitive billing**, einem gebührenbezogenen Dienst, wird der Tarif abhängig vom Standort gestaltet. Es werden unterschiedliche Telefontarife je nach Aufenthaltsort verrechnet, also zum Beispiel ein „Office-Tarif", ein „City-Tarif" und ein „Home-Tarif". Das Netz erkennt selbstständig, wo sich der Kunde befindet, am Display erscheint das jeweilige Symbol für den jeweiligen Tarif.

Unter **sicherheitsbezogenen Diensten** fallen uA Features, die es ermöglichen Notrufe zu lokalisieren. Die Europäische Kommission (EK) empfiehlt den Mitgliedstaaten (MS), die jeweiligen Mobilfunknetzbetreiber zu verpflichten, Standortdaten sogenannten Emergency Call Response Centres (ECRC) zur Verfügung zu stellen.[9] Als sicherheitsbezogene Dienste kann man auch „pull-" Services bezeichnen, die es erlauben den Standort des nächsten Krankenhauses oder Arztes zu ermitteln. Des weiteren gibt es Dienste wie das „Commercial Assistance Service", „Car Breakdown Assistance", „Car Accident Detection" oder „Rescue, Car Theft Recovery – Service". Diese Dienste erlauben die Ortung von Fahrzeugen bei KFZ-Unfällen und allgemeinen Notfällen.[10]

Die am häufigsten angewandten Services zur **Personenortung** sollte man unter Infotainment einordnen und erlauben die Ortung von Freunden oder Bekannten nach deren Einverständnis. Dienste zur Ortung von Mitarbeitern (zB Taxilenkern, Lkw-Fahrern usw.) werden unter Business Services subsumiert. Systeme zur automatischen Alarmierung von Personen fallen unter die Kategorie sicherheitsbezogene Dienste. Es ist beispielsweise möglich, den Aktionsradius von Personen zu kontrollieren (Kinder, hilfsbedürftige Personen, Straftäter usw.). So ist es beispielsweise möglich, festzustellen, ob sich Kinder innerhalb eines bestimmten Gebietes aufhalten. Services zur Personenortung werden auch als **Tracking und Tracing** Anwendungen bezeichnet.

---

[8]) Mit dem „Mobile Guide" von A1 kann beispielsweise das nächste Restaurant, Tankstelle, Bankomat oder die nächste Apotheke gefunden werden. Dieses Service funktioniert über WAP und SMS; Siehe Mobile Guide, online: www.a1.net/CDA/article/art_display/0,2756,31-574-html-de,00html [Stand 28. Juni 2003].

[9]) Dieses Themengebiet wird in Kapitel III behandelt.

[10]) *Dib/Krenn/Leitner*, Die bestehenden Möglichkeiten, Benutzer von Mobiltelefonen, GPS und der Bankomatkarte zu kontrollieren, online: http://www.ifz.tu-graz.ac.at/educate/lv_archiv/krenn_leitner_dib.pdf [Stand 28. Juni 2003].

Business Services werden in der Praxis noch nicht voll eingesetzt. Das Auffinden und Managen von Containern, LKWs, Paketsendungen oder Taxis wird in naher Zukunft das Geschäftsleben verändern.

LB-Advertising ist ein Dienst, der zu den sogenannten „push-" Services gerechnet wird. Dabei werden uA Sonderangebote (zB Happy Hour), Produktinformationen und andere Promotions-Aktivitäten an Mobilfunkteilnehmer geschickt.[11]

B. Technische Grundlagen

Die technische Grundlagen von ortsbezogenen Diensten und Mobilfunk im Allgemeinen werden in diesem Kapitel nur soweit behandelt, als dies für das allgemeine Verständnis von LBS und für die rechtlichen Schlussfolgerungen notwendig ist. Im übrigen wird auf einschlägige Literatur verwiesen.[12]

Beim Betrieb eines Mobilfunknetzes fallen notwendiger Weise **Verkehrsdaten** im Sinn des Artikels 2 lit b der Datenschutzrichtlinie für elektronische Kommunikation an.[13] Für den Kommunikationsaufbau und das Erhalten der Verbindung benötigte Verkehrsdaten beziehen sich unter anderem auch auf den Standort des Telekommunikationsendgerätes eines Absenders oder Empfängers einer Nachricht (auch LBS oder SMS).[14] Auf den juristischen Unterschied zwischen **Standortdaten** iSd Artikels 2 lit c und Verkehrsdaten iSd Artikels 2 lit b der Datenschutzrichtlinie für elektronische Kommunikation wird in Kapitel II/E/4 und /5 besonders eingegangen.[15] Festzuhalten bleibt,

---

[11]) Nochmals sei darauf hingewiesen, dass der Einsatz von LBS fast unbegrenzt scheint und die obenstehende Aufzählung nur die allerwichtigsten Anwendungen nennt. Ein Beispiel für eine ausgefallene Anwendung eines LBS ist der sogenannte „Grabfinder", welcher nicht nur das Auffinden von Gräbern erleichtert, sondern auch über deren Beschaffenheit Auskunft gibt. Dieses Service wird aber wahrscheinlich nicht via Mobiltelefon, sondern via PenPC abrufbar sein; *Huber/Jaenicke/Wallers*, GIS und Location Based Services - neue Entwicklungen der Industrie -, online: http://www.gis1.bv.tum.de/Lehre/Vertiefung/GIS-Projekte/Dokumente/Gruppe4.pdf [Stand 1. Juli 2003].

[12]) Siehe zB *Nowak*, Location Based Services – Das Telefon-Navigations-Center TelNav, online: http://www.experteam.de/startd/publikationen/Artikel/Ber03_BL.html [Stand 2. Juli 2003]; *Sehovic*, Location-based, die Herausforderung der Technik die "weiss wo Du bist", online: http://de.gsmbox.com/news/mobile_news/all/20938.gsmbox [Stand 2. Juli 2003]; *Fischer*, Location Based Service II – Die hohe Kunst der Ortung, online: http://www.networkworld.de/index.cfm?id=81901&pageid=156&type=detail [Stand 2. Juli 2003].

[13]) 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 201 vom 31.07.2002, 37.

[14]) Erwägungsgrund 15 der Richtlinie 2002/58/EG, ABl. L 201 vom 31.07.2002, 37.

[15]) Richtlinie 20002/58/EG, ABl. L 201 v 31.07.2002, 37.

dass ohne die Identifizierung der Zelle, in der sich der Kunde befindet, keine mobile Telekommunikation möglich ist.

Darüber hinaus werden ständig bessere, exaktere Ortungstechnologien entwickelt, weil Mobilfunknetzbetreiber aus wirtschaftlichen Gründen interessiert sind die geographischen Standpunkte ihrer Kunden möglichst genau zu erfassen.[16] Die wichtigsten Technologien werden im nächsten Absatz kurz aufgezählt und wird in den Fußnoten auf weiterführende Literatur verwiesen.

Grundlegende Ortungsmethoden basieren auf der Identifizierung und Verarbeitung von Zellinformation (**Cell-ID**).[17] Weiterentwickelte Techniken basieren auf sogenannter Triangulation. Dabei unterscheidet man zwischen Enhanced Observed Time Difference (**E-OTD**), das Mobiltelefon ortet sich im Netz, und Observed Time Difference of Arrival (**OTDOA**), das Netz ortet das Mobiltelefon.[18] Abgesehen von den oben genannten „traditionellen" Ortungsmethoden im Mobilfunknetzbereich wird das sogenannte Assisted Global Positioning System (**A-GPS**), auch Network Assisted GPS (**NA-GPS**) genannt, die zukünftig wichtigste Ortungstechnologie im Mobilfunkbereich sein. Diese Technik wird bereits heute eingesetzt. Die Hilfe für die Ortung durch Satelliten kommt vom Mobilfunknetzwerk selbst. Für die Ortung werden die durch das Netz selbst errechneten Daten zum ungefähren Aufenthaltsort des Nutzers im Sektor einer Zelle für die Berechnung des genauen Aufenthaltsortes durch einen eingebauten GPS-Sender verwendet. Dadurch verringert sich die Standortberechnungszeit auf wenige Sekunden, es werden nur zwei Satelliten zur Ortung benötigt und der Energieverbrauch wird

16) Wie in Kapitel I, A festgehalten, wird mit einem großen Kundeninteresse an LBS gerechnet und sollen LBS uA auch die, durch den Ausbau der UMTS-Netze angefallenen Netze wirtschaftlich rechtfertigen.

17) Der letzte bekannte Standort eines Handys ist stets im Home Location Register (**HLR**) vermerkt. Das HLR ist eine Art Stammdatenbank im Mobilfunknetz am „Heimatort" des Nutzers. Der Mobilfunkbetreiber braucht diese Information, um seinen Teilnehmer anrufen zu können; Hintergrundpapier – Ortsbezogene Mobilfunkdienste, Location Based Services, online: http://www.ericsson.de/downloads/pressenews/HintergrundpapierLBS.pdf [Stand 6. Juli 2003].

18) Für die Technik der Triangulation benötigt man zumindest drei Mobilfunksender. Befindet sich das Handy im Einzugsbereich dieser Mobilfunksender, so kann es über die Abstände zu den Sendern auf unter einen Kilometer genau geortet werden (Schnittfläche von 550-m-Feldern). Je näher die Sender beisammen stehen, desto genauer ist die Ortung möglich (bis zu 100 m). Diese Techniken funktionieren beim synkron laufenden GSM-Netz. Beim nicht synkrotisierten UMTS-Netz braucht das Handy zu seiner Ortsbestimmung Information über die unterschiedlichen Sendezeiten der Basisstationen (RTD, Relative Time Difference). Diese Zeiten können aus einer Messung an einem bekannten Ort zwischen den Stationen ermittelt werden oder von der Location Measurement Unit zur Verfügung gestellt werden. Die Location Measurement Unit erhält die präzise Zeit von GPS-Satelliten; *Baumann/Collomb/Dien/Lopes/Balletta/Casal*, IST-1999-14093 LOCUS Deliverable D6 "Final Report" (2001), 8f.

verringert.[19] Die Abbildungen 1 bis 3 im **Annex** veranschaulichen von der Praxis angewendete Ortungsmethoden visuell, Abbildung 4 gibt einen Überblick über die Genauigkeit der verschiedenen Ortungsmethoden.

[19]) Für weiter Information bezüglich dieser Technologie siehe *Djuknic/Richton*, Geolocation and Assisted-GPS, Bell Laboratories, Lucent Technologies (2001).

C. Legislatur

Dieses Kapitel ermöglicht dem Leser einen raschen Überblick über einschlägige Rechtsvorschriften des europäischen und österreichischen Rechtsrahmens.

1. Europäischer Rechtsrahmen

a) Richtlinie 95/46/EG, „Allgemeine Datenschutzrichtlinie“[20]

Die Allgemeine Datenschutzrichtlinie ist für datenschutzrechtliche Fragen bei ortsbezogenen Diensten insoweit wichtig, als sie allgemeine Grundsätze für den Schutz der Privatsphäre formuliert. Der europäische Rechtsrahmen umfasst zwei für den Datenschutz bei LBS relevante Richtlinien. Richtlinie 95/46/EG enthält allgemeine datenschutzrechtliche Vorgaben. Dagegen beinhaltet die, im nächsten Kapitel behandelte Richtlinie 2002/58/EG sektorspezifische Regelungen für den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation[21]

b) Richtlinie 2002/58/EG, „Datenschutzrichtlinie für elektronische Kommunikation“[22]

Die Datenschutzrichtlinie 97/66/EG für Telekommunikation ging als sektorspezifische Datenschutzrichtlinie uA besonders auf Verkehrsdaten, Vertraulichkeit der Telekommunikation und Daten für die Gebührenabrechnung ein.[23] Richtlinie 97/66/EG wurde durch die Datenschutzrichtlinie 2002/58/EG für elektronische Kommunikation ersetzt.[24]

---

[20]) 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 281 vom 23.11.1995, 31.

[21]) 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 201 vom 31.07.2002, 37, ABl. L 201 vom 31.07.2002, 37.

[22]) 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 201 vom 31.07.2002, 37.

[23]) Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation ABl L 24 vom 30.01.1998, 1.

[24]) Richtlinie 2002/58/EG, ABl. L 201 vom 31.07.2002, 37, ABl. L 201 vom 31.07.2002, 37.

Richtlinie 2002/58/EG setzt, wie ihre Vorgängerin allgemeine Grundsätze der Allgemeinen Datenschutzrichtlinie in sektorspezifische Vorschriften für den Telekommunikationssektor um. Ziel der Richtlinie 2002/58/EG ist die **Harmonisierung** der Vorschriften in den Mitgliedstaaten (MS), um ein gleichwertiges datenschutzrechtliches Niveau in allen MS zu gewährleisten, das Voraussetzung für den **freien Datenverkehr** in der elektronischen Kommunikation innerhalb der Gemeinschaft ist.[25] Eine Harmonisierung der Vorschriften der MS wird durch einen gleichwertigen Schutz der entsprechenden Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre (Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union).und der Vertraulichkeit der Kommunikation gewährleistet. [26]

Der europäische Rechtsrahmen musste an die Entwicklungen der Märkte und Technologien für elektronische Kommunikationsdienste angepasst werden, um den Nutzern öffentlich zugänglicher elektronischer Kommunikationsdienste unabhängig von der zugrundeliegenden Technologie den gleichen Grad des Schutzes personenbezogener Daten und der Privatsphäre zu bieten. Dies konnte durch Richtlinie 97/66/EG nicht mehr gewährleistet werden. Jene Richtlinie wurde daher aufgehoben und durch die Richtlinie 2002/58/EG ersetzt.[27] Der neue Rechtsrahmen enthält nach Möglichkeit **technologieneutrale Vorschriften**.[28]

Standortbezogene Dienste werden von der Richtlinie nicht explizit genannt. Allerdings wird erstmals der Begriff „Standortdaten" definiert und somit der Bergriff „Verkehrsdaten" klargestellt.[29]

Die MS müssen die Datenschutzrichtlinie für elektronische Kommunikation bis **31. Oktober 2003** umsetzen.[30] Dieser Verpflichtung wurde in Österreich durch den Beschluss des Nationalrats (NR) vom 10. Juli 2003 nachgekommen. Auf das Telekommunikationsgesetz 2003 (TKG) wird in Kapitel B/2 eingegangen.

---

[25]) Artikel 1 Abs 1 Richtlinie 2002/58/EG, ABl. L 201 vom 31.07.2002, 37.

[26]) Erwägungsgrund (2) RL 2002/58/EG, ABl. L 201 vom 31.07.2002, 37.

[27] Erwägungsgrund (4) RL 2002/58/EG, ABl. L 201 vom 31.07.2002, 37.

[28]) Ibid.

[29]) Vor Inkrafttreten der Richtlinie 2002/58/EG gab es bei der Verwendung von Standortdaten im Rahmen der Erbringung von LBS viele offene Fragen; Siehe beispielsweise *Fallenböck*, Der Einsatz von Location Based Services – eine erste Analyse rechtlicher Problemfelder, MR 2002, 182; Definitionsschwierigkeiten beim Begriff Verkehrsdaten werden durch Artikel 2 lit c RL 2002/58/EG großteils ausgeräumt; Siehe Kapitel II/E/4 und 5.

[30]) Artikel 17, RL 2002/58/EG ,ABl. L 201 vom 31.07.2002, 37.

2. Österreichischer Rechtsrahmen

a) Datenschutzgesetz 2000 (DSG)[31]

Obwohl das Datenschutzgesetz 2000 (**DSG**) die in Kapitel II/A/1 kurz vorgestellte „Allgemeine Datenschutzrichtlinie" 95/46/EG umsetzt, versucht es, den in Österreich bewährten Regelungsstrukturen treu zu bleiben.[32] Neben Artikel 10a StGG und Artikel 8 EMRK, die das Fernmeldegeheimnis unter Grundrechtsschutz stellen, ist auch § 1 DSG 2000 eine **Verfassungsbestimmung**, die den Datenschutz im Telekommunikationsbereich betrifft:

„*Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht*."

Das DSG bildet das datenschutzrechtliche Rückgrad für alle sektorspezifischen Datenschutzregelungen, daher auch für das Telekommunikationsgesetz 2003 (TKG). Soweit ein Sachverhalt von sektorspezifischen Datenschutzgesetzen nicht geregelt wird, ist das DSG anzuwenden.

b) Telekommunikationsgesetz 2003 (TKG)[33]

Das Telekommunikationsgesetz 1997 (**TKG 1997**)[34] wird durch das Telekommunikationsgesetz 2003 (**TKG**) ersetzt, welches der NR am 10 Juli 2003 beschlossen hat. Bis zum Inkrafttreten des TKG, sind alle Bestimmungen des TKG 1997 anwendbar.

Das TKG 2003 setzt in Abschnitt 12 „Kommunikationsgeheimnis, Datenschutz" die Richtlinie 2002/58/EG um, soweit diese für den Wirkungsbereich des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT) relevant ist.[35] Abschnitt 12 betrifft **sektorspezifische Regelungen** für den Datenschutz und den Schutz der Privatsphäre in der

---

[31]) Bundesgesetz über den Schutz personenbezogener Daten Datenschutzgesetz 2000 - DSG 2000), BGBl. I Nr. 165/1999 idF BGBl. I Nr. 136/2001.

[32]) *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz – Datenschutzgesetz, Verordnungen, datenschutzrechtliche Bestimmungen, mit ausführlichen Erläuterungen (2000), 80f. Die Neuerungen des DSG werden in folgendem Beitrag zusammengefasst: *Jahnel*, Das Datenschutzgesetz 2000. Wichtige Neuerungen, wbl 2000, 49.

[33]) Bundesgesetz mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl I 70/2003.

[34]) Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird, das Telegraphenwegegesetz, das Fernmeldegebührengesetz und das Kabel- und Satelliten-Rundfunkgesetz geändert werden sowie ergänzende Bestimmungen zum Rundfunkgesetz und zur Rundfunkverordnung getroffen werden, BGBl. I Nr. 100/1997 idF BGBl. I Nr. 16/2003 (VfGH).

[35]) Erläuterungen zur Regierungsvorlage TKG, 1.

Telekommunikation. Überspitzt formuliert ist Abschnitt 12 des TKG das Pendant zu Richtlinie 2002/58/EG. Beide konkretisieren allgemeine Datenschutzvorschriften für den (Tele-)Kommunikationsbereich.

II. Rechtsrahmen für ortsbezogene Dienste in Österreich

Ziel dieses Kapitels ist die Beschreibung der Grundsätze des für LBS-Provider relevanten Datenschutzrechts und die Analyse und Lösung konkreter datenschutzrechtlicher Problemstellungen, die bei der Erbringung von ortsbezogenen Diensten in Österreich anfallen.

A. Anwendungsbereich des TKG und des DSG

Ein **Kommunikationsdienst** wird von § 3 Z 9 TKG definiert als „*eine gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben. Ausgenommen davon sind Dienste der Informationsgesellschaft im Sinne von § 1 Abs. 1 Z 2 des Notifikationsgesetzes, BGBl. I Nr. 183/1999, die nicht ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze bestehen*".

Ortsbezogene Dienste bestehen überwiegend in der Übertragung von Signalen über Kommunikationsnetze.[36] Weiters definiert § 92 Abs 3 Z 6 TKG in Anlehnung an Richtlinie 2002/58/EG erstmals Standortdaten. §§ 92 Abs 3 Z 6 und 102 TKG beziehen sich eindeutig auf ortsbezogene Dienste. Dies führt zum Schluss, dass ortsbezogene Dienste jeglicher Art in den **Anwendungsbereich** des TKG fallen.

Artikel 2 lit g Richtlinie 2002/58/EG definiert einen **Dienst mit Zusatznutzen** als jeden Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht. Auch Erwägungsgrund 18 der Richtlinie 2002/58/EG geht auf value added services (VAS) ein und nennt als Beispiele Navigationshilfen, Verkehrsinformation, Wettervorhersage oder touristische Informationen.

Eine Diskussion, ob gewisse ortsbezogene Dienste als Auskunftsdienste (zB sogenannte „Find Next-"Dienste, zB „wo ist der nächste Bankomat") angesehen werden sollten und daher nicht in den Anwendungsbereich des TKG fallen, ist daher obsolet geworden. Der neue europäische Rechtsrahmen

[36]) Die Begriffsbestimmungen der einschlägigen Richtlinien der EG wurden auch in das österreichische Recht übernommen, um eine vollständige Umsetzung der Richtlinien sicherzustellen.

und das TKG selbst stellen klar, dass die datenschutzrechtlichen Bestimmungen des TKG für alle ortsbezogenen Dienste zu beachten sind.[37]

Ein Recht auf Datenschutz nach dem DSG und dem TKG, dh ein schutzwürdiges Geheimhaltungsinteresse setzt voraus, dass es **personenbezogene Daten** gibt, die auf eine in ihrer Identität bestimmte oder auf legale Weise bestimmbare Person zurückgeführt werden können. Weiters müssen diese Daten geheim gehalten werden können.[38] Auf die Definition von personenbezogenen Daten wird in Kapitel II/E/1 näher eingegangen.

Soweit das TKG nichts anderes bestimmt, sind auf Sachverhalte, auf die das TKG anzuwenden ist, daher auch auf LBS, die Bestimmungen des DSG anzuwenden.[39] Das DSG ist beim Datenschutz im Telekommunikationsbereich die zum TKG **subsidiäre Norm**. Das DSG wird von den sektorspezifischen datenschutzrechtlichen Bestimmungen des TKG verdrängt.

B. Konzession

Vor dem Inkrafttreten des TKG war das Anbieten von ortsbezogenen Diensten nur durch Betreiber zulässig, welche über eine Mobilfunklizenz verfügen.[40] Der neue Rechtsrahmen, der durch das TKG in nationales Recht umgesetzt wurde, macht jeden Bescheid der Regulierungsbehörde unbeachtlich, in welchem festgestellt wurde, dass für die Erbringung des mobilen Sprachtelefoniedienstes und anderer Mobilfunkdienste mittels selbstständiger Mobilkommunikationsnetze eine Konzession notwendig ist.[41]

§ 15 TKG formuliert, dass die beabsichtigte Bereitstellung eines öffentlichen Kommunikationsdienstes, daher auch eines ortsbezogenen Dienstes, sowie dessen Änderung und dessen Einstellung vor Betriebsaufnahme, Änderung oder Einstellung der Regulierungsbehörde **anzuzeigen** ist. Eine Konzession von der Regulierungsbehörde ist für das Anbieten von LBS daher nicht mehr erforderlich.[42] Die Bestätigung über die

---

[37]) Bezüglich dieser Diskussion siehe *Ruhle*, Auskunfts- und Verzeichnisdienste im österreichischen und europäischen Telekommunikationsrecht, MuR 2/99, 119.

[38]) *Dohr/Weiss/Pollirer*, Kommentar Datenschutzrecht – Datenschutzgesetz 2000 samt Europarecht, Nebengesetzen, Verordnungen und Landesdatenschutz mit Prüflisten und Mustern für die Praxis[2] (2002), 15.

[39]) § 92 Abs 1 TKG.

[40]) § 14 Absatz 1 TKG Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird, das Telegraphenwegegesetz, das Fernmeldegebührengesetz und das Kabel- und Satelliten-Rundfunkgesetz geändert werden sowie ergänzende Bestimmungen zum Rundfunkgesetz und zur Rundfunkverordnung getroffen werden, BGBl. I Nr. 100/1997 idF BGBl. I Nr. 16/2003.

[41]) Siehe zB Bescheid Z18/02-26, 30.10.2002, 8f.

[42]) Zum Zeitpunkt des Inkrafttretens des TKG bestehende Anzeigen nach § 13 TKG 1997 und Konzessionen nach § 14 TKG 1997 erlöschen mit Inkrafttreten dieses Bundesgesetzes. Die Rechte und Pflichten gelten als Nebenbestimmungen im Sinne des § 55 Abs. 10. Rechte und Pflichten, die sich aus der Zuteilung von Frequenzen an Konzessionsinhaber ergeben, bleiben unberührt; § 133 Abs 4 und 6 TKG.

eingebrachte Anzeige und die Konzessionsurkunde nach dem TKG 1997 gelten als Bestätigungen der Anzeige im Sinne § 15 Abs. 3 TKG.[43]

C. Auskunftsrecht und Rechtsschutz

Das TKG beinhaltet weder Regelungen über das **Auskunftsrecht** noch über den **Rechtsschutz**. Daher ist gemäß § 92 Abs 1 TKG auf die Bestimmungen des DSG zurückzugreifen.

Das Auskunftsrecht des Betroffenen nach § 26 DSG ist ein **höchstpersönliches Recht**, mit welchen nur der Betroffene den Auftraggeber iSd § 4 Z 4 DSG verpflichten kann, ihm Auskunft über die zu seiner Person verarbeiteten Daten zu geben.[44] Ein LBS-Provider hat auf Verlangen des Betroffenen Auskunft über die verarbeiteten Daten, ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen in allgemein verständlicher Form anzuführen.[45] Nachdem alle Daten unmittelbar nach Erbringung eines LBS gelöscht werden müssen, werden die Auskünfte von LBS-Providern im Allgemeinen nicht sehr ergiebig sein. Dies gilt nur beschränkt für Verkehrsdaten iSd § 92 Abs Z 4 TKG, welche für Zwecke der Verrechnung von Entgelten solange als unbedingt erforderlich gespeichert werden dürfen.

Auf Antrag des Betroffenen erkennt die **Datenschutzkommission** (DSK) über behauptete Verletzungen des Rechts auf Auskunft durch den Auftraggeber einer Datenanwendung.[46] Privatrechtliche Ansprüche (Unterlassungs- und Beseitigungsansprüche eines dem DSG widersprechenden Zustandes, Feststellungsklage) wegen Verletzung der Rechte auf Geheimhaltung, Richtigstellung oder Löschung sind vom Betroffenen auf dem Zivilrechtsweg vor **ordentlichen Gerichten** geltend zu machen.[47] Bei schuldhafter Verwendung von Daten entgegen den Bestimmungen des DSG hat der Betroffene ein Recht auf **Schadenersatz** nach § 33 DSG nach den allgemeinen Bestimmungen des bürgerlichen Rechts.[48]

D. Zweckbindungsgrundsatz

Die allgemeinen Regel zur Zulässigkeit der Verwendung von Daten ist § 7 Abs 1 DSG, welcher formuliert, dass Daten nur verarbeitet werden dürfen, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers

---

43) § 133 Abs 4 TKG.

44) Siehe auch die Verfassungsbestimmung des § 1 Abs 3 DSG.

45) Bezüglich der (Un-)Entgeltlichkeit der Auskunft und der Frist für die Erbringung der Auskunft siehe § 26 Abs 4 und 6 DSG.

46) § 31 Abs 1 DSG.

47) § 32 DSG.

48) Mehr zu den Konsequenzen bei Rechtsverletzungen in *Mayer-Schönberger*, Information und Recht, Vom Datenschutz bis zum Urheberrecht, Praxisbezogene Perspektiven für Österreich, Deutschland und die Schweiz (2001), 184.

gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen. Nach § 96 Abs 1 TKG dürfen Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten nur für Zwecke der Besorgung eines **Kommunikationsdienstes** (zB eines LBS) ermittelt oder verarbeitet werden.

Die Übermittlung dieser Daten darf nur erfolgen, soweit dies für die Erbringung jenes Kommunikationsdienstes, für den diese Daten ermittelt und verarbeitet worden sind, durch den Betreiber erforderlich ist. Jede andere Verwendung, beispielsweise zum Zweck der Vermarktung oder Bereitstellung von Diensten mit Zusatznutzen (zB LBS) darf nur mit einer jederzeit widerrufbaren Zustimmung erfolgen.[49]

Allgemein dürfen Daten dürfen nur übermittelt werden, wenn sie aus einer zulässigen Datenanwendung stammen, der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis im Hinblick auf den Übermittlungszweck glaubhaft macht und durch den Zweck der Übermittlung nicht die schutzwürdigen Geheimhaltungsinteressen des Betroffenen verletzt.[50]

E. Datenkategorien

1. Personenbezogene Daten

Personenbezogene Daten sind

„ [...] *Angaben über Betroffene* [Anm zB Nutzer von LBS], *deren Identität bestimmt oder bestimmbar ist; ,,nur indirekt personenbezogen" sind Daten für einen Auftraggeber* [Anm zB Mobilfunknetzprovider],[51] *Dienstleister* [Anm zB LBS-Provider][52] *oder Empfänger einer Übermittlung*

---

[49]) § 96 Abs 2 TKG.

[50]) § 7 Abs 2 DSG ; Abs 3 der selben Vorschrift verweist auf die Einhaltung der Qualitätsgrundsätze des § 6 DSG bei der Verwendung von Daten und auf die Grundrechtsbestimmung des im Verfassungsrang stehenden § 1 DSG (Verhältnismäßigkeitsgrundsatz). Für allgemeine Ausführungen zu § 7 DSG siehe *Dohr/Weiss/Pollirer*, Kommentar Datenschutzrecht – Datenschutzgesetz[2] (2000), 71ff; Die Weitergabe von Daten wird in Kapitel II/H behandelt.

[51]) Der für die Datenverarbeitung Verantwortliche ist Auftraggeber. Die Auftraggebereigenschaft einer natürlichen oder juristischen Person bleibt auch bei Datenüberlassung an einen Dritten für die Herstellung eines vom Auftraggeber bestellten Werkes erhalten. Bezüglich der Pflichten des Auftraggebers siehe *Jahnel*, Datenschutz im Internet – Rechtsgrundlagen, Cookies und Web-Logs, ecolex 2001, 84.

[52]) Aus Gründen der Einfachheit und um Verwechslungen zu vermeiden wird der Begriff „LBS-Provider“ für alle Unternehmen die potentiell ortsbezogene Leistungen anbieten verwendet; Dh für klassische Mobilfunkbetreiber, Mobile Virtuell Network Operators (MVNO), ASP und für Content Provider. Auf die Zulässigkeit der Datenweitergabe zwischen Mobilfunknetzbetreibern und Dritten wird in Kapitel II/H eingegangen.

[Anm zB ASP oder „Find a Friend" Partner][53] *dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann*."[54]

Diese Definition ist umständlicher formuliert, als die Definition der Allgemeinen Datenschutzrichtlinie, welche den Begriff „personenbezogene Daten" etwas klarer definiert als

„*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*".[55]

Personenbezogene Daten formen das **Eintrittstor zum allgemeinen Datenschutzrecht**. Datenschutzrecht ist daher nur von LBS-Provider zu beachten, die in der einen oder anderen Weise ein personenbezogenes Datum verwenden. Beispiele für personenbezogene Daten sind Daten, wie Name, Geburtsdatum, Adresse, Geschlecht, Einkommen, Vermögen, Lebensgemeinschaft, Intelligenzquotient, Umsatz, Gewinn, Beschäftigtenzahl und Werturteile.[56] Wie in Kapitel II/E/6 gezeigt wird, ist auch die, für ortsbezogene Dienste benötigte Mobile Station Integrated Services Digital Network Number (MSISDN) ein datenschutzrelevantes Datum.

2. Anonymisierte Daten und indirekt personenbezogene Daten

Anonymisierte Daten sind keiner Person zuordenbar und sind daher datenschutzrechtlich nicht relevant. Dieser allgemeine Grundsatz gilt auch für das sektorspezifische Datenschutzrecht des TKG und LBS. Typischer Weise ist die Identität einer Person durch anonymisierte Daten nicht bestimmbar. Daher sind datenschutzrechtliche Vorschriften grundsätzlich nur bei registrierten Mobilfunkteilnehmern anzuwenden. Ein LBS-Provider ist daher bei nicht registrierten Mobilfunkteilnehmern datenschutzrechtlichen Regelungen nicht unterworfen, wenn **niemand** auf deren Identität schließen kann. Nur durch eine freiwillige Registrierung wird der Prepaidkunde für jedermann identifizierbar.[57]

Anonymisierte Daten müssen von **indirekt personenbezogenen Daten** unterschieden werden. Indirekt personenbezogene Daten werden in irgendeiner

---

[53]) Der „Find a Friend" Dienst erlaubt es, andere Mobilfunkteilnehmer zu orten und sich orten zu lassen. Der Aufenthaltsort wird nach dem Einverständnis des Betroffenen bekanntgegeben. Die Ortung kann nur erfolgen, wenn sich vorher beide Teilnehmer für den Dienst registriert haben.

[54]) Artikel 4 Z 1 DSG.

[55]) Richtlinie 95/46/EG, Abl L 281 vom 23.11.1995, 31.

[56]) *Dohr/Weiss/Pollirer*, Kommentar Datenschutzrecht – Datenschutzgesetz 2000 samt Europarecht[2] (2002), 46.

[57]) *Pracher*, Datenschutz in der Telekommunikation in Forgo/Feldner/Witzmann/Dieplinger, Probleme des Informationsrechts (2003), 354.

Weise verschlüsselt. Der Verwender dieser Daten kann diese nur durch Einsatz ihm nicht zustehender legaler Mittel entschlüsseln.[58] Die Benutzer von nicht registrierten **Wertkartenmobiltelefonen** können grundsätzlich nicht bestimmt werden, sofern ihre Identität nicht auf andere Weise legal bestimmbar ist.[59] Ein LBS-Provider könnte sich beispielsweise auf illegale Weise bei einem Arbeitgeber, der seine Mitarbeiter mit nicht registrierten Wertkartentelefonen ausgestattet hat, eine Telefonliste besorgen. Erwägungsgrund 26 der Allgemeinen Datenschutzrichtlinie 95/46/EG legt nahe, den Gebrauch von nur indirekt personenbezogenen Daten unter erleichterten Bedingungen zuzulassen.[60]

3. Nicht-sensible Daten

Es macht Sinn, vor der Beschreibung der vier **sektorspezifischen Datenkategorien** (Standortdaten, Stammdaten, Inhaltsdaten und Verkehrsdaten) kurz auf personenbezogene Daten einzugehen, weil auf diesen Begriff und allgemein personenbezogene Daten wiederholt zurückgegriffen wird.[61]

Unter **nicht-sensiblen Daten** sind jene personenbezogenen Daten zu verstehen, die nicht von § 4 Z 2 DSG als **sensible Daten** aufgezählt werden. Die Generalklausel des § 8 Abs 1 DSG enthält eine nicht taxative Aufzählung von Tatbeständen, bei welchen die Verwendung von nicht-sensiblen Daten den schutzwürdigen Interessen des Betroffenen nicht entgegensteht.[62].

Der 12. Abschnitt des TKG, welcher **sektorspezifische Datenschutzvorschriften** beinhaltet, geht den allgemeinen Vorschriften des DSG als **lex specialis** vor. Die Datenkategorie des DSG „nicht-sensible Daten" ist bei die Erbringung von LBS nicht relevant.

Im folgenden werden die Datenkategorien des sektorspezifischen Datenschutzrechtes vorgestellt und auf deren Bedeutung für LBS-Provider

---

[58]) Ibid 41f und § 4 Z 1 DSG.

[59]) Die Telefonnummer eines nicht registrierten Prepaidkunden könnte beispielsweise in einer im Internet abrufbaren legalen Liste mit seinem Namen verknüpft sein.

[60]) 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 281 vom 23.11.1995, 31; Sondervorschriften bezüglich nur indirekt personenbezogener Daten: § 17 DSG (Erleichterung der Meldepflicht), § 12 Abs 3 DSG (internationaler Daten Verkehr) und §§ 8 Abs 2 und 9 Z 2 DSG (Verwendung – Nichtverletzung schutzwürdige Interessen!).

[61]) Siehe insbesondere Kapitel II/E/7 „Inhaltsdaten".

[62]) Nach Artikel 8 Abs 1 Z 4 DSG sind die schutzwürdigen Interessen des Betroffenen bei der Verwendung von nicht-sensiblen Daten insbesondere dann nicht verletzt, wenn „*überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern*". Schutzwürdige Geheimhaltungsinteressen sind insbesondere dann nicht verletzt, wenn die Verwendung der Daten zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich ist; Siehe Artikel 8 Abs 2 Z 4 DSG. Eine ähnlich liberale Regelung wäre aus Sicht der LBS-Provider auch im sektorspezifischen Datenschutzrecht begrüßenswert.

eingegangen. Dabei wird sich zeigen, dass bei wenigen ortsbezogenen Diensten Inhaltsdaten anfallen, die sensible Daten sehr ähnlich.[63]

4. **Verkehrsdaten**

Gemäß § 92 Abs 3 Z 4 TKG sind **Verkehrsdaten**

„*Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden*".

Verkehrsdaten, die zur Standortbestimmung eines Nutzers verarbeitet werden, sind Standortdaten iSd § 92 Abs 3 Z 6 TKG. Die enge Verbindung zwischen Verkehrs- und Standortdaten spiegelt sich im Titel des § 102 TKG wieder. Standortdaten unterscheiden sich von Verkehrsdaten vor allem durch den Zweck der Verarbeitung.[64]

Grundsätzlich sollen so wenig personenbezogene Daten wie möglich verarbeitet werden. Jede Tätigkeit im Zusammenhang mit der Bereitstellung elektronischer Kommunikationsdiensten, die über die Übermittlung einer Nachricht und die Fakturierung dieses Vorgangs hinausgeht, sollte auf **aggregierten Verkehrsdaten** basieren, die nicht mit Teilnehmern oder Nutzern in Verbindung gebracht werden können. Kann eine Tätigkeit nicht auf aggregierte Daten gestützt werden, so sollte sie als Erbringung eines Dienstes mit Zusatznutzen (**VAS**) angesehen werden, für welche die Einwilligung des Teilnehmers erforderlich ist.[65]

Folglich ist für den ortsbezogenen Dienst des „**Location Sensitive Billing**" und ähnliche Anwendungen die Zustimmung des Betroffenen einzuholen.

---

[63]) Kapitel II/E/7.

[64]) Standortdaten bestimmen den geographischen Standort des Nutzers meist genauer, als dies für die Weiterleitung von Nachrichten erforderlich ist. Die Identifizierung der Cell-ID ist jedenfalls zur Weiterleitung von Nachrichten notwendig; Kapitel I/B und II/E/5.

[65]) Erwägungsgrund 30 Richtlinie 2002/58/EG, ABl. L 201 vom 31.07.2002, 37

5. **Standortdaten**

§ 92 Abs 3 Z 6 TKG definiert **Standortdaten** als

„*Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografische Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben*".[66]

Erstmals bezieht sich eine Vorschrift des TKG auf ortsbezogene Dienste, allerdings ohne diese ausdrücklich zu nennen. Standortdaten iSd § 92 Abs 3 Z 6 TKG umfassen zunächst all jene Daten, die bei einer näheren Standortbestimmung eines Mobilfunkteilnehmers anfallen, als dies für die Zwecke der Weiterleitung von Nachrichten notwendig ist. Digitale Mobilfunknetze können in der Lage sein,

„ [...] *Standortdaten zu verarbeiten, die genauer sind als es für die Nachrichtenübertragung erforderlich wäre und die für die Bereitstellung von Diensten mit Zusatznutzen verwendet werden, wie z.B. persönliche Verkehrsinformationen und Hilfen für den Fahrzeugführer*".[67]

Als erstes Unterscheidungskriterium zwischen Standort- und Verkehrsdaten kann also formuliert werden, dass alle **genaueren Standortdaten** als normale Verkehrsdaten zur Nachrichtenübermittlung grundsätzlich als Standortdaten iSd § 92 Abs 3 Z 6 TKG anzusehen sind.

Weiters kommt es auf den **Zweck** der Verarbeitung von Verkehrsdaten an. Wird beispielsweise die einfache Cell-ID eines Nutzers, die eigentlich für die Weiterleitung einer Nachricht und zur Fakturierung erforderlich ist (Vermittlungsdatum), verarbeitet, um den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes anzugeben, ist dieses Datum als Standortdatum iSd § 92 Abs 3 Z 6 TKG zu qualifizieren. Daher ist jedes Datum, das in einem Kommunikationsnetz verarbeitet wird, um den Standort eines Nutzers für die Erbringung eines LBS oder eines anderes VAS anzugeben, als Standortdatum anzusehen. Wird ein solches Datum zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung

---

66) Die Begriffsbestimmungen orientieren sich an der 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 201 vom 31.07.2002, 37. Einige Begriffsbestimmungen wurden jedoch ergänzt, um den spezifischen Regelungen dieses Gesetzes zu entsprechen. Vorrang bei der Auslegung der Begriffe hat die zitierte Richtlinie. Standortdaten sind in aller Regel ein Spezialfall der Verkehrsdaten und werden in den meisten Fällen von den Regelungen über Verkehrsdaten abgedeckt. Zusätzliche Regelungen, bezogen auf den Standort des Teilnehmers stellt Artikel 9 der Datenschutzrichtlinie für elektronische Kommunikation auf. Diese Bestimmungen beziehen sich auf standortbezogene Mehrwertdienste und werden mit diesem Paragraphen umgesetzt; Siehe Erläuterungen zu §§ 92 und 102 TKG der Erläuterungen Regierungsvorlage TKG.

67) Erwägungsgrund 35 Richtlinie 2002/58/EG, ABl. L 201 vom 31.07.2002, 37

dieses Vorgangs verarbeitet, braucht keine Zustimmung eingeholt werden, weil es sich um ein Verkehrsdatum handelt.

Für die Erbringung ortsbezogener Dienste sind in einem ersten Schritt zur Standortbestimmung und Identifizierung des Teilnehmers grundsätzlich die Mobile Station Integrated Services Digital Network Number (**MSISDN)** und die **geographischen Daten zum Aufenthaltsort** des Betroffenen, erforderlich.[68] Durch die Kombination dieser beiden Daten ist der Standort einem Benutzer zurechenbar. Der Benutzer der Telekommunikationseinrichtung wird bestimmbar. Die MSISDN entspricht der Telefonnummer des Teilnehmers und wird daher im nächsten Kapitel II/B/7 „Stammdaten" behandelt.

Wie in Kapitel I/C/1/b dargelegt ist Richtlinie 2002/58/EG **technologieneutral** formuliert.[69] Durch welche Technologie der Standort der Telekommunikationsendeinrichtung, einfacher des Nutzers, für die Erbringung eines LBS ermittelt wird, spielt für rechtliche Qualifikationen keine Rolle. Es macht daher keinen Unterschied, ob der Standort des Nutzers zum Zweck der Erbringung eines LBS durch eine bereits gebräuchliche, auf dem Netz basierende Ortungsmethode, beispielsweise Triangulation (E-OTD oder OTDOA), oder durch eine neue satellitenbasierte Methode (A-GPS oder NA-GPS) festgestellt wird.[70] In jedem Fall sind die dabei anfallenden Daten als Standortdaten iSd § 92 Abs 3 Z 6 TKG zu qualifizieren.[71]

Gemäß § 102 TKG dürfen andere Standortdaten als Verkehrsdaten unbeschadet des § 98 TKG nur verarbeitet werden, wenn sie entweder **anonymisiert** sind oder der Benutzer oder Teilnehmer eine jederzeit **widerrufbare Einwilligung** gegeben hat.[72]

---

[68]) In einem zweiten Schritt werden diese Daten mit einem oder mehreren Inhaltsdaten verknüpft; Siehe Kapitel II/E/7.

[69]) Das kann auch an der Terminologie der Richtlinie erkannt werden. So ersetzen beispielsweise die Begriffe „Kommunikationsnetze" und „–dienste" die Begriffe „Telekommunikationsdienste" und „– netze". Das TKG ist daher auf **jede Übertragungsart** von Signalen betreffend elektronischer Nachrichten anzuwenden.

[70]) Bei der herkömmlichen Standortbestimmung wird der Standort des Benutzers im Netz durch die sogenannte Location Area Identification (**LAI**) ermittelt. Die LAI wird von der Basisstation zur Gebietskennung benutzt. Sie entsteht aus der Landes-, Netz- und Gebietskennzahl, dh Mobile Country Code (MCC), Mobile Network Code (MNC) und Location Area Code (LAC). Die LAI ist ein Standortdatum iSd § 92 Abs 3 Z 6 TKG. Beim Network Assisted Global Positioning System (NA-GPS) sind die, durch zwei Satelliten und das Netz ermittelten Koordinaten des Benutzerstandortes als Standortdaten anzusehen; Siehe auch Kapitel I/B und die erläuterten Abbildungen im Annex.

[71]) Der neue Rechtsrahmen stellt durch die Schaffung einer neuen Datenklasse „Standortdaten" klar, dass es sich bei geographischen Daten für LBS nicht um Verkehrsdaten handelt. Vor dem TKG war die Qualifikation dieser Daten strittig. Der Interpretationsspielraum war groß; Siehe *Köhler-Ludescher*, Location Based Services der Mobilfunkbetreiber im Lichte des neuen Kommunikations-Rechtsrahmens (2000), 95f.

[72]) § 98 TKG bezieht sich auf Auskünfte an Betreiber von Notrufzentralen und wird in Kapitel III behandelt; Bezüglich der Zustimmung siehe Kapitel II/G.

Im Falle einer Einwilligung zur Verarbeitung von Standortdaten durch den Nutzer hat dieser die Möglichkeit, die Verarbeitung von Daten für jede Übertragung einfach und kostenlos zeitweise zu **untersagen**.[73]

Das **Löschen** von Standortdaten wird nicht ausdrücklich geregelt. Nachdem die Datenkategorie „Standortdaten" allgemein als „*Andere Standortdaten als Verkehrsdaten*" bezeichnet wird und der Nahebezug zwischen diesen beiden Datenkategorien offensichtlich ist, muss die Regelung betreffend dem Löschen von Verkehrsdaten analog auf das Löschen von Standortdaten angewendet werden. Nach dieser Regelung müssen Verkehrsdaten nach Beendigung der Verbindung, bei LBS daher nach Beendigung des Dienstes, unverzüglich gelöscht oder anonymisiert werden.[74]

Die **Verarbeitung** von Standortdaten muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.[75] § 102 Abs 3 TKG statuiert in Anlehnung an § 9 der Datenschutzrichtlinie für elektronische Kommunikation einen strengen **Zweckbindungsgrundsatz** für die Verwendung von Standortdaten.[76]

Zusammenfassend kann gesagt werden, dass es vor allem auf den **Zweck der Datenverarbeitung** ankommt. Der Verarbeitungszweck entscheidet im Zweifel, ob es sich um ein Vermittlungsdatum handelt für dessen Verarbeitung grundsätzlich keine Zustimmung eingeholt werden muss, oder, ob ein Standortdatum gegeben ist, für dessen Verarbeitung die Zustimmung des Nutzers vorliegen muss.

6. **Stammdaten**

§ 92 Abs 3 Z 3 TKG definiert **Stammdaten** als

„*alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:*

a) Familienname und Vorname,

b) akademischer Grad,

c) Wohnadresse,

d) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,

e) Information über Art und Inhalt des Vertragsverhältnisses,

f) Bonität".

---

[73]) § 102 Abs 2 TKG; In der Praxis wird dies wohl durch einfachen Anruf oder signierte elektronische Nachricht geschehen können. Auch ein unsignierte SMS könnte als ausreichend angesehen werden, nachdem das Telekommunikationsendgerät durch die MSISDN einem Teilnehmer eindeutig zugerechnet werden kann, soweit dieser registriert ist.

[74]) § 99 Abs 1 TKG.

[75]) § 102 Abs 3 TKG.

[76]) Siehe dazu die allgemeinen Ausführungen in Kapitel II/D.

Die **MSISDN** ist jene Nummer eines Mobilfunkteilnehmers, die im Telefongerät gewählt wird, um den Teilnehmer dieser MSISDN anzurufen. Sie ist für die Erbringung von ortsbezogenen Diensten erforderlich und besteht aus country code (CC), national destination number (NDC) und subscriber number (SN).[77] Durch die MSISDN, welche, wie oben beschrieben, der Teilnehmernummer plus CC und NDC entspricht, wird der Betroffene mit zulässigen Mitteln bestimmbar. Dies gilt nicht oder nur beschränkt für nicht registrierte Mobilfunkteilnehmer.[78] Die MSISDN ist als Stammdatum iSd § 92 Abs 3 Z 3 zu sehen und darf nur zur „*Durchführung des Vertrages*" mit dem Teilnehmer verwendet werden, soweit das für die Erbringung des Kommunikationsdienstes erforderlich ist, die Daten anonymisiert wurden oder der Betroffene seine Zustimmung gegeben hat.[79]

Gemäß § 97 Abs 2 sind die Stammdaten spätestens nach Beendigung der vertraglichen Beziehungen mit dem Teilnehmer vom Betreiber zu **löschen**. Wird ein Stammdatum (die MSISDN) allerdings zur Erbringung eines LBS verwendet, ist § 99 Abs 1 TKG betreffen das Löschen bzw Anonymisieren von Verkehrsdaten analog anzuwenden. Nur durch das Löschen bzw Anonymisieren kann Datenmissbrauch mit Sicherheit verhindert werden.

7. **Inhaltsdaten**

Gemäß § 92 Abs 3 Z 5 TKG sind **Inhaltsdaten** die Inhalte übertragener Nachrichten. Eine **Nachricht** ist jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird.[80] Fraglich ist, wie das Wort "Nachricht" auszulegen ist. Umfasst es nur Nachrichten im engeren Sinn, wie zB E-Mails, oder bezieht sich „Nachricht" auf jeden Inhalt eines Telekommunikationsvorganges und ist deshalb weiter auszulegen? Bei einer weiteren Auslegung sind Content-Daten (bei „Find Next" Diensten zB das nächste Restaurant) unter § 92 Abs 3 Z 5 TKG zu subsumieren.

Die Informationen, wer, wann, welchen ortsbezogenen Dienst *mit welchem Inhalt* in Anspruch genommen hat, sind als Inhaltsdaten zu qualifizieren. Einer **weiten Auslegung** des Wortes „Nachricht" ist schon deshalb der Vorzug zu geben, weil die, bei der Erbringung von LBS anfallenden Inhaltsdaten nur auf diese Weise unter eine Datenkategorie des TKG zu subsumieren sind. Bei einer engeren Auslegung würden uU

---

77) Kennziffern von GSM, online: http://umtslink.at/cgi-bin/reframer.cgi?..//GSM/gsm_kennziffern.htm [Stand 10 Juli 2003].

78) Bezüglich nicht registrierter Mobilfunknetzteilnehmer siehe Kapitel II/B/2.

79) Siehe § 97 TKG, der außerdem die Änderung oder Beendigung des Vertragsverhältnisses, die Verrechnung der Entgelte, die Erstellung von Teilnehmerverzeichnissen und die Erteilung von Auskünften an Notrufträger erwähnt. § 92 Abs 3 Z 3 TKG enthält nach herrschender Auffassung eine **taxative Aufzählung** von Stammdaten; *Pracher*, Datenschutz in der Telekommunikation in Forgo/Feldner/Witzmann/Dieplinger, Probleme des Informationsrechts (2003), 355.

80) § 92 Abs 3 Z 5 TKG.

personenbezogene Daten nach dem DSG anfallen.[81] Um ein möglichst **hohes Datenschutzniveau** zu garantieren sind alle Inhaltsdaten bei LBS unter § 92 Abs 3 Z 5 TKG zu subsumieren.

Stammdaten (MSISDN) und Standortdaten (geographische Daten zum Standort des Benutzers, LAI) sind für die Standortbestimmung immer erforderlich. Bei fast allen LBS fallen auch Inhaltsdaten an.[82]

Inhaltsdaten dürfen nur **gespeichert** werden, sofern die Speicherung einen wesentlichen Bestandteil des Kommunikationsdienstes darstellt.[83] Diese Voraussetzung ist typischer Weise bei der Erbringung von ortsbezogenen Diensten erfüllt, für welche ein zusätzliches Inhaltsdatum erforderlich ist.

Die **Übermittlung und Verarbeitung** von Inhaltsdaten zum Zwecke der Bereitstellung von VAS bedarf nach § 96 Abs 2 TKG einer jederzeit widerrufbaren Zustimmung des Betroffenen.

Nach Wegfall der Gründe für die Speicherung hat der LBS-Provider die gespeicherten Daten unverzüglich zu **löschen**.[84]

Bei der Erbringung von wenigen LBS werden Inhaltsdaten verarbeitet, die **sensiblen Daten** iSd § 4 Z 2 DSG sehr ähnlich sind.

Nach § 4 Z 2 DSG sind 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.*"[85]

Bevor auf das Rechtsproblem „sensible Inhaltsdaten" eingegangen wird, muss untersucht werden, ob derartige Daten bei der Erbringung von ortsbezogenen Diensten potentiell anfallen können.[86] Dies ist beispielsweise der Fall, wenn bei einem „Find Next-"Dienst nach dem nächsten oder den

---

81) Bei einer engen Auslegung wäre zusätzlich nicht immer sichergestellt, dass der weniger strenge § 8 DSG zur Verarbeitung von nicht-sensible Daten zur Anwendung kommt, weil Inhaltsdaten nicht zwingend nicht-sensible Daten darstellen; Bezüglich nicht-sensiblen Daten siehe Kapitel II/E/3.

82) Inhaltsdaten fallen beispielsweise bei „Find Next"-Diensten an, wenn der Benutzer eines LBS angibt, was gefunden werden soll. Wird beispielsweise der nächste Bankomat, die nächste Tankstelle oder ein Freund gesucht, muss diese Information (Content) in Form einer Nachricht vom Benutzer des LBS zum LBS-Provider geschickt werden.

83) § 101 Abs 1 TKG.

84) Wieder ist § 99 Abs 1 TKG analog anzuwenden; Siehe Kapitel II/E/5.

85) Der Begriff „sensible Daten" wird durch Artikel 8 Abs 1 der Allgemeinen Datenschutzrichtlinie 95/46/EG vorgegeben; 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 281 vom 23.11.1995, 31.

86) Die nachstehende Absätze beschäftigen sich ausschließlich mit „sensiblen Inhaltsdaten" und der Frage, ob eine ausdrückliche Zustimmung zur Verwendung dieser Daten notwendig ist. Das Erfordernis der Zustimmung nach § 96 Abs 2 TKG bei „normalen Inhaltsdaten" ist unstrittig. Es bedarf dafür keiner zusätzlichen Voraussetzung.

nächsten Gebäuden einer Religionsgemeinschaft oder politischen Verbindung gesucht wird.

Durch die Verknüpfung von MSISDN, Standortdatum und Inhaltsdatum zu einem **Datenpaket**, das für die Erbringung des Dienstes erforderlich ist, wird der Benutzer des LBS auf legale Weise **bestimmbar**. Das jeweilige Datum ist ihm eindeutig zuordenbar, sofern er mit seiner Telefonnummer registriert ist. Eine unerlaubte Verküpfung von Daten durch den Auftraggeber (LBS-Provider) zur Identitätsfeststellung ist dafür nicht erforderlich.

Nach der Ansicht einer Autorin weisen die, bei ortsbezogenen Diensten anfallenden Daten per se keine unterschiedliche Sensibilisierungsqualität auf als andere Vermittlungsdaten, und stellen daher auch keine stärkere Gefährdung für das Persönlichkeitsrecht dar. Besonders schutzwürdige Daten würden bei LBS daher nicht anfallen.[87] Nach dieser Meinung müssten ortsbezogene Daten erst mit anderen Daten verknüpft werden, um qualifiziert auf beispielsweise eine politische Einstellung eines Betroffenen schließen zu können. Geographische Daten haben demnach nur nach einer unzulässigen Zusatzauswertung erhöhte Sensibilisierungsqualität.[88]

Diese Meinung ist für die MSISDN und die geographischen Daten zum Aufenthaltsort des Betroffenen, dh für die Daten, die jedenfalls für die Erbringung eines LBS erforderlich sind, zutreffend. Allein aus dem geographischen Standort eines Benutzers kann nicht auf ein sensibles Datum geschlossen werden. Der Umstand, dass eine Person zB aus dem Gebäude einer Religionsgemeinschaft einen ortsbezogenen Dienst in Anspruch nimmt, sagt noch nichts über die religiöse Einstellung dieser Person aus. Ein qualifizierter Schluss auf ein sensibles Datum (zB auf eine politische oder religiöse Einstellung) ist nicht möglich.[89]

Es muss zwischen **verschiedenen Kategorien von LBS** unterschieden werden. Bei Suchdiensten zu bestimmten „sensiblen Inhaltsdaten“ (zB Gebäude einer Religionsgemeinschaft, einer Partei, oder einer Örtlichkeit einer Gemeinschaft mit besonderen sexuellen Neigungen) ist zu differenzieren. Schon durch eine Abfrage fallen Inhaltsdaten an, die in Bezug auf den **Eingriff in die Privatsphäre** mit sensible Daten iSd § 4 Z 2 DSG verglichen werden können. Durch die MSISDN, welche im Datenpaket gemeinsam mit dem jeweiligen sensiblen Inhaltsdatum (zB „Lokal für sexuell anders Orientierte“) enthalten ist, wird der Benutzer dieses LBS bestimmbar. Es mangelt diesem Datum nicht an qualifizierter Aussagekraft. Der Schluss, dass beispielsweise grundsätzlich nur ein Mensch mit homosexueller Neigung Interesse am Standort der nächsten einschlägigen Örtlichkeit haben kann, ist logisch und hat

87) Die Autorin beschreibt den alten Rechtsrahmen; Siehe *Köhler-Ludescher*, Location Based Services der Mobilfunkbetreiber im Lichte des neuen Kommunikations-Rechtsrahmens (2000), 96ff.

88) Ibid.

89) Nachdem nach der Erbringung des LBS alle Daten unverzüglich gelöscht werden müssen, ist auf legale Weise nicht feststellbar, wie oft ein LBS von einem Ort aus in Anspruch genommen wurde. Auch bei mehrmaliger Inanspruchnahme fallen daher keine Inhaltsdaten an, die sensiblen Daten ähnlich sind.

qualifizierte Aussagekraft. Eine zusätzliche Datenauswertung ist für diese Erkenntnis nicht erforderlich.[90]

Bei „nicht-sensiblen Inhaltsdaten" stellt § 96 Abs 2 TKG klar, dass eine einfache Zustimmung für die Verwendung ausreichend ist.[91] Inhaltsdaten, welche die Voraussetzungen von sensiblen Daten iSd § 4 Z 2 DSG erfüllen, werden bei LBS kontextbedingt nicht allzu oft auftreten. Es ist fraglich, ob jemals ein ortsbezogener Dienst speziell für Menschen mit einer bestimmten religiösen oder politischen Einstellung erhältlich sein wird. Im Zuge einer umfassenden, akademischen Betrachtung dieses Themas sollte dieser Aspekt jedoch nicht außer Acht gelassen werden.

Der 12. Abschnitt des TKG bestimmt nichts über die Verwendung von sensiblen Daten. Die sektorspezifischen Bestimmungen des TKG gehen den allgemeinen Bestimmungen des DSG vor. Der bei LBS anfallenden Content ist daher, wie oben gezeigt, unter § 92 Abs 3 Z 5 TKG zu subsumieren.

Die Bestimmungen der Richtlinie 2002/58/EG, auf welchen Kapitel 12 des TKG beruht, stellen eine **Detaillierung und Ergänzung** der Richtlinie 95/46/EG dar.[92] Auf letzterer Richtlinie beruht das DSG. Richtlinie 2002/58/EG

„*zielt durch **Ergänzung** der Richtlinie 95/46/EG darauf ab, die Grundrechte natürlicher Personen, insbesondere ihr **Recht auf Privatsphäre**, sowie die berechtigten Interessen juristischer Personen zu schützen*".[93] Daher soll durch die datenschutzrechtlichen Bestimmungen des TKG ein möglichst **hohes Datenschutzniveau** erreicht werden. Das Datenschutzniveau muss zumindest dem des DSG entsprechen, nachdem das TKG eine Ergänzung des DSG darstellt.[94]

Bei Inhaltsdaten, die nach dem DSG als sensible Daten iSd § 4 Z 2 DSG zu qualifizieren wären, liegt das Schutzniveau des DSG über dem Schutzniveau des TKG, weil § 9 DSG uA eine „ausdrückliche Zustimmung"

---

90) Anderer Ansicht: *Köhler-Ludescher*, Location Based Services der Mobilfunkbetreiber im Lichte des neuen Kommunikations-Rechtsrahmens (2000), 98. Diese Autorin geht davon aus, dass eine zusätzliche und daher durch den Zweckbindungsgrundsatz verbotene Datenauswertung notwendig wäre, um auf sensible Daten schließen zu können. ME nach ist diese Aussage nicht für alle LBS richtig und muss besonders bei „Find Next-"Diensten differenziert werden. Dies veranschaulicht das oben formulierte Beispiel.

91) Siehe Kapitel II/G.

92) Artikel 1 Abs 2 Richtlinie 2002/58/EG, ABl. L 201 vom 31.07.2002, 37, ABl. L 201 vom 31.07.2002, 37.

93) Erwägungsgrund 12 Richtlinie 2002/58/EG, ABl. L 201 vom 31.07.2002, 37, ABl. L 201 vom 31.07.2002, 37. Siehe auch Erwägungsgrund 46 „*Die Richtlinie 95/46/EG gilt unabhängig von der verwendeten Technologie für alle Formen der Verarbeitung personenbezogener Daten*".

94) So bezieht sich § 95 TKG uA wohl aus diesem Grund auf § 14 DSG. Gemäß § 92 Abs 1 TKG ist das DSG anzuwenden, soweit das TKG nichts anderes bestimmt. Diese beiden Bestimmungen gehen von davon aus, dass der datenschutzrechtliche Standard des allgemeinen Datenschutzrechtes im sektorspezifischen Datenschutzrecht erreicht werden muss.

für deren Verwendung verlangt. Das sektorspezifische Datenschutzrecht muss aber das **gleiche Schutzniveau** aufweisen, wie das allgemeine Datenschutzrecht. Dies auch deshalb, weil die **Privatsphäre** bei elektronischen Kommunikationsdiensten einem besonderem **Risiko** ausgesetzt ist.[95] Daher ist beispielsweise eine Interessenabwägung wie in § 8 Abs 1 Z 4 DSG im sektorspezifischen Datenschutzrecht nicht vorgesehen. Eine Zustimmung zur Verwendung von Daten ist daher von wenigen Ausnahmen abgesehen (§ 98 TKG) immer erforderlich. Diese Argumente machen klar, dass auch „sensible Inhaltsdaten" nur mit ausdrücklicher Zustimmung nach § 9 Z 6 DSG verwendet werden dürfen. Dem Betroffen muss genauso wie im allgemeinen Datenschutzrecht durch seine ausdrückliche Zustimmung bewusst werden, auf welches Risiko er sich einlässt. § 9 Z 6 DSG ist daher **analog** auf „sensible Inhaltsdaten" iSd § 92 Abs 3 Z 5 TKG anzuwenden.[96] In den nächsten beiden Absätzen wird gezeigt, dass dies die effiziente Erbringung von LBS nicht behindert.

Nach einhelliger Auffassung ist eine ausdrückliche datenschutzrechtliche Zustimmung iSd § 9 Z 6 **nicht konkludent** zulässig.[97] Für die Gestaltung einer ausdrücklichen Zustimmung ist auf das **Rundschreiben des BKA-VD**, 810.008/1-V/1a/85 vom 10.8.1985 zu verweisen. Daraus ergibt sich, dass eine ausdrückliche Zustimmung niemals als Bestandteil von AGB gegeben werden kann. Vielmehr muss die Zustimmung getrennt von sonstigen vertraglichen Vereinbarungen erteilt werden. Die Zustimmungserklärung muss gesondert unterfertigt werden oder muss sich vom **übrigen Text abheben**. Weiters muss eine Zustimmungserklärung iSd § 9 Z 6 DSG den Zweck der Datenverarbeitung, die Datenarten, die Benennung der Übermittlungsempfänger, einen ausdrücklichen Hinweis auf die Widerrufsmöglichkeit, ausreichend Informationen über die Übermittlungszwecke beinhalten.[98] Diese „Verhaltensregeln" sind für LBS-Provider kein großes Hindernis und können in der Praxis relativ leicht erfüllt werden.

Eine praktikable Lösung liegt mE im Abschluss eines **Rahmenvertrages**, in dem eine ausdrücklicher Zustimmung entsprechend den Anforderungen des oben zitierten Rundschreibens des BKA-VD formuliert wird.[99] Die Einwilligung des Nutzers oder Teilnehmers kann in *„jeder geeigneten Weise gegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck kommt, die sachkundig und in freier Entscheidung*

---

95) Siehe Erwägungsgrund 6 und 7 der Richtlinie 2002/58/EG.

96) Die Nicht-Regelung der ausdrücklichen Zustimmung im TKG stellt eine planwidrige Lücke dar, die nur durch Analogie geschlossen werden kann.

97) *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 145; *Dohr/Weiss/Pollirer*, Kommentar Datenschutzrecht[2], 85ff.

98) Ein Hinweis auf die Übermittlungszwecke reicht aus, wenn diese eindeutig aus dem Text hervorgeht, von dem die Zustimmungserklärung ein hervorgehobener Teil ist. Für weitere Hinweise zum Rundschreiben des BKA-VD, 810.008/1-V/1a/85 vom 10.8.1985 siehe *Dohr/Weiss/Pollirer*, Kommentar Datenschutzrecht[2], 56.

99) Rundschreiben des BKA-VD, 810.008/1-V/1a/85 vom 10.8.1985.

erfolgt".[100] Wie in Kapitel II/G gezeigt, ist ein Rahmenvertrag bezüglich der Zustimmung zur Verarbeitung von Daten bei der Inanspruchnahme eines LBS ohnehin die effizienteste Lösung. Bei den wenigen LBS, welche „sensible Inhaltsdaten" verarbeiten, sind die oben angeführten Voraussetzungen für eine „ausdrückliche Zustimmung" (separate Unterfertigung, Hervorhebung im Text, usw) ohne viel Aufwand zu erfüllen. Durch eine „ausdrückliche Zustimmung" bei „sensiblen Inhaltsdaten" wird das Datenschutzniveau des TKG auf jenes des DSG gebracht und der LBS-Nutzer vor möglichen schweren Eingriffen in seine Intimsphäre entsprechend gewarnt.

F. Informationspflichten und Betriebssicherheit

Die Informationspflichten bei der Verwendung von Daten wurden durch die Datenschutzrichtlinie für elektronische Kommunikation verstärkt, was sich in § 96 TKG niederschlägt. Die Frage, ob der Teilnehmer oder der Nutzer eines Dienstes zu informieren ist, hängt von der Art des Rechtsverhältnisses zum Betreiber ab. Die meisten Informationspflichten werden nur gegenüber dem Teilnehmer und nicht dem Nutzer relevant sein, weil die meisten Informationen über das bestehende Vertragsverhältnis aufklären. Weiters ist meist der Teilnehmer bestimmbar.

Jedenfalls ist der Anbieter eines ortsbezogenen Dienstes verpflichtet, den Teilnehmer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er ermittelt, verarbeitet und übermittelt, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Diese Information hat auch auf das Recht hinzuweisen, die Verarbeitung zu verweigern. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein Kommunikationsnetz ist oder, soweit dies unbedingt erforderlich ist, um einen vom Teilnehmer oder Benutzer ausdrücklich gewünschten Dienst zur Verfügung zu stellen. Informationen haben in geeigneter Form, insbesondere im Rahmen **allgemeiner Geschäftsbedingungen** und spätestens bei Beginn der Rechtsbeziehungen zu erfolgen.[101] Den Informationspflichten kann auch in einem **Rahmenvertrag** nachgekommen werden. Diese Informationen müssen daher nicht bei jeder Inanspruchnahme eines LBS bereitgestellt werden. Es ist daher ausreichend am Anfang der Vertragsbeziehung, nur einmal alle Informationen über mögliche Datenverwendungsvorgänge bereitzustellen. Aufgrund der **Verschiedenartigkeit von LBS**, die beispielsweise eine unterschiedlich lange Speicherung der Daten notwendig macht, sollte vor

---

[100]) Erwägungsgrund 17 Richtlinie 2002/58/EG, ABl. L 201 vom 31.07.2002, 37. In der Begründung des deutschen Referentenentwurfes zum TKG wird ausdrücklich ausgeführt, dass es nicht erforderlich ist, vor jeder Inanspruchnahme eines Dienstes in die Verarbeitung einzuwilligen. Begründung zum Referenzentwurf zum (deutschen) TKG-E 2003, online: http://www.tkrecht.de/tkg_novelle/2003/material/Begruendung-RefE_TKG_Stand_30-04-03.pdf [Stand: 14. Juli 2003].

[101]) § 96 Abs 3 TKG.

Inanspruchnahme eines anderen LBS zumindest auf datenschutzrelevante Unterschiede hingewiesen werden.

LBS-Provider sind verpflichtet, entsprechend geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit ihrer Dienste zu gewährleisten. Weiters sind die Teilnehmer an einem Kommunikationsdienst entsprechend zu informieren, wenn ein **besonderes Risiko** der Verletzung der Sicherheit besteht.[102]

G. Zustimmung

Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten dürfen nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden.[103] Die Verwendung dieser Daten zum Zwecke der Bereitstellung von ortsbezogenen Diensten oder einer sonstigen Übermittlung darf nur auf Grund einer **jederzeit widerrufbaren Zustimmung** des Betroffenen erfolgen.[104] Auch das Verknüpfen von Inhaltsdaten (zB nächste Apotheke) mit Stamm- (MSISDN) und Standortdaten ist eine Form der Verarbeitung und bedarf der Zustimmung iSd § 96 Abs 2 TKG. Im Folgenden wird auf die Form und den Inhalt dieser Zustimmung näher eingegangen.[105]

Eine Interessenabwägung zwischen den schutzwürdigen Interessen des Nutzers auf der einen Seite und den berechtigten Interessen des LBS-Providers auf der anderen Seite ist, anders als in § 8 Abs 1 Z 4 DSG, im sektorspezifischen Datenschutzrecht des TKG nicht vorgesehen. Durch die Zustimmung soll sich der Nutzer eines ortsbezogenen Dienstes über die potentiellen Gefahren eines Eingriffs in seine Privatsphäre durch die Verarbeitung von Standortdaten im Klaren sein.

Meist ist nur der Teilnehmer iSd § 3 Z 19 TKG Betroffener iSd § 96 TKG. Der registrierte Teilnehmer ist durch die MSISDN bestimmbar. Ein Nutzer iSd § 3 Z 14 TKG, der einen Dienst in Anspruch nimmt, ohne registriert zu sein, braucht seine Zustimmung nicht zu geben.[106]

Im Rahmen der **informationellen Selbstbestimmung** kann der Betroffene, seine Geschäftsfähigkeit vorausgesetzt (§ 865 ABGB), seine

---

[102]) Artikel 4 2002/58/EG, ABl. L 201 vom 31.07.2002, 37 und § 95 TKG, der in Bezug auf Datensicherheitsmaßnahmen auf § 14 DSG verweist.

[103]) Zur Erbringung eines ortsbezogenen Dienstes wird immer ein Stammdatum (MSISN) mit einem Standortdatum (zB LAI oder Koordinaten bei A-GPS) verknüpft. Meist wird ein Inhaltsdatum aus einer Datenbank hinzugefügt (zB der nächste Bankomat). Alle drei Daten werden zu einem Datenpaket verknüpft.

[104]) § 96 Abs 2 TKG stellt nunmehr klar, dass alle Daten mit Zustimmung des Betroffenen für die Erbringung von Diensten mit Zusatznutzen verarbeitet werden dürfen.

[105]) Bezüglich der Besonderheiten der „ausdrücklichen Zustimmung" nach § 9 Z 6 DSG bei der Verarbeitung von sensiblen Daten siehe Kapitel II/B/8.

[106]) Bei einem nicht registrierten Nutzer fallen bei der Bereitstellung von LBS meist anonymisierte Daten an, die datenschutzrechtlich nicht relevant sind; Siehe Kapitel II/E/2.

Beziehungen zur Umwelt nach seinem Willen gestalten.[107] Weiters muss zur Geschäftsfähigkeit die Einwilligung gemäß § 869 ABGB frei, ernstlich, bestimmt und verständlich erklärt werden. [108]

Bezüglich der Freiheit, Ernstlichkeit und Verständlichkeit der Erklärung werden im Allgemeinen keine besonderen Probleme auftreten.[109] Der **Bestimmtheitsgrundsatz** schließt eine allumfassende Zustimmung des Betroffenen zur Verarbeitung von Daten zum Zwecke der Bereitstellung von ortsbezogenen Diensten aus. Wie in Kapitel I/A gezeigt, gibt es eine fast unüberschaubare Anzahl ortsbezogener Dienste, mit unterschiedlichsten Inhalten. Für unterschiedliche **Dienstekategorien**, sind neben der MSISDN (Stammdatum) und den geographischen Daten zum Nutzerstandort jeweils andere Inhaltsdaten erforderlich. Eine allgemeine Formulierung der Zustimmungserklärung wie:

„*Ich stimme der elektronischen Verarbeitung meiner personenbezognen Daten zu*“,

wäre nicht hinreichend bestimmt. Es ist allerdings möglich in einem **Rahmenvertrag** oder in **allgemeinen Geschäftsbedingungen** zur Verwendung von personenbezogenen Daten zuzustimmen.[110] Eine Zustimmungserklärung zur Verarbeitung von personenbezogenen Daten für jede Dienstekategorie (zB „Tracking-“Dienst und „Location Based-Advertising“) ist aufgrund des Bestimmtheitsgrundsatzes erforderlich. Jedenfalls muss auf die datenschutzrelevanten Unterschiede zwischen

---

107) Das Recht auf informationelle Selbstbestimmung ist ein Teil des allgemeinen Persönlichkeitsrechtes nach § 16 ABGB; *Barta*, Wissenschaft und Verantwortlichkeit (1994), 89f. Das Recht auf informationelle Selbstbestimmung bestimmt die dritte Generation der Datenschutzrechte. Die Vorstellung vom Einsatz dieses Rechtes als Abwehrrecht wurde vom Recht auf Privatsphäre zurückgedrängt, Abwehrrechte wurden zu Gestaltungsrechten transformiert. Die vierte Generation des Datenschutzes versucht eine verschuldensunabhängige Haftung für Rechtsverletzungen durch Informationsverarbeitung zu installieren. Man spricht von „*holistischen und sektoralen Perspektiven*“; *Mayer-Schönberger*, Information und Recht, Vom Datenschutz bis zum Urheberrecht, Praxisbezogene Perspektiven für Österreich, Deutschland und die Schweiz (2001), 122.

108) Dabei sind die Regeln über verborgene oder gröblich benachteiligende Vertragsklauseln nach § 879 ABGB zu beachten; Siehe *Lechner* in Schweighofer/Menzel/Kreuzbauer, IT in Recht und Staat – Aktuelle Fragen der Rechtsinformatik (2002), 354.

109) Verständlich ist grundsätzlich auch eine Erklärung, die via Internet und/oder durch ein Mobilfunkendgerät abgegeben wird, nachdem die Einwilligung in jeder geeigneten Weise gegeben werden kann, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck kommt, die sachkundig und in freier Entscheidung erfolgt. Hierzu zählt auch das Markieren eines Feldes auf einer Internet Website; Erwägungsgrund 32, RL 2002/58/EG, ABl. L 201 vom 31.07.2002, 37.

110) In der Begründung zu § 93 (Standortdaten) des Referenzentwurfes zum deutschen TKG wird ausgeführt, dass es nicht erforderlich ist, vor jeder Inanspruchnahme eines Dienstes einzuwilligen. „*Ausreichend ist eine Einwilligung z.B. in einem Rahmenvertrag oä*“; siehe Begründung zum Referenzentwurf zum (deutschen) TKG-E 2003, online: http://www.tkrecht.de/tkg_novelle/2003/material/Begruendung-RefE_TKG_Stand_30-04-03.pdf [Stand: 14. Juli 2003].

verschiedenen Kategorien von LBS bei der Datenverarbeitung hingewiesen werden. Die Zustimmungserklärung muss die übermittelten Datenkategorien, deren Empfänger und den Zweck der Übermittlung bezeichnen.

Inhaltsdaten, die sensiblen Daten iSd § 4 Z 2 DSG darstellen, dürfen, wie in Kapitel II/E/7 dargelegt, nur durch „ausdrückliche Zustimmung" verarbeitet werden. Dem Betroffenen muss bei der Zustimmung zur Verarbeitung von „sensiblen Inhaltsdaten" besonders bewusst sein, dass er dem LBS-Provider uU sehr intime Daten seiner Privatsphäre anvertraut.

Eine Zustimmungserklärung zur Datenverarbeitung/-übermittlung darf nicht im „Kleingedruckten" stehen, weil der Betroffene dort damit nicht rechnen muss.[111]

Es ist zu empfehlen in Allgemeinen Geschäftsbedingungen oder in einem Rahmenvertrag (zB Anmeldeformular für ortsbezogene Dienste)

- die einzelnen Dienstkategorien und deren datenschutzrechtliche Unterschiede genau zu beschreiben,
- die jeweils verarbeiteten Daten genau zu beschreiben,
- den Zweck der Verarbeitung/Übermittlung von Daten zu erklären
- gegebenenfalls genau anzuführen, an wen und zu welchem Zweck die Daten weitergegeben werden, und
- eine separate und beweisbare Zustimmung für jede Dienstekategorie einzuholen.[112]

Die Zustimmung kann auch **konkludent** erklärt werden.[113] Daher könnte man argumentieren, dass bei der Inanspruchnahme eines ortsbezogenen Dienstes durch einen Betroffenen die Zustimmung zur Verwendung von personenbezogenen Daten für die Erbringung des Dienstes jedes Mal konkludent gegeben wird. Auch die, in § 96 Abs 3 TKG formulierten Informationspflichten stehen einer konkludenten Zustimmung nicht entgegen. Allerdings wird nach österreichischer Rechtsprechung eine wirksame Zustimmung nur vorliegen, wenn der Betroffene weiß, welche seiner Daten zu welchem Zweck verwendet werden sollen.[114] Ein Hinweis auf dem Display des Mobiltelefons des Betroffenen bezüglich der verwendeten Daten und dem Verarbeitungszweck würde **Erklärungsbewusstsein** schaffen. Ohne Hinweis ist dem Betroffenen nach österreichischer Rechtssprechung die Tragweite seiner konkludenten Einwilligung nicht bewusst. Nachdem eine Aufklärung über die oben erwähnten Umstände am Display eines Mobiltelefons unrealistisch ist, wird die Einholung der Zustimmung in Rahmenverträgen oder AGBs die praktikablere Lösung darstellen.

---

111) OGH 27.1.1999, 7 Ob 170/98w.

112) Eine E-Signatur wäre eine sichere und praktikable Form der Zustimmungserklärung.

113) *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz – Datenschutzgesetz, Verordnungen, datenschutzrechtliche Bestimmungen, mit ausführlichen Erläuterungen (2000), 125 und *Dammann/Simitis*, EG-Datenschutzrichtlinie (1997), 115.

114) OGH 22.3.2001, 4 Ob 28/01y.

Grundsätzlich könnte die Zustimmungserklärung über SMS, E-Mail oder sonst in einem, über das Mobiltelefon auszufüllenden Formular eine Zukunftslösung sein. Es muss allerdings möglich sein den oben angeführten Voraussetzungen für eine gültige Zustimmung im mobilen Kommunikationsumfeld zu entsprechen. Informationen und Verträge im Volltext könnten durch einen Link für den Betroffenen abrufbar gemacht werden. Richtlinie 2002/58/EG steht modernen Arten der Zustimmungserklärung positiv gegenüber, indem Erwägungsgrund 17 formuliert:

„*Die Einwilligung kann in jeder geeigneten Weise gegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck kommt, die sachkundig und in freier Entscheidung erfolgt; hierzu zählt auch das Markieren eines Feldes auf einer Internet-Website*".

Im Lichte des neunen Rechtsrahmens scheint die Zustimmung zur Datenverarbeitung vor der jeweiligen Inanspruchnahme eines LBS nicht mehr realistisch. Das Erfordernis einer jeweiligen Zustimmung vor der Inanspruchnahme eines LBS würde den kommerziellen Erfolg von ortsbezogenen Diensten gefährden.[115]

Der **Referentenentwurf zum deutschen TKG** geht auf die Einwilligung zur Verarbeitung von Daten näher ein als sein österreichisches Pendant. So formuliert § 89 des Referentenentwurf zum deutschen TKG ausdrücklich, dass die Einwilligung auch elektronisch erklärt werden kann, wenn der Diensteanbieter sicherstellt, dass die Einwilligung auf einer eindeutigen und bewussten Handlung des Teilnehmers oder Nutzers beruht, die Einwilligung protokolliert wird, der Teilnehmer oder Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und der Teilnehmer oder Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. ME ist die Einwilligung dem Teilnehmer nur mit einer elektronischen Signatur eindeutig zurechenbar. Bisweilen sind elektronische Signaturen bekanntlich gering verbreitet, sodass dieser Vorschrift zumindest in näherer Zukunft wenig Anwendungsspielraum zukommen dürfte.

H. Datenweitergabe

Ortsbezogene Dienste werden von Mobilfunkbetreibern selbst und vor allem von Dritten, meist von (ASP), durchgeführt und betreut.[116] Die Weitergabe von Daten spielt daher in der Praxis eine wichtige Rolle.

Grundsätzlich sollten so wenig personenbezogene Daten wie möglich übermittelt werden.[117] Können die Daten an einen oder mehrere Dritte

115) Es gibt allerdings Stimmen, die darauf hinweisen, dass eine allgemeinere Zustimmung mangels Bestimmtheit der Datenverarbeitungstatbestände möglicherweise unwirksam wäre, da der Nutzer nicht ausreichend konkret den Zweck der Datenverarbeitung erkennen könnte; *Hellmich*, MMR 2002, 156.

116) Neben ASP können solche Unternehmen auch als Portal-Betreiber oder Content-Provider bezeichnet werden. Aus Gründen der Einfachheit und um Verwechslungen zu vermeiden wird im Folgenden nur der Terminus ASP verwendet.

weitergegeben werden, so muss der Teilnehmer über diese Möglichkeit und über den Empfänger oder die Kategorien möglicher Empfänger unterrichtet werden. Voraussetzung für die Weitergabe ist, dass die Daten nicht für andere Zwecke als diejenigen verwendet werden, für die sie erhoben wurden. Wünscht derjenige, der die Daten beim Teilnehmer erhebt, oder ein Dritter, an den die Daten weitergegeben wurden, diese Daten zu einem weiteren Zweck zu verwenden, so muss entweder der ursprüngliche Datenerheber oder der Dritte, an den die Daten weitergegeben wurden, die erneute Einwilligung des Teilnehmers einholen.[118]

Gemäß § 96 Abs 2 TKG ist die Übermittlung von Daten an Dritte bei der Erbringung von LBS nur zulässig, wenn diese **erforderlich** ist. Weiters ist die jederzeit widerrufliche **Zustimmung** des Betroffenen einzuholen.[119]

Das TKG formuliert in § 96 Abs 1 und 2 eindeutig, dass alle Datenkategorien mit Zustimmung des Betroffenen weitergegeben werden können. Die Zweifel bezüglich Stammdaten sind somit ausgeräumt.

1. Räumlicher Anwendungsbereich

Die Übermittlung von Daten ins Ausland ist für LBS-Provider und Telekommunikationsunternehmen im Allgemeinen besonders wichtig, zumal sich sowohl ihre Kunden, als auch ihre Geschäftspartner (ASP, Content-Provider) im Ausland befinden können.

Der 12. Abschnitt des TKG und das DSG sind nach § 3 DSG iVm § 92 Abs 1 TKG auf jede Datenverwendung in Österreich anzuwenden. Neben dem **Territorialitätsprinzip** gilt das **Sitzstaatprinzip** innerhalb der EU. Für einen LBS-Provider mit Sitz in einem EU-MS ist immer der Ort der Niederlassung der maßgebliche Anknüpfungspunkt für die Frage des anwendbaren Rechts. Für LBS-Provider mit einem Sitz außerhalb der EU, ist der Ort der Datenverarbeitung der Anknüpfungspunkt. Liegt dieser in Österreich, ist österreichisches Datenschutzrecht anzuwenden. Die bloße Durchfuhr von personenbezogenen Daten durch einen MS ist ausgenommen.[120]

2. Übermittlung von Daten ins Ausland

Grundvoraussetzung für die Zulässigkeit der Datenübermittlung ins Ausland ist die Rechtmäßigkeit der Datenanwendung im Inland. Grundsätzlich ist nach § 13 DSG eine Genehmigung bei der DSK einzuholen.[121]

Der **freie Verkehr** von personenbezogenen Daten (auch in der elektronischen Kommunikation) innerhalb der Gemeinschaft soll sowohl durch

---

117) Erwägungsgrund 30 Richtlinie 2002/58/EG, ABl. L 201 vom 31.07.2002, 37.

118) Erwägungsgrund 39 Richtlinie 2002/58/EG, ABl. L 201 vom 31.07.2002, 37.

119) Die Ausführungen bezüglich der Zustimmung des Betroffenen in Kapitel II/G gelten auch für dieses Kapitel.

120) *Schaar*, Datenschutz im Internet, Die Grundlagen (2002), 270ff. und *Jahnel*, Das Datenschutzgesetz 2000. Wichtige Neuerungen, wbl 2000, 49.

121) §§ 7 DSG; Für näher Ausführungen siehe *Jahnel*, Datenschutzrecht in Jahnel/Schramm/Staudegger, Informatikrecht[2] (2003), 254f.

Richtlinie 95/46/EG als auch durch Richtlinie 2002/58/EG gewährleistet werden.[122] § 12 DSG formuliert, dass der Datenverkehr in EU-MS **genehmigungsfrei** ist.

Der Verkehr personenbezogener Daten in **Drittländer** ist grundsätzlich gemäß Art 25 der allgemeinen Datenschutzrichtlinie 95/46/EG zulässig, wenn im jeweiligen Land ein **angemessenes Datenschutzniveau** gewährleistet ist. Nach drei Entscheidungen der Kommission ist ein angemessenes Datenschutzniveau derzeit in der **Schweiz, Ungarn** und **Kanada** gegeben.[123] Soweit der Datenverkehr mit dem Ausland nicht gemäß § 12 DSG genehmigungsfrei ist, hat der Auftraggeber vor der Übermittlung oder Überlassung von Daten in das Ausland eine Genehmigung der DSK (§§ 35 ff) einzuholen.[124]

Die Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in Drittländer, die **kein angemessenes Schutzniveau** gewährleisten können, ist zulässig, wenn bestimmte Garantien vorliegen. Solche Garantien können durch besondere Vertragsklauseln gewährleistet werden.[125] Die Kommission hat in ihrer Entscheidung 2001/491/EG **Standardvertragsklauseln** für die Übermittlung personenbezogener Daten in Drittländer geschaffen.[126] Standardvertragsklauseln sollen den notwendigen Strom personenbezogener Daten zwischen der EU und Drittländern ohne unnötige Belastung der Wirtschaftsakteure aufrechterhalten. Durch die Aufnahme von Standardvertragsklauseln wird die rechtmäßige Übermittlung von personenbezogenen Daten in Drittländer erheblich erleichtert. Die Standardvertragsklauseln sind praktisch unterschriftsreif formuliert. Die

---

[122]) Artikel 1 2002/58/EG, ABl. L 201 vom 31.07.2002, 37 und Erwägungsgründe 7, 8 und 9 der Richtlinie 95/46/EG, Abl L 281 vom 23.11.1995, 31.

[123]) Entscheidung der Kommission 2000/519/EG vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in Ungarn, ABl L 215 25.08.2000, 4; Entscheidung der Kommission 2000/518/EG vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz ABl L 215 25.08.2000, 1 und Entscheidung der Kommission 2002/2/EG vom 20. Dezember 2001gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet, Abl L 2 04.01.2002, 13.

[124]) § 13 Abs 1 DSG; Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen binden. Für weiter Ausführung siehe § 13 Abs 2 DSG.

[125]) Artikel 26 Abs 2 Richtlinie 95/46/EG.

[126]) Artike 26 Abs 4 Richtlinie 95/46/EG ermächtigt die EK zu befinden, dass Standardvertragsklauseln ausreichende Garantien für eine Datenübermittlung in Drittländer nach § 26 Abs 2 Richtlinie 95/46/EG bieten können; Entscheidung der Kommission 2001/497/EG vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG, Abl. L 181 vom 04.07.2001, 19.

Parteien müssen nur die persönlichen Daten sowie die Einzelheiten der Übermittlung (Datenkategorien, Zweck der Übermittlung) ergänzen. Die Klauseln können in einer Anlage einem Vertrag angefügt werden.[127] Der Datenexporteur (LBS-Provider) muss Anfragen der betroffenen Person (des Nutzers) und der DSK beantworten. Ein Kopie des Vertrages muss dem Betroffenen ausgehändigt werden. Der Datenimporteur (ASP) verpflichtet sich uA Anfragen seines Vertragspartners bzw des Betroffenen zur Verarbeitung von Daten zu beantworten. Weiters muss der Datenimporteur eine Prüfung der Datenverarbeitung zulassen.[128] Der Betroffene kann einen Großteil der in den Klauseln festgelegten Pflichten geltend machen.[129] Diese Bestimmungen macht die Standardvertragsklauseln zu **einem Vertrag zu Gunsten Dritter** iSd § 881 Abs 2 ABGB.[130] Eine **gesamtschuldnerische Haftung** der Parteien für Schäden des Betroffenen und der Umstand, dass sich die Parteien nur von der Haftung befreien können, wenn sie nachweisen, dass keiner von ihnen für die Verletzung der Standardvertragsklauseln verantwortlich ist, stärken die Stellung des Betroffen zusätzlich.[131] Artikel 10 enthält eine für den Betroffenen günstige Rechtswähl- und Gerichtsstandsklausel.

Für Dienstleister in Drittstaaten, daher auch für ASP in Drittstaaten, sind die „**Auftragsverarbeiter-Standardvertragsklauseln**[132]“ einschlägig, welchen den Standardvertragsklauseln inhaltlich sehr ähnlich sind.[133] In diesen Klauseln wurde besonders Absätze 2 und 3 des Artikels 17 der allgemeinen Datenschutzrichtlinie 95/46/EG eingearbeitet, welche die Datenverarbeitung an sich (technische Sicherheitsmaßnahmen, Schutzniveau) regeln. Bei der Übermittlung von sensiblen Daten in Drittstaaten mit nicht ausreichendem Datenschutzniveau muss der Betroffene **informiert** werden.[134]

Im **Safe-Harbor-Abkommen** werden Grundsätze des Datenschutzes („*Safe Harbor Principles*“) festgelegt, denen sich **US-Unternehmen** unterwerfen können, um in der EU als Unternehmen mit ausreichenden Datenschutzstandard anerkannt zu werden.[135]

---

127) Knyrim, Neuerungen im Datenverkehr mit Drittländern, ecolex 2002, 466.

128) Klausel 5 der Standardvertragsklauseln; Entscheidung der Kommission 2001/497/EG vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG, Abl. L 181 vom 04.07.2001, 19.

129) Klausel 5 ibid.

130) Knyrim, ecolex 2002, 466.

131) Klausel 6 der Standardvertragsklauseln.

132) Klausel 4 und 5 der Auftragsverarbeiter-Standardvertragsklauseln.

133) Entscheidung der Kommission 2002/16/EG vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG, ABl. L 6 10.01.2002, 52.

134) Die Vorschrift wird kritisiert, weil sie einen Vorteil von Standardvertragsklauseln (keine Information des Betroffenen) zunichte macht; Siehe Knyrim, ecolex 2002, 466.

135) Entscheidung der Kommission 2000/520/EG vom 26. Juli 2000 gem. der Richtlinie 95/46/EG des Europaeischen Parlaments und des Rates über die

Telekommunikationsunternehmen fallen bislang nicht unter das Safe Harbor Abkommen.[136]

Für LBS-Provider ist auch § 12 Abs 3 DSG bedeutend, der festlegt, dass der Datenverkehr ins Ausland uA genehmigungsfrei ist, wenn *„der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat“*. Besonders wegen der Haftung der Vertragsparteien und der Drittbegünstigung der Datensubjekte bei den oben beschriebenen Standardvertragsklauseln ist eine **direkte Zustimmung** des jeweiligen Betroffenen eine sichere, aber uU aufwendige Alternative.

Angemessenheit des von den Grundsätzen des "sicheren Hafens" und der diesbezüglichen "Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA ABl L 215 25.08.2000, 7.

136) *Schaar*, Datenschutz im Internet, Die Grundlagen (2002), 275.

III. Europäisches Notrufsystem

Um für Einrichtungen, die Notrufe bearbeiten und die dafür von einem Mitgliedstaat anerkannt sind, einschließlich Strafverfolgungsbehörden, Ambulanzdiensten und Feuerwehren, die Beantwortung von Notrufen zu erleichtern, haben die Mitgliedstaaten nach Artikel 10 der Richtlinie 2002/58/EG die Möglichkeit vorzusehen, die **Unterdrückung der Anzeige der Rufnummer** des Anrufers aufzuheben, und die **Standortdaten** trotz vorübergehender Untersagung oder fehlender Einwilligung des Teilnehmers/Nutzers zu verarbeiten.

Für Rettungsdienstorganisationen, besonders für die allgemeine Rettung, Feuerwehr, Berg- und Wasserrettung ist es besonders wichtig zu wissen wer die jeweilige Organisation angerufen hat und wo sich die zu rettende Person aufhält. Die Europäische Union hat eine eigene Arbeitsgruppe für die Koordination des Zugangs zu Standortinformation für Rettungsdienstorganisationen („**C.G.A.L.I.E.S.**“) eingerichtet. Dadurch sollen die technischen Fortschritte im Bereich Mobilfunk für Rettungsdienstorganisationen zugänglich gemacht werden.[137] Im Folgenden wird das Europäische Notrufsystem vorgestellt und datenschutzrechtliche Fragestellungen erörtert.

A. Beschreibung des europäischen Notrufsystems

Der Ursprung des europäischen Notrufsystems, das mit der **Notrufnummer „112“** eng verknüpft ist, liegt in der Entscheidung des Rates vom 29. Juli 1991 zur Einführung einer einheitlichen europäischen Notrufnummer, die in Österreich neben den allgemein bekannten Notrufnummern (122, 133, 144) für Touristen installiert ist. Der Anrufer wird zu einer von 99 Polizeidienststellen geleitet.[138] Das Notrufsystem des

---

[137]) Dieses Gemeinschaftsprojekt ist bekannt unter dem Schlagwort „C.G.A.L.I.E.S.“ (Coordination Group on Access to Location Informatoin for Emergency Services). Für weiterführende technische Information siehe *Ludden/Pickofrod* u.A., Report on implementation issues related to access to location information by emergency services (E112) in the European Union (2002).

[138]) Entscheidung 91/396/EWG des Rates vom 29. Juli 1991 zur Einführung einer einheitlichen europaeischen Notrufnummer ABl L 217 vom 06.08.1991, 31; Für allgemeine Information zum Europäischen Notrufsystem siehe SOS 112 Europa, online: http://www.sos112.info [Stand 15. Juli 2003]. Für weitere Informationen bezüglich des Implementierungsstandes der europäischen Notrufnummer siehe European Commission, Directorate B, State of Implementation of the single European emergency call number „112“ ´(2001).

Österreichischen Roten Kreuzes mit 103 call centres ist vom Notrufsystem der Polizei völlig abgekoppelt.[139]

Ein Ausblick auf andere europäischen Länder zeigt, dass die verschiedensten Notrufsysteme und Nummern existieren.[140] Das Notrufsystem in Österreich zählt im internationalen Vergleich nicht zu den modernsten. Dem Roten Kreuz Österreich stehen heute im Allgemeinen keine Standortdaten zur Verfügung.[141]

B. Rechtsrahmen

Der im internationalen Vergleich relativ niedrige Standard österreichischer Notrufsysteme, vor allem was die Verfügbarkeit von Stammdaten und Standortdaten betrifft, könnte bereits in nächster Zukunft gehoben werden. Die unten zitierten Richtlinien verpflichten die Mobilfunknetz- und Festnetztelefonbetreiber, Standortdaten und bestimmte

139) Aritikel 1 der Entscheidung 91/396/EWG vom 06.08.1991, ABl L 217, 31, bestimmt, dass die Mitgliedstaaten dafür Sorge tragen, dass die Nummer 112 als einheitliche europäische Notrufnummer in die öffentlichen Fernsprechnetze sowie in künftige diensteintegrierende digitale Netze und öffentliche Mobilfunkdienste aufgenommen wird. Die einheitliche europäische Notrufnummer kann parallel zu anderen vorhandenen nationalen Notrufnummern eingeführt werden. Die Entscheidung 91/396/EWG vom 06.08.1991, ABl L 217, 31 wurde ersetzt durch Richtlinie 98/10/EG des Europäischen Parlaments und des Rates vom 26. Februar 1998 über die Anwendung des offenen Netzzugangs (ONP) beim Sprachtelefondienst und den Universaldienst im Telekommunikationsbereich in einem wettbewerbsorientierten Umfeld, ABl L 101 vom 01.04.1998, 24 (siehe insbesondere Artikel 7) und Richtlinie 2002/22/EG, ABl. L 108 vom 24.04.2002 (siehe insbesondere Artikel 26 und Erwägungsgrund 36).

140) Schweden, Finnland, Dänemark, Irland, Luxemburg und Island verwenden beispielsweise ein völlig **zentralisiertes Notrufsystem**, mit einem zentralen call centre für unterschiedlichste Notfalldienste. In Schweden beitreibt ein vom Staat subventioniertes Unternehmen (SOS-Alarm) das call centre, dem Informationen wie die Telefonnummer, die Adresse und Standortdaten zur Verfügung stehen. Die meisten der aufgezählten Staaten mit zentralem call centre haben nur eine Notrufnummer „112". England implementiere ein semi-zentralisiertes System, das ähnlich modern und digital arbeitet. Die übrigen Länder haben mehr oder weniger undurchschaubare **dezentralisierte Notrufsysteme**. Oft haben allgemeiner Rettungsdienst und Polizei unabhängige Notrufsysteme; Siehe *Pfarl*, 112 – Emergency Call Systems in Europe, Internal Paper, NetLight (2003), 5ff und *Baumann/Collomb*, IST-1999-14093 LOCUS – Enhanced Emergency Call Services (2001), 6f. Einen sehr guten Überblick über das englische Notrufsystem gibt das Dokument von Oftel, An overview of the fixed telephone emergency services (999/112) – An explanatory document issued by the DG of Telecommunication (2002), online: http://www.oftel.gov.uk/publications/ind_guidelines/emer1002.htm [Stand 25. Juli 2003].

141) Der Ex-Monopolist in Österreich, die Telekom Austria weigert sich beharrlich, dem Roten Kreuz Standortdaten zur Verfügung zu stellen. Dies sei laut TA aus technischen Gründen nicht möglich. Information von MR Dipl.Ing. Walter Marxt, Oberste Fernmelde Behörde (BMVIT) und Mag. Gerry Foitik, Österreichisches Rotes Kreuz.

Stammdaten an Notrufstellen, sogenannte Emergency Call Response Centers (ECRC) zu übermitteln. Es wird allerdings allgemein von einem „**soft approach**" gesprochen, weil keine Bestimmung der relevanten Richtlinien Parameter spezifizieren, nach denen diese Daten bereitgestellt werden müssen. Erwägungsgrund 36 der Universaldienstrichtlinie 2002/22/EG führt aus, dass die Betreiber die Angabe des Anruferstandorts den Notrufstellen „*soweit technisch möglich*" zu übermitteln haben. Die Übermittlung der Anrufe mit den zugehörigen Daten an die jeweiligen Notrufstellen soll den Nutzern des europäischen Notrufs einen besseren Schutz und mehr Sicherheit geben und den Notrufstellen die Wahrnehmung ihrer Aufgaben erleichtern. [142]

Die Mitgliedstaaten sollen sicherstellen, dass Notrufe unter der einheitlichen europäischen Notrufnummer „112" angemessen entgegengenommen und auf eine Weise bearbeitet werden, die der nationalen Rettungsdienstorganisation am besten angepasst ist und den technischen Möglichkeiten der Netze entspricht.[143] Besonders soll sichergestellt sein, dass die Unternehmen, die öffentliche Telefonnetze betreiben, den Notrufstellen bei allen unter der einheitlichen europäischen Notrufnummer durchgeführten Anrufen Informationen zum Anruferstandort übermitteln, soweit dies technisch möglich ist. [144]

1. Datenschutz

Nachdem im Rahmen des europäischen Notrufsystems vorgesehen ist Standortdaten und Stammdaten für möglichst viele Rettungsorganisationen in

---

142) Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie), ABl. L 108 vom 24.04.2002, 51.

143) Wie oben beschrieben wird die europäische Notrufnummer „112" zu einer von 99 Polizeikommissariaten geleitet. Sie ist also nur mit der Polizei-Notrufnummer „133" direkt gekoppelt. Es ist fraglich, ob dieses System gewährleistet, dass Anrufe „*angemessen entgegengenommen*" werden. Weiters ist fraglich, ob dieses System der österreichischen Rettungsdienstorganisation am besten entspricht. Diese Problematik ergibt sich nicht nur für Touristen, welche nach der Wahl von „112" häufig die Rettung alarmieren wollen.

Am besten an jede Rettungsdienstorganisation angepasst scheint ein zentrales EMCRC zu sein. Dies ist beispielsweise in Schweden durch das Unternehmen SOS-Alarm realisiert, welches vom Staat subventioniert wird. SOS-Alarm ist das einzige EMCRC in Schweden und leitet alle Notrufe zu verschiedensten Rettungsdienstorganisationen. Diese sind sehr vielschichtig. Darunter fallen nicht nur Polizei, Rettung und Feuerwehr, sondern auch Veterinärmedizin, Umweltnotdienste, Dienste für psychisch Kranke usw. In Schweden existiert die europäische Notrufnummer und eine traditionelle Notrufnummer, die parallel geschaltet ist. Für mehr Information siehe *Ringertz*, Bid Proposal – European Market Strategy for Location Information Systems for E- 112, Stockholm; Oftel

144) Artikel 26 Abs 2 und 3 Richtlinie 2002/22/EG, ABl. L 108 vom 24.04.2002, 51. Seit einiger Zeit bemüht sich das Rote Kreuz Österreich vergebens Standortdaten bei Notrufen von der TA übermittelt zu erhalten.

möglichst effektiver Weise bereitzustellen, ergibt sich die Frage, wie dieser Vorgang datenschutzrechtlich zu behandeln ist.

Die Mitgliedstaaten können die Rechte der Nutzer und Teilnehmer auf Privatsphäre in Bezug auf die **Rufnummernanzeige** und **Standortdaten** einschränken, wenn dies erforderlich ist, um Notfalldiensten zu ermöglichen, ihre Aufgaben so effektiv wie möglich zu erfüllen. Die MS können besondere Vorschriften erlassen, um die Anbieter von elektronischen Kommunikationsdiensten zu ermächtigen, einen Zugang zur Rufnummernanzeige und zu Standortdaten ohne vorherige Einwilligung der betreffenden Nutzer oder Teilnehmer zu verschaffen.[145]

Die Unterdrückung der Anzeige der Rufnummer des Anrufers kann ohne Einwilligung des Nutzers aufgehoben werden und Standortdaten können trotz der vorübergehenden Untersagung oder fehlenden Einwilligung durch den Teilnehmer oder Nutzer verarbeiten werden, um einem in einem Mitgliedstaat anerkannten Notrufdienst, einschließlich Strafverfolgungsbehörden, Ambulanzdiensten und Feuerwehren, effektives Arbeiten zu ermöglichen.[146]

a) Umsetzung in Österreich

Das TKG bindet die Auskünfte über Standortdaten und Stammdaten an Betreiber von Notrufdiensten an mehr Voraussetzungen, als dies der europäische Rechtsrahmen vorgibt.

Voraussetzung für die Übermittlung ist ein **Notfall**, der nur durch Bekanntgabe dieser Informationen abgewehrt werden kann. Weiters muss die Notwendigkeit der Informationsübermittlung vom Betreiber des Notrufdienstes **dokumentiert** werden und ist die Dokumentation des Notfalls dem Betreiber des jeweiligen Kommunikationsnetzes spätestens innerhalb von 24 Stunden nachzureichen. Allerdings darf der Betreiber iSd § 3 Z 4 TKG die Übermittlung nicht von der vorherigen Darlegung der Notwendigkeit abhängig machen. Die **Verantwortung** für die rechtliche Zulässigkeit des Auskunftsbegehrens trifft den Notrufdienst.[147]

Das TKG definiert nicht, welche Rettungsdienstorganisationen die Übermittlung von Stamm- und Standortdaten begehren können. Es muss sich um eine **anerkannte Rettungsdienstorganisation** handeln.[148] Die parlamentarischen Materialien zu § 98 TKG führen aus, dass der Begriff „Notrufträger“ nicht taxativ umschrieben werden kann. Der Begriff ergibt sich aus den jeweiligen Gesetzesmaterialen.[149] Trotzdem wird das Wort

---

145) Erwägungsgrund 36 Richtlinie 2002/58/EG, ABl L 201 vom 31.07.2002, 37.

146) Artikel 10 Richtlinie 2002/58/EG, ABl L 201 vom 31.07.2002, 37.

147) § 98 TKG.

148) Artikel 10 Richtlinie 2002/58/EG, ABl L 201 vom 31.07.2002, 37.

149) Einschlägige Materialiengesetze sind sehr unterschiedlich gestaltet. Vergleiche beispielsweise das Gesetz vom 4. März 1988 über das Hilfs- und Rettungswesen im Land Oberösterreich (Oö. Rettungsgesetz 1988), LGBl.Nr. 27/1988 idF LGBl.Nr. 90/2001 mit dem Gesetz vom 7. Dezember 1989 über die Rettungsdienste (Steiermärkisches Rettungsdienstgesetz), LGBl. Nr. 20/1990 idF LGBl. Nr. 21/2002.

„Notrufträger" in den Materialien weit definiert als „*eine Einrichtung, die mit der Abwehr unmittelbarer Gefahren für Leib, Leben, Gesundheit und Eigentum von Menschen befasst ist*".[150] Diese Definition umfasst alle denkbaren Rettungsdienstorganisationen und grenzt daher den Kreis der Berechtigten nicht ein. Jedenfalls lässt sich sowohl aus den europarechtlichen Angaben (FN 98 oben), als auch aus § 98 TKG ableiten, dass jede, in Österreich anerkannte Rettungsdienstorganisation, die sich mit der Abwehr unmittelbarer Gefahren für Leib, Leben, Gesundheit und Eigentum von Menschen befasst, das Recht hat, Auskünfte über Stamm- und Standortdaten zu fordern, falls eine Notfallsituation vorliegt. Die Anerkennung von Rettungsdienstorganisationen wird durch Landesgesetze geregelt.[151]

Wann ist die Übermittlung von Stamm- und Standortdaten notwendig iSd § 98 TKG? Eine **Notfallsituation** muss gemäß § 98 TKG derart gestaltet sein, dass sie nur durch die Bekanntgabe von Stammdaten bzw. Standortdaten abgewehrt werden kann. Meiner Ansicht nach kann ein Notfall „*nur durch Bekanntgabe dieser Informationen*" abgewehrt werden, wenn Stammdaten bzw Standortdaten potentiell helfen, die Notfallsituation schneller oder effektiver zu klären. Die Situation sollte daher immer **ex ante** beurteilt werden. Eine Übermittlung ist immer dann notwendig, wenn eine Rettungsdienstorganisation geographische Daten zum Aufenthaltsort eines

---

Ein anerkannter Rettungsdienst muss verschiedenste Voraussetzungen erfüllen. Es wird schwer sein die Erfüllung aller Voraussetzungen, wie in den Materialien gefordert, spätestens innerhalb von 24 Stunden nach Auskunftsbegehren nachzuweisen. Für die Definition eines Rettungsdienstes siehe beispielsweise §§ 2 und 3 des Steiermärkischen Rettungsdienstgesetzes, LGBl. Nr. 20/1990 idF LGBl. Nr. 21/2002. In Oberösterreich muss eine Feuerwehr in das „Feuerwehrbuch" eingetragen werden, um anerkannt zu sein. Dies erfolgt nur, wenn ein Reihe von Auflagen erfüllt sind; Siehe Landesgesetz vom 26. September 1996 über das Feuerwehrwesen in Oberösterreich (Oö. Feuerwehrgesetz - Oö. FWG) LGBl.Nr. 111/1996 idF LGBl.Nr. 90/2001. Der Bergrettungsdienst wird von einschlägigen Materialiengesetzen explizit genannt; Siehe beispielsweise § 5ff. Steiermärkisches Rettungsdienstgesetz. LGBl. Nr. 20/1990 idF LGBl. Nr. 21/2002; Andere Rettungsdienste werden gesammelt behandelt; Siehe beispielsweise §§ 8ff Steiermärkisches Rettungsdienstgesetz LGBl. Nr. 20/1990 idF LGBl. Nr. 21/2002.

150) § 98 TKG, der Erläuterungen zur Regierungsvorlage zum TKG; Punkt 1 der Empfehlung der Kommission zur Verarbeitung von personenbezogenen Daten in elektronischen Kommunikationsnetzwerken, European Commission, DG Information Society, Communications Services. Implementatoin/Committees, COCOM 03-02, DG INFSO/B2, 1. Juli 2003 definiert ein „**emergency service**" wie folgt:

„„*emergency service" means a service, recognised as such by the Member State, that provides immediate and rapid assistance in situations where there is a direct risk to life or limb, individual or public health or safety, to provate or public property, or the enviroment but not necessarily limited to theses situations*".

151) Siehe beispielsweise Steiermärkisches Rettungsdienstgesetz. LGBl. Nr. 20/1990 idF LGBl. Nr. 21/2002; Oberösterreichisches Rettungsgesetz 1988, LGBl.Nr. 27/1988 idF LGBl.Nr. 90/2001 oder Oberösterreichisches Feuerwehrgesetz LGBl.Nr. 111/1996 idF LGBl.Nr. 90/2001. Es wird an den einzelnen Rettungsdienstorganisationen liegen, einem Betreiber vorab nachzuweisen, dass sie anerkannt sind.

Anrufers für eine aktuelle Rettungsaktion potentiell benötigt. Die Vorgabe des europäischen Rechtsrahmen, Standortdaten an Rettungsdienstorganisationen weiterzugeben, weil diese „*so effektiv wie möglich*" arbeiten sollen, ist ein weiteres Argument für eine weite Auslegung des Wortes „Notfall" in § 98 TKG.[152] Potentiell liegt daher immer dann ein Notfall vor, wenn eine Notrufnummer gewählt wird.

Der Betreiber eines Kommunikationsnetzes hat dem Auskunftsbegehren nachzukommen und darf die Übermittlung nicht von der vorherigen Darlegung der Notwendigkeit abhängig machen. Die **Verantwortung** für die rechtliche Zulässigkeit des Auskunftsbegehrens trifft immer den Betreiber des Notrufdienstes.[153] Rechtliche Konsequenzen für eine Rettungsdienstorganisation, die Standortdaten bzw. Stammdaten ohne Notwendigkeit von einem Betreiber begehrt, werden vom TKG nicht formuliert. Dies scheint auch nicht notwendig zu sein, weil im Zweifel, nach einer ex ante Betrachtungsweise wohl immer eine Notfallsituation vorliegt. Im Übrigen ist mangels einschlägiger Regelung im TKG auf das DSG zu verweisen.[154]

Nach der Übermittlung der Daten vom Betreiber an die Rettungsdienstorganisation sind die Daten unverzüglich zu **löschen**, sobald diese nicht mehr zur Verhinderung des Notfalles gebraucht werden. Dies ergibt sich aus § 99 Abs 1 TKG für Verkehrsdaten, welcher analog auf Standortdaten anzuwenden ist.[155]

Gemäß § 98 TKG muss die Notwendigkeit der Informationsübermittlung vom Betreiber des Notrufdienstes dokumentiert werden. Dies darf nicht so interpretiert werden, dass der Betreiber eines Notrufdienstes eine **Dokumentationspflicht** im Sinne einer Archivierungspflicht hat. Die Notfallsituation muss nur solange dokumentiert werden, solange der Notfall andauert. Wird dies nicht gemacht, muss ein anonymisiertes Dokument über die Notfallsituation spätestens innerhalb von 24 Stunden nachgereicht werden.

b) Rechtsvergleich - Deutschland

Ein Blick nach Deutschland zeigt, dass Auskünfte an Betreiber von Notrufdiensten rechtlich einfacher geregelt werden könnten. § 103 Abs 1 Referenzentwurf zum deutschen TKG formuliert klar und eindeutig:

„*Wer Telekommunikationsnetze betreibt, die für öffentliche Telefondienste genutzt werden, ist verpflichtet, Notrufe einschließlich*

---

152) Erwägungsgrund 36 der Richtlinie 2002/22/EG, ABl. L 108 vom 24.04.2002, 51.

153) Erläuterungen zu § 98 TKG der Erläuterungen zur Regierungsvorlage zum TKG.

154) Gemäß § 92 Abs 1 TKG sind, soweit das TKG nichts anderes bestimmt, auf die im TKG geregelten Sachverhalte die Bestimmungen des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999, anzuwenden.

155) Siehe Kapitel II/E/5.

1. der Rufnummer des Anschlusses, von dem die Notrufverbindung ausgeht und

2. der Daten, die zur Ermittlung des Standortes, von dem die Notrufverbindung ausgeht, und zur Verfolgung von Missbrauch des Notrufs erforderlich sind, an die örtlich zuständige Notrufabfragestelle zu übermitteln".[156]

2. Ausblick

Eine sich noch in Vorbereitung befindliche **Empfehlung der EK** zur Verarbeitung von personenbezogenen Daten in elektronischen Kommunikationsnetzwerken geht davon aus, dass Betreiber von Telekommunikationsnetzen bei Anrufen über die europäischen **Notrufnummer** (112) und nationalen Notrufnummern (in Österreich va 122, 133, 144) ortsbezogene Daten, soweit technisch möglich, **weiterleiten müssen**. Die Implementierung wird durch eine eigene Arbeitsgruppe für die Koordination des Zugangs zu Standortinformation für Rettungsdienstorganisationen („**C.G.A.L.I.E.S.**") überwacht und koordiniert.[157]

Gemeinsame technische Standards und Praktiken werden von C.G.A.L.I.E.S. entwickelt.[158] Eine Harmonisierung wird durch die technischen, organisatorischen und strukturellen Unterschiede der verschiedenen länderspezifischen Notrufsysteme schwer zu erreichen sein.[159]

Die Mitgliedstaaten müssen zukünftig effektive call centres installieren.[160] Dies könnte in Österreich dazu führen, dass es zu einer Zusammenlegung der einzelnen Notrufsysteme kommt. Derzeit ist das Notrufsystem der Ambulanzdienste vom Notrufsystem der Polizei und Feuerwehr getrennt. Ruft jemand die Nummer "112", wird er/sie zum nächstliegenden der 99 call centres der Polizei verbunden. Wird eine andere Rettungsdienstorganisation benötigt, muss manuell verbunden werden. Eine Zusammenlegung oder zumindest eine **Kopplung der Notrufsysteme** durch ein gemeinsames

---

156) Das Wort „Notrufabfragestelle" wird allerdings im deutschen Referenzentwurf 2003 nicht definiert und muss daher auf landesrechtliche Regelungen über Notrufabgabestellen zurückgegriffen werden. Auf eine Dokumentationspflicht der Notfallsituation wurde verzichtet.

157) Erwägungsgrund 2, 3 und 4 der Empfehlung der Kommission zur Verarbeitung von personenbezogenen Daten in elektronischen Kommunikationsnetzwerken, European Commission, DG Information Society, Communications Services. Implementatoin/Committees, COCOM 03-02, DG INFSO/B2, 1. Juli 2003.

158) Erwägungsgrund 7 Empfehlung der Kommission zur Verarbeitung von personenbezogenen Daten in elektronischen Kommunikationsnetzwerken, COCOM 03-02, DG INFSO/B2, 1. Juli 2003.

159) *Pfarl*, 112 – Emergency Call Systems in Europe, Internal Paper, NetLight (2003).

160) Erwägungsgrund 11 Empfehlung der Kommission zur Verarbeitung von personenbezogenen Daten in elektronischen Kommunikationsnetzwerken, COCOM 03-02, DG INFSO/B2, 1. Juli 2003.

Interface, wie dies in Vorarlberg zwischen Rotem Kreuz und Feuerwehr der Fall ist, wird durch die neue Empfehlung wahrscheinlich notwendig sein. Es muss zumindest möglich sein, ortsbezogene Daten und Stammdaten effektiv zu bearbeiten, zu empfangen und möglicherweise weiterzuleiten. Jeder Mitgliedstaat soll einen gemeinsamen „**interface standard**" für alle call centres anwenden, damit ortsbezogene Information und Stammdaten (Adresse, Name, Telefonnummer) effektiv behandelt werden können.[161]

Die Mitgliedstaaten sollen **detaillierte Regelungen** erlassen, die Betreiber von Telekommunikationsnetzen **verpflichten**, bestmögliche Informationen an call centres weiterzugeben. Es wird daher vom derzeitigen „soft approach" abgerückt und werden durch detailliertere Regelungen den Betreibern Verpflichtungen auferlegt. ME nach ist die Weiterleitung von ortsbezogenen Daten und bestimmten Stammdaten zu Rettungsdienstorganisationen in Österreich technisch bereits jetzt möglich. In anderen Mitgliedstaaten (zB Schweden, England) sind ortsbezogene Informationen für Rettungsdienstorganisationen bereits erhältlich. Die oben zitierte Empfehlung geht davon aus, dass den Rettungsdienstorganisationen schon bald präzise ortsbezogene Daten durch A-GPS-Technologie zur Verfügung stehen werden.[162]

Zwischen eigenen Kunden und anderen Teilnehmern (Roamingkunden, oder Kunden anderer Betreiber ohne Netzabdeckung) darf nicht unterschieden werden. Jeder Notruf soll auf sein Ursprungsnetz verweisen. Auch deshalb ist ein gemeinsamer „interface standard" aller Netzbetreiber und/oder ein gemeinsames „interface" unerlässlich.

Die Betreiber müssen Adressinformationen und andere Informationen **aktuell** halten.

Call centres müssen die Möglichkeit haben, ortsbezogene Informationen auch bei **abgebrochenen Anrufen** zu erhalten und den jeweiligen Teilnehmer zurückrufen können.[163]'

Weiters sollen die Bürger der Mitgliedstaaten über die Möglichkeiten der Nummer "112" **informiert** werden.[164] Die Nummer "112" wird EU-intern gegenüber den traditionellen Notrufnummern bevorzugt behandelt. Viele MS, darunter Österreich präverieren nationale Notrufnummern. Daher sind ein gemeinsames „interface" bzw gemeinsame Standards für eine effektive

---

161) Der gemeinsame „interface standard" muss flexibel sein, um an zukünftige Veränderungen angepasst werden zu können; Punkt 10 der Empfehlung der Kommission zur Verarbeitung von personenbezogenen Daten in elektronischen Kommunikationsnetzwerken, COCOM 03-02, DG INFSO/B2, 1. Juli 2003.

162) Punkt 12 der Empfehlung der Kommission zur Verarbeitung von personenbezogenen Daten in elektronischen Kommunikationsnetzwerken, COCOM 03-02, DG INFSO/B2, 1. Juli 2003.

163) Punkte 4-9 der Empfehlung der Kommission zur Verarbeitung von personenbezogenen Daten in elektronischen Kommunikationsnetzwerken, COCOM 03-02, DG INFSO/B2, 1. Juli 2003.

164) Punkte 11 der Empfehlung der Kommission zur Verarbeitung von personenbezogenen Daten in elektronischen Kommunikationsnetzwerken, COCOM 03-02, DG INFSO/B2, 1. Juli 2003.

Beantwortung von Notrufen mit verschiedenen Notrufnummern besonders wichtig.[165]

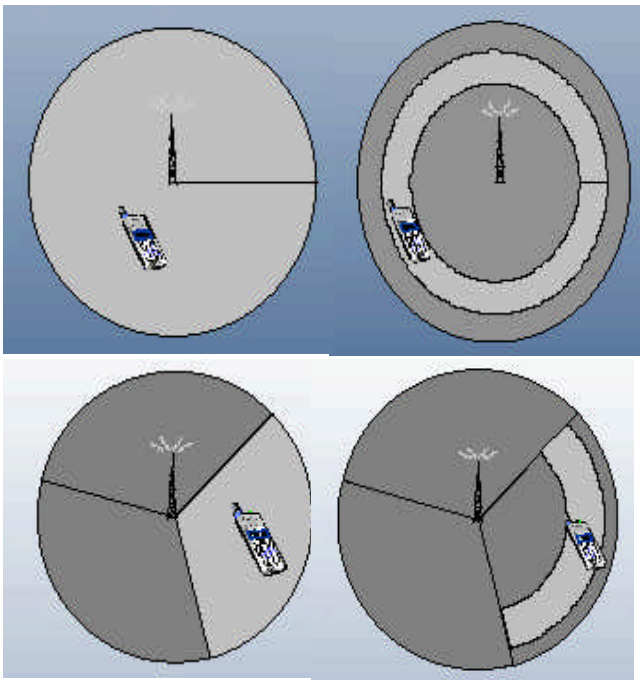
Nach dem Entwurf der oben zitierten Empfehlung müssen die MS die EK bis **Mitte 2004** über **Implementierungsschritte** unterrichten.

165) Ob Österreichs heute der Verpflichtung ein effizientes Notrufsystem zu gewährleisten nachkommt, wird uU von ordentlichen Gerichten geprüft, nachdem ein Teilnehmer eines Jugendlagers wegen verspäteter Hilfeleistung an einer allergischen Reaktion nach einem Wespenstich gestorben ist. Die Polizeidienststelle war nicht in der Lage den Notruf unter der europäischen Notrufnummer effizient an Rettungsdienststellen weiterzuleiten. Eine derartige Verpflichtung könnte wie oben gezeigt aus europarechtlichen Vorgaben abgeleitet werden; Tödlicher Wespenstich vor Gericht, Kurier vom 27.8.2003, online http://www.kurier.at/chronik/364136.php [Stand 4. September 2003].

Annex -

Die Abbildungen wurden dem Autor dankenswerter Weise von der Firma NetLight (www.netlight.se) zur Verfügung gestellt.

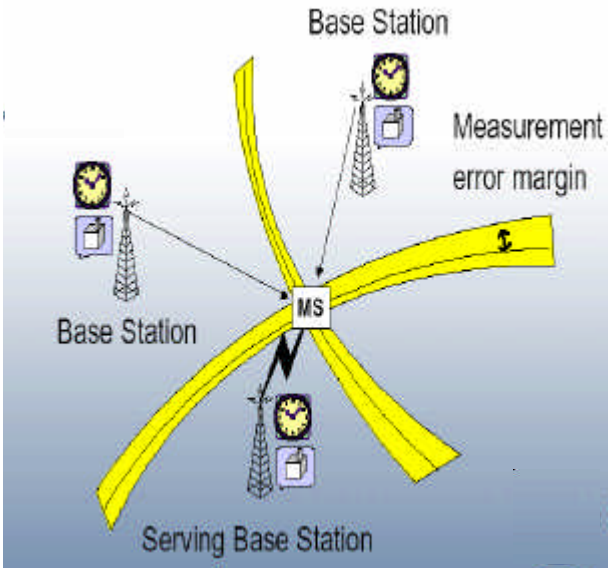
Abbildung 1:



Cell Global Identity: Die Genauigkeit bei dieser Methode hängt von der Größe des Zellenradius ab (100m – 35km).

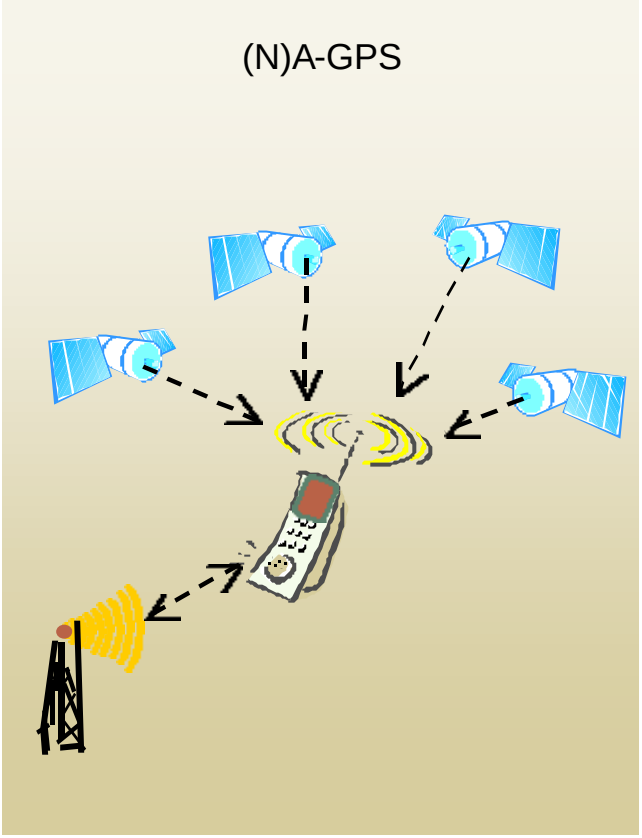
Cell Global Identity and Time Advance (CGI+TA): Die Genauigkeit hängt von der Entfernung zur Basestation ab.

Abbildung 2:



Uplink Time of Arrival: Die jew. Basestationen (BS) werden durch das SMLC (Serving Mobile Location Centre) instruiert auf das Signal des MS (Mobile Terminal+SIM) zu hören. Für diese Weiterentwicklung des CGI+TA müssen die BS mit LMUs (Location Measurement Unit) ausgestattet werden.

Abbildung 3:



Network Assisted Global Positioning System ((N)A-GPS): Die MS erhält „Hilfsdaten“ von der Position zweier Satelliten, welche von der MS selbst durch einen kleinen GPS Empfänger empfangen werden.

Abbildung 4:
Genauigkeitsangaben der verschiedenen Ortungsmethoden:

Technology	Rural	Rural extreme	Sub-urban	Sub-urban ex-treme	Urban	Urban extreme	Indoor user	Comments
Cell ID	1-35 km	1-100 km	1-10 km	1-10 km	50m-1km	50m-1km	No change unless there is a pico-cell	Cell shape can be returned. Possibility of incorrect sector
Cell ID and Timing Advance	1-35 km	1-100 km	1-10 km	1-10 km	50m-1km	50m-1km	No change unless there is a pico-cell	Radial distance can be improved for ranges above 550m Possibility of incorrect sector
E-OTD	50-150m	50-150m or unavailable if not 3 BTS	50-150m	100-250m	50-150m	100-300m	Slight degradation but penetrates well indoors	Mobile needs to see least 3 BTS. Falls back to Cell/TA if unavailable
A-GPS (To be confirmed)	10m	10m	20m	50-100m	30-100m	50-100 if available	In-building coverage by windows but not deep inside.	Cell Id fall-back