

Christoph Schnabel

Datenschutz bei profilbasierten Location Based Services

Die datenschutzadäquate Gestaltung von Service-Plattformen
für Mobilkommunikation

Gliederung

1	Einleitung	22
1.1	Methodik	30
1.2	Gang der Untersuchung	36
2	Rechtsrahmen für den Datenschutz	37
2.1	Anfänge und Grundlagen des Datenschutzes	39
2.2	Der internationale Rechtsrahmen	42
2.2.1	Vereinte Nationen	43
2.2.1.1	Allgemeine Erklärung der Menschenrechte der Vereinten Nationen	43
2.2.1.2	Internationaler Pakt über bürgerliche und politische Rechte der Vereinten Nationen	44
2.2.2	Europarat	45
2.2.2.1	Konvention zum Schütze der Menschenrechte und Grundfreiheiten des Europarats	45
2.2.2.2	Datenschutzkonvention	47
2.2.3	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung	48
2.2.4	Die Europäische Gemeinschaft	50
2.2.4.1	Europäische Verträge	50
2.2.4.2	Die Grundrechtecharta der Europäischen Union	53
2.2.4.3	Der Europäische Verfassungsvertrag	54
2.2.4.4	EU-Reformvertrag (Vertrag von Lissabon)	55
2.2.4.5	Richtlinien	56
2.2.4.5.1	Die allgemeine Datenschutzrichtlinie	57
2.2.4.5.1.1	Anwendungsbereich	59
2.2.4.5.1.2	Verarbeitungsregeln	59
2.2.4.5.1.3	Sensible Daten	62
2.2.4.5.1.4	Kontrolle	62
2.2.4.5.1.5	Datentransfers in Drittstaaten	63
2.2.4.5.1.6	Umsetzung	64
2.2.4.5.2	Die Datenschutzrichtlinie für elektronische Kommunikation	65
2.2.4.5.2.1	Anwendungsbereich	66
2.2.4.5.2.2	Verkehrs- und Standortdaten	66
2.2.4.5.2.3	Verarbeitungsregeln	67
2.2.4.5.2.4	Schutzumfang	68
2.2.4.5.3	Vorratsspeicherungs-Richtlinie	68
2.2.4.5.3.1	Vorgaben der Vorratsspeicherung	69
2.2.4.5.3.2	Regelungskompetenz der Gemeinschaft	70
2.3	Der nationale Rechtsrahmen	71
2.3.1	Der verfassungsrechtliche Rahmen	71
2.3.1.1	Das Recht auf informationelle Selbstbestimmung	73
2.3.1.2	Fernmeldegeheimnis	83
2.3.1.3	Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme	85
2.3.1.3.1	Vorlauf zur Entscheidung des Bundesverfassungsgerichts	85
2.3.1.3.2	Das Grundrecht in der Entscheidung des Bundesverfassungsgerichts	86
2.3.1.3.3	Anwendbarkeit auf die Service-Plattform	89
2.3.1.3.3.1	Informationstechnisches System	90

2.3.1.3.3.2 Eigenes System.....	92
2.3.2 Schutzdimension der Grundrechte.....	94
2.3.3 Das einfache Gesetzesrecht.....	98
2.3.3.1 Das Bundesdatenschutzgesetz.....	99
2.3.3.1.1 Geltungsbereich.....	100
2.3.3.1.2 Zulässigkeit des Umgangs mit personenbezogenen Daten.....	103
2.3.3.1.3 Verarbeitungsregeln.....	105
2.3.3.1.4 Einwilligung gemäß § 4a BDSG.....	107
2.3.3.1.5 Betroffenenrechte.....	110
2.3.3.1.6 Organisatorische und verfahrensrechtliche Vorschriften.....	112
2.3.3.2 Telekommunikationsdatenschutz.....	115
2.3.3.2.1 Geltungsbereich.....	116
2.3.3.2.2 Zulässigkeit des Umgangs mit personenbezogenen Daten.....	117
2.3.3.2.3 Vorratsspeicherung.....	121
2.3.3.2.4 Verarbeitungsregeln.....	122
2.3.3.3 Telemediendatenschutz.....	123
2.3.3.3.1 Geltungsbereich.....	124
2.3.3.3.2 Zulässigkeit des Umgangs mit personenbezogenen Daten.....	127
2.3.3.3.3 Verarbeitungsregeln.....	130
2.4 Grundsätze der Verarbeitung personenbezogener Daten.....	133
2.4.1 Selbstbestimmung.....	134
2.4.2 Transparenz.....	135
2.4.3 Zweckbindung.....	136
2.4.4 Erforderlichkeit.....	137
2.4.5 Systemdatenschutz.....	138
2.4.6 Selbstdatenschutz.....	140
2.4.7 Betroffenenrechte.....	141
Service-Plattformen.....	143
3.1 Technische Grundlagen einer Service-Plattform.....	143
3.2 Szenario.....	149
3.3 Fokusgruppen-Interviews.....	159
3.3.1 Allgemeine Erkenntnisse.....	161
3.3.2 Datenschutz.....	162
3.3.3 Ergebnisse und Schlussfolgerungen..... ?	163
3.4 Präzisierung der Untersuchungsschwerpunkte.....	165
Profile.....	169
4.1 Spezifische Risiken der Profilerstellung.....	171
4.1.1 Kernbereich der Persönlichkeit.....	172
4.1.2 Kontextverlust.....	174
4.1.3 Automatisierte Entscheidung.....	174
4.1.4 Schlussfolgerung.....	175
4.2 Begriff des Profils.....	175
4.2.1 Begriff des Persönlichkeitsprofils im Datenschutzrecht.....	177
4.2.2 Definition des Profils.....	178
4.3 Technische Grundlagen der Profilerstellung.....	180
4.3.1 Profil-Struktur.....	181
4.3.2 Definition technischer Begriffe.....	181
4.3.3 Beispiel eines Profils.....	183
4.3.4 Die Abfrage von Nutzer-Daten.....	184
4.3.5 Learning by Using.....	185
4.3.6 Technische Grundlagen des Learning and Recommending-Systems.....	187

4.4 Das Nutzer-Profil der Service-Plattform.....	189
4.5 Verfassungsrechtliche Zulässigkeit der Profilbildung.....	191
4.5.1 Die Würde des Menschen.....	192
4.5.2 Erstellung von Profilen im nicht-öffentlichen Bereich.....	194
4.6 Datenschutzrechtliche Zulässigkeit der Verarbeitung von Profildaten 196	
4.6.1 Personenbezogene Daten.....	196
4.6.2 Kategorisierung der Daten.....	200
4.6.3 Profildienst als Telemediendienst.....	202
4.6.4 Dreiteilung der Profildaten.....	204
4.6.5 Verwendung von Profildaten.....	206
4.6.6 Verarbeitung von Nutzungsdaten.....	207
4.6.7 Verbot der Datenspeicherung auf Vorrat.....	209
4.6.8 Speicherdauer.....	211
4.6.9 Besondere Arten personenbezogener Daten.....	214
4.6.9.1 Verwendungszusammenhang.....	215
4.6.9.2 Vertrag als Verarbeitungsgrundlage.....	218
4.6.9.3 Einwilligung als Verarbeitungsgrundlage.....	221
4.6.10 Bilder.....	229
4.6.10.1 Das Recht am eigenen Bild.....	230
4.6.10.2 Einwilligung.....	232
4.6.10.3 Anwendbarkeit des Datenschutzes auf Bilder.....	236
4.6.10.4 Recht am eigenen Bild als <i>lex specialis</i>	238
4.6.10.5 Europarechtliche Implikationen.....	239
4.6.10.6 Schlussfolgerung.....	240
Location Based Services.....	242
5.1 Konstellationen von Location Based Services.....	243
5.2 Technische Grundlagen von Location Based Services.....	246
5.2.1 Satellitengestützte Positionsbestimmung.....	246
5.2.2 Netzwerkbasierte Positionsbestimmung.....	249
5.2.3 Positionsbestimmung mithilfe kabelloser Technologien.....	251
5.2.4 Überblick Reichweite von Methoden zur Positionsbestimmung.....	253
5.3 Rechtliche Bewertung.....	253
5.3.1 Positionsdaten als personenbezogene Daten.....	253
5.3.2 Dienste mit satellitengestützter Ortung.....	254
5.3.2.1 Pull-Dienst mit satellitengestützter Ortung im Zwei-Personen-Verhältnis.....	255
5.3.2.1.1 Erhebung der Positionsdaten.....	255
5.3.2.1.2 Übermittlung der Positionsdaten.....	256
5.3.2.1.3 Verarbeitung der Positionsdaten.....	256
5.3.2.1.3.1 Anwendbarkeit des Telekommunikationsgesetzes.....	256
5.3.2.1.3.2 Anwendbarkeit des Telemediengesetzes.....	259
5.3.2.1.3.3 Positionsdaten als sensible Daten.....	261
5.3.2.1.4 Zwischenergebnis.....	263
5.3.2.2 Push-Dienst mit satellitengestützter Ortung im Zwei-Personen-Verhältnis.....	263
5.3.2.2.1 Erhebung und Übermittlung der Positionsdaten.....	264
5.3.2.2.2 Verarbeitung der Positionsdaten.....	264
5.3.2.2.3 Zwischenergebnis.....	265
5.3.2.3 Pull/Push-Dienst mit satellitengestützter Ortung im Zwei-Perspnen-Verhältnis.....	266
5.3.2.3.1 Weitergabe der Positionsdaten an andere End-Nutzer.....	266

5.3.2.3.2	Zwischenergebnis.....	268
5.3.3	Dienste mit netzwerkbasierter Ortung.....	268
5.3.3.1	Pull-Dienst mit netzwerkbasierter Ortung im Zwei-Personen-Verhältnis.....	268
5.3.3.1.1	Verhältnis zwischen Verkehrs- und Standortdaten.....	270
5.3.3.1.2	Erhebung der Positionsdaten.....	271
5.3.3.1.3	Übermittlung der Positionsdaten.....	272
5.3.3.1.4	Verwendung der Positionsdaten.....	273
5.3.3.1.5	Zwischenergebnis.....	278
5.3.3.2	Push-Dienst mit netzwerkbasierter Ortung im Zwei-Personen-Verhältnis.....	279
5.3.3.3	Pull/Push-Dienst mit netzwerkbasierter Ortung im Zwei-Personen-Verhältnis.....	279
5.3.4	Mehr-Personen-Verhältnisse.....	280
5.3.4.1	Drei-Personen-Verhältnis bei satellitengestützter Ortung des End-Nutzers.....	280
5.3.4.2	Drei-Personen-Verhältnisse bei netzwerkbasierter Ortung des End-Nutzers.....	285
5.3.4.2.1	Externer Mobilfunkanbieter und Service-Plattform als LBS-Anbieter.....	285
5.3.4.2.1.1	Erhebung und Übermittlung der Positionsdaten.....	285
5.3.4.2.1.2	Verwendung der Positionsdaten.....	287
5.3.4.2.2	Externer LBS-Anbieter und Service-Plattform als Mobilfunkanbieter.....	287
5.3.4.3	Vier-Personen-Verhältnis.....	287
5.3.4.4	Mehrere End-Nutzer.....	288
5.3.5	Positionsbestimmung mit Hilfe kabelloser Technologien.....	290
5.3.5.1	RFID.....	290
5.3.5.2	Wireless Local Area Network (WLAN).....	294
5.3.5.3	Wireless Personal Area Network (WPAN)/Bluetooth.....	296
5.3.6	Einwilligung.....	298
5.3.6.1	Umfang der Einwilligung.....	299
5.3.6.2	Person des Einwilligenden.....	302
5.3.6.3	Informationspflichten des Teilnehmers gegenüber Mitbenutzern.....	304
5.3.6.4	Besonderheiten der Einwilligung bei Minderjährigen.....	306
5.3.6.5	Besonderheiten bei Arbeitnehmern.....	308
5.3.7	Informationspflichten des Betreibers der Service-Plattform.....	310
5.3.8	Sonderregelungen bei Notfällen.....	312
5.3.9	Speicherdauer der Positionsdaten.....	315
5.3.9.1	Vorratsdatenspeicherung.....	316
5.3.9.2	Positionsdaten als Profil-Daten.....	318
	Empfehlungen zur Technikgestaltung.....	321
6.1	Grundsätze des Datenschutzes.....	321
6.1.1	Selbstbestimmung.....	322
6.1.2	Transparenz.....	322
6.1.3	Zweckbindung.....	323
6.1.4	Erforderlichkeit.....	324
6.1.5	Systemdatenschutz.....	325
6.1.6	Selbstdatenschutz.....	327
6.1.7	Betroffenenrechte.....	328
6.2	Profile.....	329

6.2.1	Selbstbestimmung.....	329
6.2.1.1	Vorrang der Grundeinstellungen vor Zusatzdaten.....	330
6.2.1.2	Einwilligungsmanagement.....	331
6.2.1.3	Speicherort des Profils.....	332
6.2.1.4	Kontrolle des End-Nutzers über den Inhalt des Profils.....	333
6.2.2	Transparenz.....	334
6.2.2.1	Hinweis- und Unterrichtspflichten.....	335
6.2.2.2	Anzeige des End-Nutzer-Profiles.....	337
6.2.3	Zweckbindung.....	338
6.2.4	Erforderlichkeit.....	340
6.2.5	Systemdatenschutz.....	341
6.2.5.1	Funktionstrennung.....	341
6.2.5.2	Zentrale Pseudonymisierung.....	341
6.2.5.3	Datensparsamkeit.....	343
6.2.5.4	Datensicherheit.....	345
6.2.5.5	Löschungsmanagement.....	346
6.2.6	Selbstdatenschutz.....	347
6.2.6.1	Datensafe.....	347
6.2.6.2	Kontrolle des End-Nutzers über sein Profil.....	348
6.2.6.3	Selbstgewählte Pseudonyme oder Anonymisierung.....	349
6.2.7	Betroffenenrechte.....	349
6.2.7.1	Auskunftsrecht.....	349
6.2.7.2	Berichtigungs- und Lösungsansprüche.....	351
6.3	Location Based Services.....	353
6.3.1	Selbstbestimmung.....	353
6.3.2	Transparenz.....	355
6.3.3	Zweckbindung.....	357
6.3.4	Erforderlichkeit.....	358
6.3.5	Systemdatenschutz.....	358
6.3.6	Selbstdatenschutz.....	360
6.3.6.1	Unterbrechung der Ortung.....	360
6.3.6.2	Pseudonyme.....	361
6.3.7	Betroffenenrechte.....	363
6.4	Service-Plattform.....	364
6.4.1	Selbstbestimmung.....	365
6.4.1.1	Elektronische Entmündigung.....	365
6.4.1.2	Unverlangte Werbung.....	366
6.4.2	Transparenz.....	367
6.4.3	Zweckbindung.....	367
6.4.4	Erforderlichkeit.....	369
6.4.5	Systemdatenschutz.....	369
6.4.6	Selbstdatenschutz.....	370
6.4.7	Betroffenenrechte.....	371
6.4.7.1	Auskunftsrecht.....	372
6.4.7.2	Berichtigungs- und Lösungsansprüche.....	373
	Empfehlungen zur Rechtsgestaltung.....	374
7.1	Profile.....	374
7.1.1	Definition für Profile.....	375
7.1.2	Unterscheidung verschiedener Arten von Profilen.....	376
7.1.3	Voraussetzungen für die Erstellung und Führung eines Profils.....	378
7.1.4	Verschiedene Arten von Daten in einem Profil.....	379

7.1.5	Zweckbindung.....	380
7.1.6	Zusammenfassung.....	381
7.2	Location Based Services.....	381
7.2.1	Verhältnis personenbezogene Daten/Standortdaten/Verkehrsdaten... ..	382
7.2.2	Unterscheidung zwischen Tracking und Positioning.....	384
7.2.3	Alternative Methoden der Lokalisierung.....	384
7.2.4	Einwilligungserfordernis.....	386
7.2.5	Person des Einwilligenden.....	387
7.2.6	*' Spezialregelungen für Arbeitnehmer und Kinder.....	388
7.2.7	Regelung zu Standortdaten im nationalen Recht.....	389
7.2.7.1	Erheben der Standortdaten.....	389
7.2.7.2	Anwendungsbereich der Regelung über Standortdaten.....	389
7.2.8	Zusammenfassung.....	389
7.3	Allgemein zur Service-Plattform.....	391
7.3.1	Mitteilungspflicht bei Sicherheitsverletzungen.....	391
7.3.2	Vorsorgeregelungen.....	393
7.3.3	Vorgehen gegen unverlangte Werbung.....	394
7.3.4	Zusammenfassung.....	395
7.4	Ausblick.....	395
8	Schlussbetrachtung.....	397
	Literaturverzeichnis.....	401