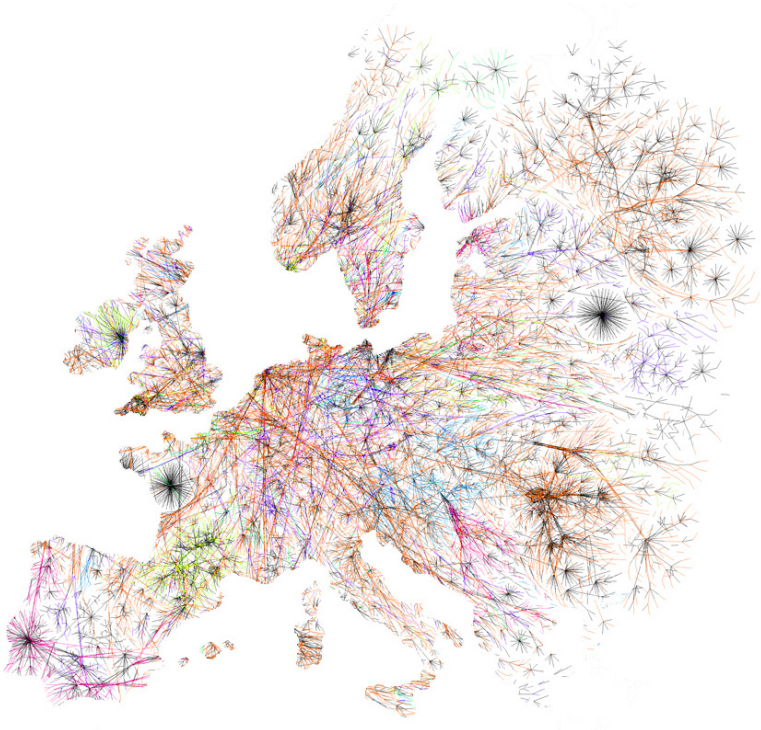
Universität Regensburg
Fakultät für Sprach-, Literatur- und Kulturwissenschaften
Institut für Information und Medien, Sprache und Kultur (I:IMSK)

Magisterarbeit

Die Vorratsdatenspeicherung

in Europa, Deutschland und Bayern

Eine vergleichende Betrachtung und Bewertung
aus Sicht der IT-Sicherheit



Michael Biendl
Matr.-Nr.: 1215803
Aufbaustr. 26
94315 Straubing

Erstgutachter: Prof. Dr. Christian Wolff
Zweitgutachter: Prof. Dr. Hannes Federrath

Deckblatt: Visualisierung der Infrastruktur des Internets in Europa (bearbeitete Grafik),
Quelle im Internet abrufbar unter der URL http://blyon.com/blyon-cdn/opte/maps/static/1105841711.LGL.2D.1024x1024.png

Die Internetadressen wurden zuletzt am 22. August 2011 auf Aktualität überprüft.

Meinen Eltern

Inhaltsverzeichnis

Abkürzungsverzeichnis IV

Abbildungsverzeichnis VII

Tabellenverzeichnis X

A. Einführung 1

I. Motivation und Heranführung an das Thema 1

II. Grundsätzliches zur Vorratsdatenspeicherung 4

III. Zielsetzung und Betrachtungsverlauf 5

B. Technische und rechtliche Grundlagen 8

I. Grundlagen der IT-Sicherheit 8

1. Begriff der IT- und Datensicherheit im Kontext des Datenschutzes 8

2. Die IT-Schutzzieldogmatik im Kontext des Datenschutzrechts 9

a) Verfügbarkeit 10

b) Vertraulichkeit 11

c) Integrität 11

d) Authentizität 11

e) Verbindlichkeit 12

II. Juristische Datenkategorien und netzseitige Infrastrukturen 12

1. Personenbezogene Daten 12

2. Inhaltsdaten 13

3. Verkehrsdaten 13

a) Verkehrsdaten im Bereich der Festnetztelefonie 14

b) Verkehrsdaten im Bereich des Mobilfunks 15

c) Verkehrsdaten im Bereich des Internetzugangs 17

d) Verkehrsdaten im Bereich des E-Mail-Verkehrs 22

e) Verkehrsdaten im Bereich der Internet-Telefonie 24

4. Bestandsdaten 25

5. Standortdaten 25

6. Vorratsdaten 25

7. Zusammenfassung 26

C. Grundüberlegungen zum erforderlichen Schutzniveau 27
I. Schutzinteressen der beteiligten Akteure 27
1. Schutzinteressen der Telekommunikationsteilnehmer 28
2. Schutzinteressen der Ermittlungsbehörden 29
3. Schutzinteressen der Telekommunikationsdiensteanbieter 31
II. Bedrohungspotential 31
1. Angriffe auf die Schutzinteressen der TK-Nutzer 32
2. Angriffe auf die Schutzinteressen der Ermittlungsbehörden 33
3. Mächtigkeit potentieller Angreifer 37
III. Schutzbedarfsfeststellung 38

D. Europarechtliche Vorgaben 39
I. Vorgaben in Bezug auf die Datenkategorien, Speicherfrist und Zweckbindung 39
1. Kategorien der zu speichernden Daten 39
a) Vorratsdaten im Bereich des Festnetzes 41
B) Vorratsdaten im Bereich des Mobilfunks 42
c) Vorratsdaten im Bereich des Internetzugangs 44
d) Vorratsdaten im Bereich des E-Mail-Verkehrs 45
e) Vorratsdaten im Bereich der VoIP-Telefonie 47
F) Zusammenfassung 49
2. Speicherdauer 51
3. Zugriffsschwelle 51
II. Vorgaben in Bezug auf die Datensicherheit der Vorratsdaten 51
1. Sekundärrechtliche Vorgaben 52
a) Vorgaben aus der VDSRL: Die vier Grundsätze der Datensicherheit 52
b) Vorgaben aus der EDSRL 54
c) Vorgaben aus der DSRL 55
2. Europaweite Technische Standards 56
a) Technische Spezifikation 102 656 V1.2.1 (2008-12) 56
b) Technische Spezifikation 102 657 V1.7.1 (2010-10) 57
III. Fazit 57

E. Vergleichende Betrachtung der einzelstaatlichen Umsetzungen 60
I. Aktueller Umsetzungsstand 60
II. Kategorien der zu speichernden Daten 62

II. Speicherfristen ... 63
IV. Zugriffsschwellen ... 64
V. Technische und organisatorische Sicherheitsvorkehrungen ... 65
1. Rechtliche Betrachtung ... 65
2. Praktische Betrachtung ... 67
b) Maßnahmen zum Schutz der Vertraulichkeit und Integrität ... 68
c) Maßnahmen zum Schutz der Verfügbarkeit ... 70
d) Konkrete Ausgestaltung des Übermittlungsverfahrens ... 70
VII. Fazit ... 71

F. Die Umsetzung in der Bundesrepublik Deutschland ... 72
I. Die rechtliche Umsetzung der Vorratsdatenspeicherung in Deutschland ... 72
1. Einfachgesetzliche Sicherheitstechnische Vorgaben ... 73
a) Vorgaben aus dem TKG ... 73
b) Vorgaben aus dem BDSG ... 74
2. Sicherheitstechnische Vorgaben auf Verwaltungsebene ... 77
II. Sicherheitsspezifische Aspekte des Urteils des Bundesverfassungsgerichts ... 78
III. Die Praktische Umsetzung in der Bundesrepublik Deutschland ... 80
1. Speicherung und Aufbewahrung der Daten ... 80
2. Übermittlung der Daten an die Ermittlungsbehörde ... 80

G. Fazit ... 81

Literaturverzeichnis ... 83
Anhang ... 88

ABKÜRZUNGSVERZEICHNIS

ACL	Access Control List
AT	Österreich
BDSG	Bundesdatenschutzgesetz
BE	Belgien
BG	Bulgarien
BKA	Bundeskriminalamt
BMWi	Bundesministerium für Wirtschaft und Technologie
BND	Bundesnachrichtendienst
BNetzA	Bundesnetzagentur
BSC	Base Station Controller
BVerfG	Bundesverfassungsgericht
CAS	Content-Adressed Storage
CCC	Chaos Computer Club
CD	Compact Disc
CMTS	Cable Modem Termination System
CS	Circuit Switched (leitungsvermittelnd)
DK	Dänemark
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
DSRL	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
DSS	Digital Signature Standard
DVD	Digital Versatile Disc
EDSRL	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)
EE	Estland
ELENA	Elektronisches Verfahren zum Einkommensnachweis
E-Mail	Electronic Mail
ENISA	European Network and Information Security Agency
ES	Spanien
ETSI	European Telecommunications Standards Institute
ETSI	European Telecommunications Standards Institute

FI	Finnland
FICORA	Finnish Communications Regulatory Authority
FR	Frankreich
GB	Großbritannien
GG	Grundgesetz
GR	Griechenland
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HU	Ungarn
IDS	Intrusion Detection System
IE	Irland
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMF	Internet Message Format
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Italien
LT	Littauen
LU	Luxemburg
LV	Lettland
MAC	Message Authentication Code / Media Access Control
MT	Malta
NL	Niederlande
PGP	Pretty Good Privacy
PL	Polen
POP	Post Office Protocol
PS	Packet Switched (paketvermittelnd)
PSTN	Public Switched Telephone Network
PT	Portugal
SI	Slowenien
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIP	Session Initiation Protocol
SK	Slowakei
SMTP	Simple Mail Transfer Protocol

SPAM	Unerwünschte E-Mails, die den Empfängern unverlangt zugestellt werden (meistens mit werbendem Inhalt)
SSH	Secure Shell
TCP	Transmission Control Protocol
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜV	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung) vom 3.11.2005 (BGBl. I, S. 3136), zuletzt geändert durch Artikel 4 des Gesetzes vom 25. Dezember 2008 (BGBl. I, S. 3083)
TLS	Transport Layer Security
TR TKÜV	Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten (TR TKÜV), Ausgabe 6.0 vom 2.12.2009
URI	Uniform Resource Identifier
VDS	Vorratsdatenspeicherung
VDSRL	Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG
VoIP	Voice over IP
WLAN	Wireless Local Area Network
WORM	Write Once Read Many
WORM	Write Once Read Many

ABBILDUNGSVERZEICHNIS

Seite

Abb. 1: Rechtssetzungssystematik in Bezug auf die Vorratsdatenspeicherung 6
Eigene Darstellung

Abb. 2: An den spezifischen Anforderungen des Datenschutzrechts orientierte Schutzzieldogmatik 10
Quelle: Rost/Bock: Privacy By Design und die Neuen Schutzziele, in: DuD 1/2011, S. 32

Abb. 3: Vermittlung einer Telefonverbindung über das leitungsgebundene Telefonfestnetz (schematisch) 14
Eigene Darstellung, angelehnt an Kühling/Elbracht: Telekommunikationsrecht, S. 36

Abb. 4: Schematische Struktur des Mobilfunknetzes 16
Quelle: Bundesnetzagentur: Konsultationsentwurf zu Anrufzustellung in einzelnen Mobilfunknetzen, S. 4

Abb. 5: Möglichkeiten des Zugangs zum Internet (schematisch) 17
Eigene Darstellung, in Anlehnung an Milford: The Data Retention Directive too fast, too fourious a response?, S. 43

Abb. 6: Exemplarischer *RADIUS*-Log bei erfolgreichem Aufbau einer ADSL-Verbindung 18
Quelle: Milford: The Data Retention Directive too fast, too fourious a response?, S. 13

Abb. 7: OSI-Referenzmodell mit zugehörigen Protokolleschichten im Internetverkehr 19
Eigene Darstellung, in Anlehnung an Stampfel/Ganster/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 18

Abb. 8: Protkollkopf eines IP-Pakets (IPv6) 20
Quelle: Tannenbaum: Computernetzwerke, S. 511

Abb. 9: Inhalte der Protokollköpfe auf den unterschiedlichen Schichten beim Versand einer E-Mail über das Internet 21
Eigene Darstellung, in Anlehnung an Freiling: Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, S. 5

Abb. 10: Ablauf einer E-Mail-Kommunikation nach dem *store&forward*-Prinzip und der verwendeten Kommunikationsprotokolle 22
Eigene Darstellung, in Anlehnung an Stampfel/Ganster/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 54 und Damker/Federrath/Schneider: Maskerade-Angriffe im Internet, S. 2

Abb. 11: Bestandteile der Übermittlung einer E-Mail unter Verwendung des SMTP-Protokolls 23
Eigene Darstellung, in Anlehnung an Stampfel/Ganster/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 56

Abb. 12: Exemplarischer mit Verkehrsdaten bestückter Header einer E-Mail-Nachricht (Betreff, aktuelle E-Mail und IP-Adressen wurden anonymisiert) 23
Quelle: Milford: The Data Retention Directive too fast, too fourious a response?, S. 16

Abb. 13: Exemplarischer Protokollkopf einer SIP-Gesprächsanfrage zur Telefonie über VoIP 24
Quelle: Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 114

Abb. 14: Gesetzliche Datenkategorien und deren Überschneidungen mit Beispielen 26
Eigene Darstellung

Abb. 15: Schutzinteressen der an der Vorratsdatenspeicherung beteiligten Akteure (exemplarisch am Beispiel Deutsche Telekom und Bundeskriminalamt) 27
Eigene Darstellung

Abb. 16: Schematische Darstellung des Wegs der Vorratsdaten aus den Kommunikationsnetzen / IT-Systemen der TK-Diensteanbieter / Netzbetreiber zu den Ermittlungsbehörden 29
Eigene Darstellung

Abb. 17: Schutzinteressen der Ermittlungsbehörden (mit Ausnahme der Vertraulichkeit) 30
Eigene Darstellung

Abb. 18: Potentielle Angriffsszenarien 32
Eigene Darstellung

Abb. 19: Verschleierung von Verkehrsdaten durch die Nutzung von Anonymisierungsdiensten 35
Eigene Darstellung

Abb. 20: Verschleierung von Verkehrsdaten durch die Nutzung eines SSH-Servers 36
Eigene Darstellung

Abb. 21: Nach Art. 5 I VDSRL zu speichernde Verkehrsdaten im Falle des Telefonanrufs von Alice an Bob im Festnetz 42
Eigene Darstellung

Abb. 22: Nach Art. 5 I VDSRL zu speichernde Verkehrsdaten im Falle des Telefonanrufs von Alice an Bob im Mobilfunknetz 43
Eigene Darstellung

Abb. 23: Nach Art. 5 I VDSRL zu speichernde Verkehrsdaten im Falle des Internetzugangs von Alice über das Telefonnetz 45
Eigene Darstellung

Abb. 24: Nach Art. 5 I VDSRL zu speichernde Verkehrsdaten im Falle des E-Mail-Verkehrs zwischen Alice und Bob 47
Eigene Darstellung

Abb. 25: Nationaler Umsetzungsstand der VDSRL im Vergleich 61
Eigene Darstellung, Datenquelle: Anhang, Abschnitt 1

Abb. 26: Nationale Speicherfristen im Vergleich 63
Eigene Darstellung, Datenquelle: Anhang, Abschnitt 1

Abb. 27: Nationale Zugriffsschwellen im Vergleich 64
Eigene Darstellung, Datenquelle: Anhang, Abschnitt 1

Abb. 28: Praktizierte Datentrennung im Vergleich 68
Eigene Darstellung, Datenquelle: Anhang, Abschnitt 4

Abb. 29: Praktizierte Verschlüsselung der Vorratsdaten im Vergleich 69
Eigene Darstellung, Datenquelle: Anhang, Abschnitt 4

Abb. 30: Protokollierung des Zugriffs auf die Vorratsdaten im Vergleich 70
Eigene Darstellung, Datenquelle: Anhang, Abschnitt 4

Abb. 31: Public Key Infrastruktur zur Übermittlung der Vorratsdaten 78
Eigene Darstellung

TABELLENVERZEICHNIS

Seite

Tab. 1: Exemplarischer DCR im Bereich der Festnetztelefonie 15
Eigene Darstellung, in Anlehnung an Milford: The Data Retention Directive too fast, too fourious a response?, S. 10

Tab. 2: Gewichtung der Schutzinteressen 38
Eigene Darstellung

Tab. 3: Exemplarisches Schema eines Datensatzes, der entsprechend Art. 5 VDSRL im Festnetzbereich zu speichern ist 41
Eigene Darstellung

Tab. 4: Exemplarisches Schema eines Datensatzes, der entsprechend Art. 5 I VDSRL im Mobilfunkbereich zu speichern ist 43
Eigene Darstellung

Tab. 5: Exemplarisches Schema eines Datensatzes, der entsprechend Art. 5 VDSRL vom ISP zu speichern ist 45
Eigene Darstellung, in Anlehnung an Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 47 f.

Tab. 6: Schema eines Datensatzes, der entsprechend Art. 5 VDSRL vom E-Mail-Anbieter zu speichern ist 46
Eigene Darstellung, in Anlehnung an Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 85 f.

Tab. 7: Nach Art. 5 I VDSRL zu speichernde Verkehrsdaten im Falle eines VoIP-Telefonats zwischen Alice und Bob 48
Eigene Darstellung

Tab. 8: Kategorien und Typen der zu speichernden Daten nach Art. 5 VDSRL 50
Eigene Darstellung

Tab. 9: Europarechtliche Vorgaben mit datensicherheitstechnischem und -organisatorischem Bezug 59
Eigene Darstellung

Tab. 10: Einfachgesetzliche Vorgaben mit datensicherheitstechnischem und -organisatorischem Bezug in Deutschland 76
Eigene Darstellung

A. EINFÜHRUNG

I. MOTIVATION UND HERANFÜHRUNG AN DAS THEMA

„Unser Leben wird in Bits und Bytes gespeichert, egal ob wir wollen oder nicht.“[1] Diese These aus einem Artikel einer bekannten Tageszeitung bringt die zunehmend empfundene Ohnmacht und Skepsis gegenüber modernen Informations- und Telekommunikationstechnologien zum Ausdruck. Doch ist uns die Kontrolle darüber, wer welche Informationen über uns besitzt, wer also was über uns weiß, wirklich bereits entglitten? Verfolgt man die Berichterstattung in den Medien, so zeichnet sich durchaus ein derartiges Bild ab. Der oberste Datenschützer Deutschlands, *Peter Schaar*, verkündete bereits im Jahr 2007 in einer Monographie mit dem Titel „Das Ende der Privatsphäre“ den „Weg in die Überwachungsgesellschaft“[2], der *Spiegel* fragt sich, ob die Privatsphäre noch zu retten ist[3] und das *Handelsblatt* bezeichnet Unternehmen und staatliche Stellen als „Datensammler vom Dienst“[4], so dass z.B. die „Datenkrake“[5] *Google* inzwischen nicht nur weiß, was dich im Internet interessiert und wie dein Haus aussieht, sondern auch „wo du bist“[6] und vielleicht auch bald was du tun wirst.

In der Tat wächst das Interesse staatlicher und privatwirtschaftlicher Stellen an personenbezogenen Daten stetig. Dies zeigt auch der Anstieg der weltweit verfügbaren Datenbestände, deren Größe inzw. auf 1,8 Zettabyte[7] geschätzt wird. Die zugrunde liegenden Motive zur systematischen Sammlung, Aggregation und Verarbeitung von Daten im wirtschaftlichen und staatlichen Bereich sind unterschiedlicher Natur.

Im privatwirtschaftlichen Bereich ist es vor allem das Streben nach Gewinn, das Online-Communities und die Werbebranche dazu veranlasst, möglichst viele Daten über potentielle Kunden zu sammeln. Der Unternehmenswert derartiger Unternehmen errechnet sich anhand von drei Kriterien: (1) Der Anzahl der Benutzer, (2) wie viel Zeit die Nutzer auf einer Webseite verbringen und (3) wie viele Daten diese von sich offen legen.[8] Der Großteil dieser Daten wird von den Nutzern derartiger Plattformen freigiebig zur Verfügung gestellt, ohne die datenschutzrechtliche Einwilligungserklärung vor der Zustimmung zu dieser zu lesen und ohne mögliche Auswirkungen, die sich daraus ergeben, dass die Daten im Internet weltweit einer breiten (oft unbegrenzten) Öffentlichkeit zur Verfügung stehen, kritisch zu reflektieren. Verschiedene Bereiche des Privatlebens, z.B. die Kommunikation mit Freunden und Bekannten werden teilweise sogar vollständig in die digitale Welt der sog. *Social Networks* verlagert.[9] Eine Kontrolle der Verbreitung der dabei zur Verfügung gestellten Informationen ist, sobald diese einmal in die digitale Welt gelangt sind, nahezu ausgeschlossen. Auch der in der Politik diskutierte „digitale Radiergummi“ hat sich technisch als Wunschvorstellung entpuppt.[10] Neben den allseits be-

---

[1] Artikel „Spur der Speicher“ von Constanze Kurz und Frank Rieger, in: FAZ, 17. April 2011, S. 28.
[2] So der zugespitzte Titel und Untertitel der im Jahr 2007 erschienenen Monographie von Peter Schaar.
[3] Artikel „Im Netz der Späher“ von Manfred Dworschak, in: DER SPIEGEL, 10.1.2011, S. 114 ff.
[4] Titel eines Online-Handelsblatt-Artikels vom 13. April 2011, im Internet abrufbar unter der URL http://www.handelsblatt.com/technologie/it-tk/mobile-welt/die-datensammler-vom-dienst/v_detail_tab_print,3015618.html.
[5] Artikel „Alles im Griff der Datenkrake“, in FOCUS ONLINE, 8.11.201, im Internet abrufbar unter der URL http://www.focus.de/finanzen/boerse/aktien/tid-20348/tid-20350/google-alles-im-griff-der-datenkrake_aid_569099.html.
[6] Vgl. Artikel „Google weiß, wo du bist“ von Götz Hamann und Marcus Rohwetter, in: ZEIT ONLINE, 26.2.2009, im Internet abrufbar unter der URL http://www.zeit.de/2009/07/Google.
[7] Vgl. Artikel „Zettabyte“, in: FAZ vom 30. Juni 2011, S. 2 (1 Zettabyte entspricht 1 Milliarde Terabyte).
[8] Vgl. Artikel „Spur der Speicher“ von Constanze Kurz und Frank Rieger, in: FAZ, 17. April 2011, S. 28.
[9] Hierzu kritisch Lanier: You are not a gadget, S. 3 ff.
[10] Vgl. Federrath/Fuchs/Hermann/Maier/Scheuer/Wagner: Grenzen des „digitalen Radiergummis“, in: DuD 6/2011, S. 407.

kannten Online-Communities existiert zudem eine Vielzahl an Unternehmen, die mit Hilfe von personenbezogenen Daten ihren Umsatz bestreiten. Ein Beispiel dafür ist das Unternehmen *Paypal*, das Informationen über unser Kauf- und Konsumverhalten sammelt, oder die *Schober Information Group*, die mit sensiblen personenbezogenen Daten, explizit mit 50 Mio. Privatadressen inklusive Familienstand Kontodaten und 5,5 Mio. Firmendaten (Betriebsgröße, Umsatz, Branche, Entscheider-Typologie und akademischer Grad der Führungskräfte) handelt.[11] In Bezug auf all diese Beispiele darf jedoch nicht vergessen werden, dass es zumeist in der Hand der Informationserbringer liegt, wo bzw. wem eigene Daten zur Verfügung gestellt werden. Dementsprechend ist die eingangs zitierte These jedenfalls im privatwirtschaftlichen Bereich zu relativieren.

Im staatlichen Bereich sind es vorrangig sicherheitspolitische Erwägungen, die zur vermehrten Erhebung, Verarbeitung, Speicherung und Übermittlung von Daten führen. Im Unterschied zu den o.g. privatwirtschaftlichen Beispielen liegt es hier zumeist nicht in der Hand des einzelnen Individuums, sich der Datenerhebung oder Speicherung zu entziehen und so frei über die (Nicht-)Herausgabe seiner personenbezogenen Daten zu entscheiden. Betrachtet man die Sicherheitsgesetzgebung in Deutschland, so findet man eine Vielzahl an Beispielen, die in den letzten Jahren zu einer verstärkten Zunahme der Datenerhebung und Datensammlung durch staatliche Stellen geführt hat: So wurden z.B. im Jahr 1994 die Befugnisse des Bundesnachrichtendienstes zur Überwachung, Aufzeichnung und Auswertung des Telekommunikationsverkehrs ausgeweitet.[12] Dem folgte das Gesetz zur Bekämpfung des internationalen Terrorismus von 2002[13], das den Sicherheitsbehörden des Bundes neue Datenerhebungs- und Austauschmöglichkeiten einräumte und das Antiterrordateigesetz von 2006[14], das zu einer von 38 Ermittlungsbehörden gemeinsam genutzten Personendatenbank führte. Den vorläufigen Höhepunkt staatlich initiierter Datensammlung aus Sicherheitsgründen in Deutschland stellt die Umsetzung[15] der Vorratsdatenspeicherungsrichtlinie in das deutsche Telekommunikationsgesetz Ende 2007 dar.

Die zunehmende Erhebung, Speicherung, Vernetzung und Auswertung von Daten durch öffentliche und private Stellen führt zu einer zunehmenden Bedrohungskulisse im Hinblick auf den Schutz der Privatsphäre des Einzelnen. Vor dem Hintergrund der soeben aufgezeigten Entwicklungen warnen Datenschützer und das Bundesverfassungsgericht in seiner Funktion als Hüter der Grundrechte verstärkt vor den Gefahren für das Recht auf informationelle Selbstbestimmung, das „die Befugnis des Einzelnen [beinhaltet] grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“[16]. Sie mahnen einerseits den Gesetzgeber zur Einhaltung des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes. Andererseits fordern sie die erhebenden und verarbeitenden Stellen, ob privat oder staatlich, zur Einhaltung der datenschutzrechtlichen Vorschriften, die dafür sorgen sollen, dass das Recht auf informationelle Selbstbestimmung trotz verstärkter Datenerhebung und -aggregation nicht verletzt wird, auf. Aus datenschutzrechtlicher Sicht bedeutet dies z.B., dass personenbezogene Daten nur innerhalb des gesetzlich festgelegten oder privatautonom vereinbarten

[11] Vgl. Artikel „Die Datensammler vom Dienst“, in: Handelsblatt, 13. April 2011, im Internet abrufbar unter der URL http://www.handelsblatt.com/technologie/it-tk/mobile-welt/die-datensammler-vom-dienst/v_detail_tab_print,3015618.html.
[12] Vgl. BGBl. 1994 I, S. 3186 und zugehörige BVerfG-Entscheidung (BVerfGE 100, 313).
[13] Vgl. BGBl.2002 I, S. 361, berichtigt auf S. 3142.
[14] Vgl. BGBl. 2006 I, S. 3409.
[15] Vgl. BGBl. 2007 I, S. 3198, im Internet abrufbar unter der URL http://www.bgbl.de/Xaver/text.xav?bk=Bundesanzeiger_BGBl&start=%2F%2F*[%40attr_id%3D%27bgbl107s3307.pdf%27]&wc=1&skin=WC.
[16] BVerfGE 65, 1 (43).

Zwecks erhoben und verwendet werden dürfen, während ihrer Verwendung gegen unbefugte Kenntnisnahme zu schützen sind und – sofern sie für den erhobenen Zweck nicht mehr benötigt werden – zu löschen oder anonymisieren sind.

Die Umsetzung der datenschutzrechtlichen Vorschriften und der ausreichende Schutz der Datensammlungen vor Datenmissbrauch stellen eine komplexe Herausforderung für privatwirtschaftliche Unternehmen und staatliche Stellen dar. Dass diese in Bezug auf den Schutz der personenbezogenen Daten oftmals überfordert sind bzw. zu leichtfertig oder in manchen Fällen gar vorsätzlich rechtswidrig mit sensiblen Daten umgehen, zeigt die nicht zu vernachlässigende Anzahl von Datenskandalen in den letzten Jahren: So hat die *Deutsche Bahn AG* in den Jahren 2002/2003 eigenmächtig die Daten von 173.000 Mitarbeitern mit den Daten von 80.000 Lieferanten abgeglichen, um ihre Mitarbeiter auf Korruptionsverdacht zu überprüfen[17]. Die *Deutsche Telekom AG* hat in den Jahren 2005/2006 eigenmächtig Verbindungsdaten von Aufsichtsräten, Journalisten und eigenen Mitarbeitern überwacht, um die Veröffentlichung vertraulicher Informationen zu unterbinden.[18] Zudem häufen sich Meldungen von Datendiebstählen. Schlagzeilen wie „Telekom Datenskandal – Daten von 17 Millionen Kunden gestohlen“[19], „Millionen Bankdaten illegal im Umlauf“[20] (21 Mio. Datensätze), „*Sony* entschuldigt sich für Datenklau bei seinen Kunden“[21] (77 Mio. Datensätze), „Hacker klauen *Sega* Millionen Kundendaten“[22] (1,3 Mio. Datensätze) deuten, wenn nicht auf eine strukturelle Insuffizienz des Datenschutzrechts, jedenfalls auf ein datenschutzrechtliches Vollzugsdefizit „schrecklichen Ausmaßes“[23] hin. Sie bestätigen auch einen erheblichen Nachholbedarf in Bezug auf die technische Absicherung der Daten. Auch Behörden und staatliche Stellen sind von der negativen Datenschutzberichterstattung nicht ausgenommen: So soll z.B. das Bundeskriminalamt nach den Terroranschlägen vom 11. September 2001 ohne Rechtsgrundlage Millionen von Kundendaten von der Telekom zur systematischen Auswertung erhalten haben.[24] Die Polizei in Dresden erfasste bei einer Demonstration im Februar 2011 in rechtswidriger Weise mehr als eine Million Verbindungsdaten aller Handynutzer, die sich in bestimmten Stadtteilen befanden (Anwohner, Demonstranten, Journalisten, Anwälte, Politiker und Einsatzkräfte) per Funkzellenauswertung.[25] Und sogar auf Computern der Bundesregierung sollen 2007 monatelang vermutlich sensible Informationen mit Hilfe von Spionagesoftware nach China gesendet und Datenbe-

---

[17] vgl. Artikel „Datenskandal - Bahn schaltet Staatsanwaltschaft ein“, in: SPIEGEL-ONLINE, 30. Januar 2009, im Internet abrufbar unter der URL http://www.spiegel.de/wirtschaft/0,1518,604541,00.html.

[18] vgl. Artikel „Telekom bespitzelte auch eigene Mitarbeiter“, in: SPIEGEL-ONLINE, 25.10.2008, im Internet abrufbar unter der URL http://www.spiegel.de/wirtschaft/0,1518,586516,00.html.

[19] Vgl. Artikel „Daten von 17 Millionen Kunden gestohlen“, in: ZEIT-ONLINE, 4. 10. 2008, im Internet abrufbar unter der URL http://www.zeit.de/online/2008/41/telekom-datenklau.

[20] vgl. Artikel „Millionen Bankdaten illegal im Umlauf“, in: sueddeutsche.de-Digital, 6.12.2008, abrufbar unter der URL http://www.sueddeutsche.de/digital/2.220/zeitschrift-millionen-bankdaten-illegal-im-umlauf-1.373504.

[21] Vgl. Artikel „Sony entschuldigt sich für Datenklau bei seinen Kunden“, in: FAZ, 2.5.2011, S. 11.

[22] Vgl. Artikel „Hacker klauen Sega Millionen Kundendaten“, in: Sueddeutsche.de, 19.6.2011, im Internet abrufbar unter der URL http://www.sueddeutsche.de/digital/angriff-auf-videospiel-firma-hacker-klauen-sega-millionen-kundendaten-1.1110158.

[23] So das Ergebnis einer Untersuchung des praktizierten Datenschutzes im Bereich der Telemedien, Kühling/Sivridis/Schwuchow/Burghardt: Das datenschutzrechtliche Vollzugsdefizit im Bereich der Telemedien – ein Schreckensbericht, in: DuD 6/2009, S. 342.

[24] Vgl. Artikel “Telekom soll BKA mit Millionen Kundendaten beliefert haben“, in: SPIEGEL-ONLINE, 2.4.2009, im Internet abrufbar unter der URL http://www.spiegel.de/wirtschaft/0,1518,617044,00.html.

[25] Vgl. Artikel „Polizei wertete Tausende Handy-Daten aus“, in: SPIEGEL-ONLINE, 19.6.2011, im Internet abrufbar unter der URL http://www.spiegel.de/netzwelt/web/0,1518,769275,00.html und Artikel „Sachsens Polizei spähte mehrere Stadtteile aus“, in: SPIEGEL-ONLINE, 24.6.2011, im Internet abrufbar unter der URL http://www.spiegel.de/netzwelt/netzpolitik/0,1518,770473,00.html.

stände unbemerkt verändert worden sein.[26] Neben diesen punktuellen Beispielen bestätigt ein im August 2011 veröffentlichter Sicherheitsbericht der Sicherheitsfirma *McAfee* das Ausmaß einer systematischen digitalen Spionage in 70 globalen Unternehmen, Regierungen und Non-Profit-Organisationen während der letzten fünf Jahre.[27]

Diese Beispiele bestätigen die zunehmende Bedeutung und Erforderlichkeit von technischen und organisatorischen Sicherheitsmaßnahmen zum Schutz von sensiblen Daten vor Datenmissbrauch und deuten auf einen in der Praxis erheblich ausgeprägten Anpassungs- und Nachholbedarf hin. In diesem Themenfeld bewegt sich die vorliegende Magisterarbeit. Am Beispiel der Vorratsdatenspeicherung wird untersucht, inwieweit der Gesetzgeber und die Telekommunikationsdiensteanbieter der Gefahr des Datenmissbrauchs in rechtlicher und praktischer Hinsicht mit technischen und organisatorischen Sicherheitsmaßnahmen versuchen zu begegnen. Vor allem der Gesetzgeber ist als Initiator der Vorratsdatenspeicherung in der Pflicht, die den „Datenpools" innewohnenden Missbrauchsgefahren mit der gesetzlichen Normierung eines hohen Sicherheitsstandards entgegenzuwirken.

Dass komplexe sicherheitstechnische Anforderungen sogar zum Scheitern gesamtstaatlicher IT-Projekte führen können, zeigt aktuell die Einstellung des *ELENA*-Verfahrens.[28] Die sicherheitstechnischen Vorgaben und die tatsächliche Absicherung der Daten im Rahmen der Vorratsdatenspeicherung können insofern auch als Indikator für die Sensibilität und Fähigkeit staatlicher und wirtschaftlicher Akteure gesehen werden, sicherheitstechnische Schutzziele im Rahmen zukünftiger IT-Projekte ausreichend zu adressieren.

II. Grundsätzliches zur Vorratsdatenspeicherung

Der Begriff Vorratsdatenspeicherung bezeichnet in der rechtspolitischen Debatte die rechtliche Verpflichtung von Telekommunikationsunternehmen, Daten über die Kommunikationsumstände (wer hat mit wem, wann, wie lange, von wo aus kommuniziert) ihrer Nutzer über einen bestimmten Zeitraum hinweg zu speichern, so dass diese unter bestimmten Voraussetzungen an staatlichen Ermittlungsbehörden zur Verhinderung und Verfolgung von Straftaten übermittelt werden können. Initiator der Speicherverpflichtung ist die Europäische Union, die in der Richtlinie 2006/24/EG alle Mitgliedstaaten verpflichtete, die Speicherverpflichtung über einen Zeitraum von sechs bis 24 Monaten in ihren Rechtsordnungen zu verankern. Betroffen sind die Bereiche des Festnetz- und Mobilfunks, des Internetzugangs, E-Mail-Verkehrs und der *VoIP*-Telefonie.

Die sog. Kommunikationsumstände sind für Ermittlungsbehörden besonders interessant. In Anbetracht dessen, dass der Großteil zwischenmenschlicher Kommunikation heutzutage über elektronische Telekommunikationsinfrastrukturen abgewickelt wird, ermöglicht die Auswertung der gespeicherten Daten ein umfassendes Gesamtbild über das soziale Umfeld von Personen, deren Vorlieben und Gewohnheiten, deren Einbindung in Organisationsstrukturen und teilweise sogar deren Bewegungsprofile. Im

[26] Vgl. Meldung des CCC „Online-Durchsuchung bei der Bundesregierung" vom 27.08.2007, im Internet abrufbar unter der URL http://www.ccc.de/updates/2007/trojanerbeimbund.
[27] Vgl. Alperovitch: An investigation of targeted intrusions into 70+ global companies, governments and non-profit organizations during the last 5 years, August 2011, im Internet abrufbar unter der URL http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.
[28] Vgl. Pressemitteilung des BMWi vom 18.7.2011, im Internet abrufbar unter der URL http://www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen,did=424742.html.

Gegensatz zu den übermittelten Telekommunikationsinhalten können die sog. Verkehrsdaten größtenteils automatisiert ausgewertet werden.

Die Verpflichtung der Telekommunikationsanbieter, die Verkehrsdaten der nahezu gesamten Bevölkerung verdachtsunabhängig auf Vorrat zu speichern, um diese zur späteren anlassbezogenen Übermittlung an Ermittlungsbehörden bereitzuhalten, bricht gleichermaßen mit zweierlei rechtlichen Traditionen.

Einerseits im Bereich des Sicherheitsrechts: Während die Einschränkung von Grundrechtspositionen aufgrund sicherheitsrelevanter Überlegungen früher nur bei Vorliegen einer Gefahr bzw. eines konkreten Verdachts gerechtfertigt werden konnte, wird im Rahmen der Vorratsdatenspeicherung vorsorglich und verdachtsunabhängig in einer noch nie dagewesenen Streubreite in das Telekommunikationsgeheimnis der nahezu gesamten Bevölkerung eingegriffen.[29] Dies bestätigt die tendenzielle Entwicklung hin zu einer eher proaktiven Gefahrenabwehr, die unter anderem auf das zuletzt durch den Doppelanschlag in Norwegen gesteigerte Sicherheitsbedürfnis in der Bevölkerung zurückzuführen ist. Der Staat soll in der Lage sein, Gefahren abzuwenden, die bisher außerhalb unserer Kontrolle lagen. Der „Traum einer risikofreien Gesellschaft“[30] erscheint jedoch auch durch die Vorratsdatenspeicherung nicht in Erfüllung zu gehen. So konnte auch die Vorratsdatenspeicherung in Norwegen die schrecklichen Anschläge nicht verhindern.

Der zweite Paradigmenwechsel, den die Vorratsdatenspeicherung mit sich bringt, betrifft den Bereich des Datenschutzrechts. Aufgrund der Sensibilität von Verkehrsdaten war deren Speicherung vor Einführung der Vorratsdatenspeicherung grundsätzlich verboten. Nur punktuelle Ausnahmen erlaubten deren Speicherung, z.B. sofern diese zu Abrechnungszwecken benötigt wurden. Mit Einführung der Vorratsdatenspeicherung wurde dieses grundsätzliche Speicherverbot in eine grundsätzliche Speicherpflicht gewandelt und damit im Rahmen der Abwägung zwischen Privatsphäre und kollektivem Sicherheitsinteresse Zweiterem ein deutlich stärkeres Gewicht zugemessen.

Abzugrenzen ist die Vorratsdatenspeicherung vom sog. Quick Freeze-Verfahren, das in den USA praktiziert wird. Bei diesem Verfahren werden Daten über die Kommunikationsumstände nicht umfassend vorsorglich gespeichert. Die Speicherung erfolgt erst auf einen konkreten Anfangsverdacht hin und nur beschränkt auf die verdächtigte Person bzw. den verdächtigten Personenkreis.

III. Zielsetzung und Betrachtungsverlauf

Ziel der vorliegenden Magisterarbeit ist es, das rechtliche Framework und die praktische Implementierung des Ermittlungsinstruments der Vorratsdatenspeicherung in Europa aus Sicht der IT-Sicherheit, vorrangig der Datensicherheit, analytisch und vergleichend zu betrachten und zu bewerten.

In einem knappen, der eigentlichen Untersuchung vorangestellten Teil (Kapitel B.), werden zunächst die grundlegenden Begrifflichkeiten und Schutzziele des Fachbereichs der IT-Sicherheit im Kontext des Datenschutzrechts sowie die unterschiedlichen Datenkategorien, zwischen denen der Gesetzgeber unterscheidet, dargestellt. Soweit für die nachfolgende Betrachtung erforderlich, erfolgt hierbei eine

[29] Vgl. BVerfG, Urteil vom 2. März 2010, Az.: 1 BvR 256/08, Rn. 210.
[30] Vgl. Rauhofer: The Retention of Communications Data in Europe and the UK, in: Edwards/Waelde (Hrsg.): Law and the Internet, S. 598.

technische Konkretisierung der entsprechenden Daten. Dies erfordert im Hinblick auf die sog. Verkehrsdaten eine kurze Darstellung der gegenwärtig verwendeten Telekommunikationsinfrastrukturen.

Ausgangspunkt und Maßstab der abschließenden Bewertung der rechtlichen und praktischen Ausgestaltung der Sicherheit der Vorratsdaten ist die Identifikation der Schutzinteressen aller an der Vorratsdatenspeicherung beteiligten Entitäten und der damit korrespondierenden denkbaren Angriffsszenarien (Kapitel C.). Diese geben Auskunft über die Höhe des theoretisch erforderlichen Aufwands bzw. die Stärke der erforderlichen Anstrengung zur Gewährleistung eines ausreichenden Sicherheitsniveaus der Vorratsdaten.[31] Die Benennung aller Schutzinteressen ermöglicht die anschließende Ermittlung eines Deltas zwischen der theoretisch wünschenswerten und der rechtlich-praktischen Ausgestaltung der Sicherheitsmaßnahmen zum Schutz der Vorratsdaten (vgl. die Fazite in Kapitel D. und E.).

Die Reihenfolge der Analyse und Bewertung orientiert sich primär an der dogmatischen und zeitlichen Wirkungsweise der rechtlichen Vorgaben.

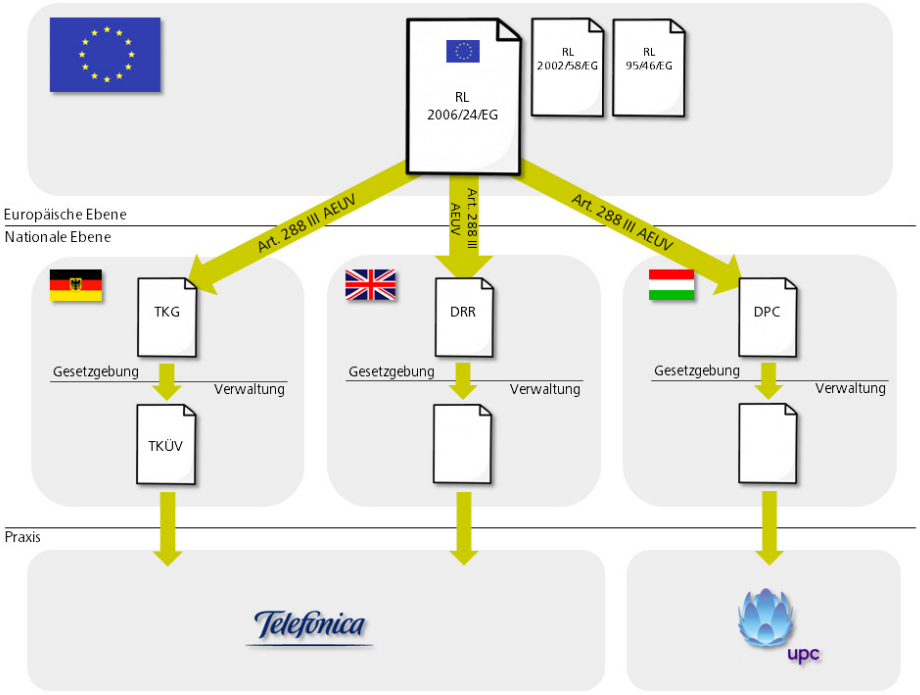


Abb. 1: Rechtssetzungssystematik in Bezug auf die Vorratsdatenspeicherung

So werden in Kapitel D. zunächst die einen datensicherheitstechnischen Bezug aufweisenden europarechtlichen Vorschriften dargestellt und konkretisiert. Hierbei werden die einzelnen Vorschriften den in Kapitel C. skizzierten Schutzzielen zugeordnet, um im Ergebnis das für die Vorratsdaten geltende, europarechtlich normierte Sicherheitsniveau zu bewerten. Zudem werden die Vorgaben in Bezug auf die zu speichernden Datenkategorien, die Speicherdauer, die Zweckbindung und das Übermittlungsverfahren herausgearbeitet, weil diese Rückschlüsse auf sicherheitsspezifische Rahmenbedingungen wie die Größe, Zusammensetzung und Sensibilität der zu speichernden Datenmengen sowie den Umfang des rechtlich zulässigen Nutzerkreises ermöglichen.

[31] Vgl. zu diesen Kriterien Müller: IT-Sicherheit mit System, S. 28.

Da die europarechtlichen Vorgaben nicht unmittelbar verpflichtend für die Telekommunikationsbetreiber sind, sondern zuvor von den Rechtsetzungsorganen der einzelnen Mitgliedstaaten in nationales Recht umgesetzt werden müssen, werden in Kapitel E. die einzelstaatlichen Umsetzungen der europarechtlichen sicherheitstechnischen Vorgaben skizziert und miteinander verglichen. Dies ermöglicht Aussagen über das rechtlich verbindlich zu gewährleistende europaweite Sicherheitsniveau der Vorratsdaten. Um den Umfang der Arbeit nicht zu sehr ausufern zu lassen, erfolgt die rechtliche Betrachtung der nationalen Umsetzungen nur bis zur Ebene der einfachen Gesetze, die im Vergleich zu den europäischen Vorgaben schon etwas konkreter ausgestaltet sind, aber immer noch einen hohen Abstraktionsgrad aufweisen.[32] Der Untersuchung der rechtlichen Vorgaben folgt ein erster Blick auf die in der Praxis betriebene sicherheitstechnische und organisatorische Absicherung der Vorratsdaten. Anhand der Ergebnisse einer Untersuchung[33] der *Artikel-29-Datenschutzgruppe*[34] wird aufgezeigt, welche Sicherheitsmaßnahmen konkret von den Telekommunikationsdiensteanbietern in Europa ergriffen wurden, um die Vorratsdaten vor Beeinträchtigungen der in Kapitel C. aufgezeigten Schutzziele zu schützen.

In Kapitel F. verengt sich der Fokus der Betrachtung auf die Umsetzung bzw. die Umsetzungsgeschichte der Vorratsdatenspeicherung in Deutschland. Der Analyse und Bewertung der rechtlichen sicherheitstechnischen Vorgaben folgt die Darstellung der sicherheitsspezifischen Aspekte des Urteils des Bundesverfassungsgerichts. Dieses hat die Vorratsdatenspeicherung unter anderem aufgrund mangelhafter gesetzlicher sicherheitstechnischer Vorgaben für nichtig erklärt. Um festzustellen, ob sich diese gesetzgeberischen Mängel in der praktischen Absicherung der Vorratsdaten bei den Telekommunikationsunternehmen widerspiegelt, folgt anschließend die Untersuchung der implementierten Sicherheitsmaßnahmen bei drei in Deutschland und insbesondere in Bayern tätigen Telekommunikationsanbietern.

Abschließend erfolgt eine kritische Bewertung der rechtlichen und praktischen Ausgestaltung der Vorratsdatenspeicherung aus Sicht der IT-Sicherheit.

[32] Eine Einbeziehung der Verwaltungsvorschriften erfolgt in diesem Abschnitt nur in dem Maße, in dem diese von der Europäischen Kommission im Rahmen ihrer Evaluation erfolgte.
[33] Vgl. Artikel-29-Datenschutzgruppe: Bericht 01/2010.
[34] Die Artikel-29-Datenschutzgruppe ist ein unabhängiges europäisches Gremium, das die EU-Kommission in Datenschutzfragen berät.

B. Technische und rechtliche Grundlagen

Im Folgenden werden die grundlegenden Begrifflichkeiten des Fachbereichs der IT-Sicherheit im Kontext des Datenschutzrechts knapp beschrieben. Zudem werden die verschiedenen juristischen Datenkategorien zwischen denen der Gesetzgeber unterscheidet kurz dargestellt. Soweit für die nachfolgende Betrachtung erforderlich, erfolgt hierbei eine technische Konkretisierung der entsprechenden Daten. Dies erfordert im Hinblick auf die sog. Verkehrsdaten eine kurze Darstellung der gegenwärtig verwendeten Telekommunikationsinfrastrukturen.

I. Grundlagen der IT-Sicherheit

1. Begriff der IT- und Datensicherheit im Kontext des Datenschutzes

Der Begriff der IT-Sicherheit – ausführlich Sicherheit der Informationstechnik – bezeichnet „den Zustand eines IT-Systems oder eines IT-Prozesses, in dem die Risiken, die beim Einsatz dieses Systems oder des Prozesses aufgrund von Gefährdungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind.“[35] In Abhängigkeit vom Betrachtungsgegenstand kann das Themenfeld der IT-Sicherheit in die Teilbereiche der Funktionssicherheit, der Informationssicherheit und der Datensicherheit unterteilt werden.[36]

Die Funktionssicherheit eines Systems fokussiert die im System enthaltenen Funktionalitäten und ist damit die Grundlage eines vertrauenswürdigen Systems. Sie ist gegeben, wenn die „Ist-Funktionalität der verschiedenen Komponenten mit deren spezifizierter Soll-Funktionalität übereinstimmt“[37].

Die Informationssicherheit bezieht sich auf die im System enthaltenen semantischen Informationen. Informationssicher ist das System dann, wenn es nur solche Systemzustände annimmt, „die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen“ [38].

Die Eigenschaft der Datensicherheit fokussiert die Daten in ihrer physikalischen Form und geht noch etwas weiter als die Informationssicherheit. Datensicherheit umfasst zusätzlich Maßnahmen zur Absicherung der Daten vor Datenverlust. Um Datensicherheit zu gewährleisten, darf das System „nur solche Systemzustände annehmen, die zu keinem unautorisierten Zugriff auf Systemressourcen und insbesondere auf Daten führen“[39].

Neben dieser Unterteilung existiert eine Vielzahl an gleichwertigen Unterteilungen des Fachbereichs der IT-Sicherheit, wie z.B. in *security* (Angriffssicherheit) als Schutz gegen beabsichtigte Angriffe und *safety* (Betriebssicherheit) als Schutz vor unbeabsichtigten/zufälligen Ereignissen.[40] Gemeinsam ist allen Systematisierungsversuchen, dass sie auf Kategorisierungen der verschiedenen Bedrohungsszenarien und damit korrespondierender Schutzziele beruhen.

---

[35] Vgl. Reinhard/Pohl/Capellaro: IT-Sicherheit und Recht, S. 352.
[36] Vgl. Eckert: IT-Sicherheit, S. 4.
[37] Vgl. Eckert: IT-Sicherheit, S. 4.
[38] Vgl. Eckert: IT-Sicherheit, S. 4.
[39] Vgl. Eckert: IT-Sicherheit, S. 4.
[40] Vgl. Federrath: Sicherheit im Netz, in: Moritz/Dreier (Hrsg.): Rechts-Handbuch zum E-Commerce, S. 2.

Vor welchen Gefährdungen ein IT-System zu schützen ist, ergibt sich aus dem jeweiligen Kontext. Im datenschutzrechtlichen Kontext[41] wird der Begriff der Datensicherheit als das „Ergebnis des Einsatzes geeigneter und ausreichender Maßnahmen der Datensicherung[42]“ definiert, „die eine wesentliche Voraussetzung sind, um einen gezielten Datenschutz zu gewährleisten“[43], insbesondere personenbezogene Daten vor Missbrauch bei der Datenverarbeitung zu schützen. Datensicherheit ist hiernach als das Ergebnis eines nicht endenden Prozesses der Datensicherung, der die Grundvoraussetzung für die Gewährleistung eines wirksamen Datenschutzes darstellt, anzusehen.

Ohne ausreichenden technischen und organisatorischen Schutz der Daten sind eine Kontrolle z.B. des Kreises der Zugangsberechtigten und damit ein effektiver Schutz der datenschutzrechtlichen Rechte der betroffenen Personen unmöglich. Die Datensicherheit fokussiert hierzu spezielle Techniken, deren Gestaltung sich „im Hinblick auf die Verarbeitung personenbezogener Daten am Ziel Datenschutz orientiert.“[44] Diese Verschränkung von Recht und Technik wird als „regulierte Selbstregulierung“[45] bezeichnet. Die verwendeten Techniken, wie z.B. Verschlüsselungsverfahren, Message Authentication Codes und Digitale Signaturen bilden das „Rückgrat des Datenschutzes in IT-Systemen“[46].

Da im Rahmen der vorliegenden Arbeit vorrangig Aspekte der durch die Vorratsdatenspeicherung ausgelösten Datensammlungen behandelt werden, werden im Folgenden die Begriffe IT-Sicherheit und Datensicherheit gleichbedeutend verwendet. Diese umfassen im Rahmen dieser Arbeit alle im Rahmen der Vorratsdatenspeicherung zu berücksichtigenden Schutzziele (siehe Kapitel C.). Der Begriff „Sicherheit“ ist zudem dynamisch zu verstehen. Die Sicherheit der Daten kann wie ein Risiko Werte annehmen, der Begriff deckt sich also inhaltlich mit dem Begriff Sicherheitsniveau.[47] Das Sicherheitsniveau gibt Auskunft darüber, ob und inwieweit die im konkreten Fall zu gewährleistenden Schutzziele erreicht wurden.

2. Die IT-Schutzzieldogmatik im Kontext des Datenschutzrechts

Schutzziele dienen im Bereich der IT-Sicherheit dazu, verschiedene Bedrohungsszenarien und wünschenswerte Systemeigenschaften zu kategorisieren und zusammenzufassen, um eine systematisierte Betrachtung und Bewertung des Sicherheitsniveaus eines konkreten IT-Systems zu ermöglichen. Die drei bedeutendsten Schutzziele der IT-Sicherheit sind die Verfügbarkeit, Integrität und Vertraulichkeit von Daten. Seitdem hat sich die Dogmatik der Schutzziele weiter ausdifferenziert[48] und an die Anforderungen des modernen Datenschutzes angepasst. Zu den klassischen Schutzzielen der Vertraulichkeit, Integrität und Verfügbarkeit traten u.a. Schutzziele, die nicht die Informationsinhalte sondern das Informationsumfeld betreffen, sowie die speziell datenschutzspezifischen Schutzziele der Transparenz, Nichtverkettbarkeit und Intervenierbarkeit.[49] Die in der folgenden Abbildung jeweils gegenüberlie-

[41] Vgl. zur Abgrenzung von Datensicherheit und Datenschutz Sicherheit im Netz, in: Moritz/Dreier (Hrsg.): Rechts-Handbuch zum E-Commerce, S. 1.
[42] Der Begriff „Datensicherung“ wird in der aktuellen politischen Diskussion auch als Synonym für das „Quick Freeze“-Verfahren gebraucht; in der vorliegenden Arbeit wird Datensicherung nur in seiner Bedeutung als Prozess der Herstellung von Datensicherheit verstanden; ebenso Ernestus in: Roßnagel (Hrsg.): Handbuch Datenschutzrecht, S. 270.
[43] Wildhaber: Informationssicherheit, S. 17.
[44] Federrath/Pfitzmann in: Roßnagel (Hrsg.): Handbuch Datenschutzrecht, S. 63 ‚Rn. 7.
[45] Gusy: Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, in: DuD 1/2009, S. 35.
[46] Federrath/Pfitzmann in: Roßnagel (Hrsg.): Handbuch Datenschutzrecht, S. 84, Rn. 85.
[47] Vgl. Müller: IT-Sicherheit mit System, S. 28.
[48] Vgl. Pfitzmann/Rost: Datenschutz-Schutzziele – revisited, in: DuD 6/2009, S. 353 ff.
[49] Vgl. Rost/Bock: Privacy By Design und die Neuen Schutzziele, in: DuD 1/2011, S. 32.

genden Schutzziele zielen in gegensätzliche Richtungen. So ist z.B. im Rahmen der Vertraulichkeit zu gewährleisten, dass der unberechtigte Zugriff auf bestimmte Daten durch einen bestimmten Personenkreis verhindert wird. Im Rahmen der Verfügbarkeit ist dagegen zu gewährleisten, dass bestimmte Daten oder Dienste einem bestimmten Personenkreis zur Verfügung stehen. Widersprechen müssen sich diese beiden Schutzziele dennoch nicht. Die Grenze zwischen diesen bestimmen die datenschutzrechtlichen Befugnisnormen, so dass berechtigte Personen auf die Daten zugreifen können – nicht berechtigte Personen jedoch nicht.

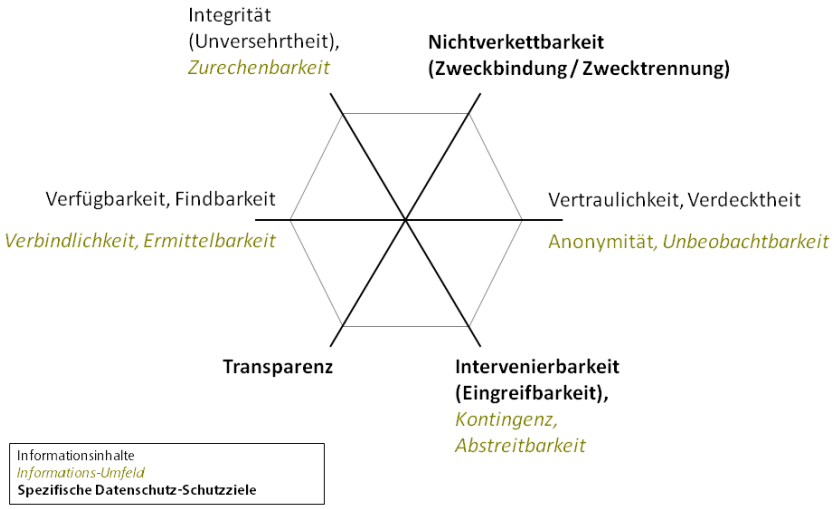


Abb. 2: An den spezifischen Anforderungen des Datenschutzrechts orientierte Schutzzieldogmatik

Anschließend werden die Begrifflichkeiten der grundlegenden Schutzziele kurz erläutert. Welche Schutzziele im Rahmen der Vorratsdatenspeicherung konkret zu gewährleisten sind, wird in Kapitel C.) beschrieben.

a) Verfügbarkeit

Verfügbarkeit bedeutet, dass „etwas für ein spezifisches Ziel an einem bestimmten Ort und zu einer bestimmten Zeit nutzbar einsetzbar ist“[50]. Ist Verfügbarkeit in Bezug auf bestimmte Daten sichergestellt, so wird gewährleistet, dass „authentifizierte und autorisierte Subjekte in der Wahrnehmung ihrer Berechtigungen [– dem rechtmäßigen Zugriff auf die Daten –] nicht unautorisiert beeinträchtigt werden können“[51]. Maßnahmen zur Sicherstellung der Verfügbarkeit von Daten sind folglich darauf ausgerichtet, vor unbefugter oder zufälliger Beeinträchtigung der Bereitstellung bestimmter Dienstleistungen in „definierter Qualität und Zeit“[52] – im konkreten Beispiel der Bereitstellung von Daten – zu schützen. Techniken hierzu stellen z.B. der Aufbau redundanter verteilter Strukturen, Backup-Lösungen und die Einführung von Quoten dar. In der vorliegenden Arbeit wird die Verfügbarkeit der Vorratsdaten weit interpretiert, so dass auch die verschiedenen Methoden, die von vornherein das Anfallen von aussagekräftigen Vorratsdaten bei den Telekommunikationsunternehmen unterbinden, als Angriffe auf die Verfügbarkeit der Vorratsdaten angesehen werden.

[50] Wildhaber: Informationssicherheit, S. 19.
[51] Eckert: IT-Sicherheit, S. 9.
[52] Coester/Hein: IT-Sicherheit für den Mittelstand, S. 29.

b) Vertraulichkeit

Unter Vertraulichkeit von Daten versteht man deren Schutz vor unbefugtem Informationsgewinn. Es muss ausgeschlossen werden können, dass Informationen von unautorisierten Subjekten zur Kenntnis genommen werden können. Ohne eine technische wirkungsvolle Beschränkung und Kontrolle des Zugangs zu Informationen liefe der Großteil der datenschutzrechtlichen Bestimmungen weitestgehend in die Leere. Bezugsobjekt der Vertraulichkeit können neben den Inhalten von Dateien und Nachrichten auch Verkehrsdaten sein. So kann zum Beispiel in bestimmten Fällen ein berechtigtes Interesse an Anonymität der Kommunikationspartner (z.B. anonyme Kontaktmöglichkeiten mit Suchtberatungsstellen) und Unbeobachtbarkeit einer Kommunikation (z.B. zum Informantenschutz im Pressewesen) bestehen. Es existiert eine Vielzahl von Techniken zum Schutz der Vertraulichkeit von Daten und Informationen. Exemplarisch seien physische Zugangskontrollen, Authentifizierungsmechanismen, kryptographische Verfahren, Labeling-Techniken und Anonymisierungstechniken wie Mix-Kaskaden oder Onion Routing aufgezählt. Da der Schutz vor unbefugtem Informationsgewinn theoretisch am Größten ist, wenn ganz auf die Speicherung und Übertragung bestimmter Daten verzichtet wird, können die datenschutzrechtlichen Grundsätze der Datenvermeidung und Datensparsamkeit auch als dem Schutzziel der Vertraulichkeit dienend angesehen werden.[53] Die Vertraulichkeit steht damit in gegensätzlichem Verhältnis zur Verfügbarkeit der Daten.

c) Integrität

Das Schutzziel der Integrität wird als Schutz vor unbefugter Modifikation von Informationen definiert.[54] Sog. Datenintegrität wird gemäß dieser Definition gewährleistet, wenn „es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.“[55] Positiv formuliert kann Integrität mit „Vollständigkeit und Ganzheit, nicht beeinträchtigt, einwandfrei und anerkannte Grundsätze einhaltend“[56] umschrieben werden. Maßnahmen zur Gewährleistung der Integrität sind z.B. eine sachgemäße Rechteverwaltung und die Verwendung von mit Hilfe von kryptografisch sicheren Hashfunktionen gebildeten Message Authentification Codes.

d) Authentizität

Authentizität bezeichnet die Echtheit und Glaubwürdigkeit eines Objekts bzw. Subjekts.[57] Diese wird technisch anhand von charakteristischen Eigenschaften von Objekten oder Subjekten überprüft. Im Rahmen von Kommunikationsverbindungen kann die Identität der Kommunikationspartner zum Beispiel mit zertifizierten Signaturen nachgewiesen werden. Die Authentifizierung eines Benutzers an einem IT-System kann zum Beispiel mit wissensbasierten oder biometrischen Verfahren durchgeführt werden.

---

[53] vgl. Federrath/Pfitzmann im Roßnagel (Hrsg.) Handbuch Datenschutzrecht, S. 63 Rn. 9 f.
[54] Vgl. Federrath: Sicherheit im Netz, in: Moritz, Hans-Werner Moritz/ Dreier, Thomas (Hrsg): Rechts-Handbuch zum E-Commerce, S. 2.
[55] Eckert: IT-Sicherheit, S. 7.
[56] Wildhaber: Informationssicherheit, Rechtliche Grundlagen und Anforderungen an die Praxis, S. 19.
[57] Vgl. Eckert: IT-Sicherheit, S. 6 f.

e) Verbindlichkeit

Das Schutzziel der Verbindlichkeit gewann im Zuge der Zunahme des elektronischen Geschäftsverkehrs zunehmend an Bedeutung. Bezugsobjekt sind infolgedessen überwiegend Aktionen von Nutzern. Verbindlichkeit wird gewährleistet, „wenn es nicht möglich ist, dass ein Subjekt im Nachhinein die Durchführung einer […] Aktion abstreiten kann."[58] Dies ist der Fall, wenn bewiesen werden kann, dass ein Subjekt eine bestimmte Aktion getätigt hat. Das juristische Äquivalent dieses sicherheitstechnischen Schutzziels ist die Nachweisbarkeit[59] oder auch Beweisbarkeit. Technisch wird das Schutzziel der Verbindlichkeit meist mit Hilfe von (qualifizierten) Signaturverfahren realisiert.

II. Juristische Datenkategorien und netzseitige Infrastrukturen

Im folgenden Abschnitt werden die unterschiedlichen juristischen Datenkategorien beschrieben, die für die nachfolgende Betrachtung von Bedeutung sind.

1. Personenbezogene Daten

Der Begriff des personenbezogenen Datums ist das zentrale Bezugsobjekt des Datenschutzrechts. Nach der europäischen Legaldefinition in Art. 2 lit. a) DSRL[60] umfasst der Begriff der personenbezogenen Daten „alle Informationen über eine bestimmte oder bestimmbare natürliche Person". Bestimmbarkeit ist gegeben, wenn die entsprechende Person anhand von bestimmten Kennzeichen wie z.B. Name, Kundennummer, *IP*-Adresse zu einer bestimmten Zeit, Wohnort oder Telefonnummer singularisiert[61] werden und damit direkt oder indirekt identifiziert werden kann. Dieser weite Begriff der personenbezogenen Daten deckt damit alle Informationen ab, die mit einer Person in Verbindung gebracht werden können[62] und eröffnet einen weiten Anwendungsbereich für die Vorschriften der europäischen DSRL. Der deutsche Gesetzgeber greift die europarechtliche Definition in § 3 I BDSG auf, in dem personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" definiert werden. Auch dieser Begriff ist nach höchstrichterlicher Rechtsprechung – vor dem Hintergrund, dass es in unserer Zeit der zunehmenden Datenverarbeitung und Vernetzung lokaler Datenbestände kein belangloses Datum mehr gibt[63] – sehr weit zu fassen. Belanglos für die Einordnung als personenbezogenes Datum ist die Repräsentation der Information (Sprache, Schrift, Zeichen, Bild, Ton oder Bits).[64] Liegt ein personenbezogenes Datum vor, so besteht eine grundrechtstypische Gefährdungslage für das Recht auf Achtung des Privatlebens (Art. 8 I Alt. 1 EMRK), das Recht auf informationelle Selbstbestimmung (Art. 2 I i.V.m. Art. 1 I GG) oder das Fernmeldegeheimnis (Art. 10 I Var. 3 GG). Die Bestimmungen des Datenschutzrechts finden dann Anwendung. Auf Daten ohne Personenbezug (z.B. Daten, die anonymisiert wurden) ist das Datenschutzrecht nicht anwendbar.

---

[58] Vgl. Eckert: IT-Sicherheit, S. 10.
[59] So Wildhaber: Informationssicherheit, Rechtliche Grundlagen und Anforderungen an die Praxis, S. 21.
[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.
[61] Vgl. Artikel-29-Datenschutzgruppe: Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 16, im Internet abrufbar unter der URL http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf.
[62] Ehmann/Helfrich: EG Datenschutzrichtlinie, 1999, Art. 2 Nr. 17.
[63] So BVerfGE 65, 1 (45).
[64] Vgl. Kühling/Seidel/Sivridis: Datenschutzrecht, S. 79.

2. Inhaltsdaten

Der Begriff der Inhaltsdaten wird im Kontext elektronischer Kommunikation als „Inhalt der übermittelten Informationen“ definiert (vgl. Erwägungsgrund 13 der VDSRL). Hierunter fallen z.B. übermittelte Sprachdaten bei Telefongesprächen und der Text von SMS-Mitteilungen und E-Mails. Bei letzteren ist die Betreffzeile ebenfalls als Inhaltsdatum einzustufen. Verglichen mit altbewährten Kommunikationsformen sind Inhaltsdaten im elektronischen Bereich das, was sich im Postverkehr innerhalb des Briefumschlags oder Päckchens befände.

3. Verkehrsdaten

Um in einem elektronischen Kommunikationsnetz Nachrichten zwischen zwei Endstellen auszutauschen – sei es ein Telefongespräch zu vermitteln und Sprachdaten zu übertragen oder SMS-Mitteilungen, E-Mails oder den Inhalt von Webseiten über *HTTP*-Datenverkehr von einem Sender zu einem Empfänger zu leiten – müssen die Inhaltsdaten durch ein weltweit verzweigtes Telekommunikationsnetz transportiert und geleitet werden. An den verschiedenen Verzweigungsstellen des Netzes müssen Informationen verfügbar sein, die es diesen Stellen ermöglichen, die elektronischen Informationen in die richtige Richtung, also die Richtung des Empfängers weiterzuleiten. Die hierzu benötigten Daten werden als Verkehrsdaten bezeichnet. Sie stehen in „unmittelbarem Zusammenhang mit einem konkreten Telekommunikationsvorgang“[65]. Wie die sog. Verkehrsführung (engl. *Routing*) technisch ausgestaltet ist, hängt stark von der zugrunde liegenden Infrastruktur des Kommunikationsnetzes und der eingesetzten Technik ab. Meist werden Verkehrsdaten an die Inhaltsdaten geknüpft und mit diesen in das Kommunikationsnetz eingespeist. An den einzelnen Netzknoten werden die Verkehrsdaten anschließend ausgelesen, so dass die Inhaltsdaten in die richtige Richtung weitergeleitet werden können.

Nach der Definition in Art. 2 lit. b) EDSRL sind unter den Begriff der Verkehrsdaten neben den Daten, „die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz“ benötigt werden zudem die Daten zu fassen, die „zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden“. Ob Verkehrsdaten zu Rechnungszwecken verarbeitet werden müssen, ist abhängig von den verwendeten Geschäftsmodellen der TK-Diensteanbieter. Im Endkundenmarkt werden diese zunehmend von Flatrate-Modellen dominiert, die volumenunabhängig abgerechnet werden. Im Rahmen dieser Kommunikationsverbindungen ist keine Verarbeitung von Verkehrsdaten zur Bestimmung des monatlichen Rechnungsbetrags mehr erforderlich. Im Mobilfunk-Bereich sind derartige Flatrates aufgrund größerer Bandbreitenknappheit meist auf ein bestimmtes Volumen beschränkt. Den dort anfallenden Verbindungsdaten ist (sobald das definierte Volumen überschritten wurde) Fakturierungsrelevanz zuzusprechen. Die volumenabhängige Bepreisung von Telekommunikationsverbindungen dominiert zudem die Geschäftsmodelle von Telefonie-Dienste-Anbietern, wenn Verbindungen zu Teilnehmern anderer konkurrierender Netze aufgebaut werden.

Der deutsche Gesetzgeber verzichtet auf das Merkmal der Fakturierungsrelevanz und definiert Verkehrsdaten in § 3 Nr. 30 TKG als Daten, „die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden“.

Um zu bestimmen, welche Daten zum „Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz„ konkret benötigt und dementsprechend von den Betreibern auch erhoben,

[65] Gausling: Verdachtsunabhängige Speicherung von Verkehrsdaten auf Vorrat, S. 9.

verarbeitet oder genutzt werden, ist ein Blick auf die verwendeten Telekommunikationstechnologien und die zugrunde liegenden Netzinfrastrukturen erforderlich. Im Folgenden werden die für die Vorratsdatenspeicherung relevanten Bereiche der Festnetztelefonie, des Mobilfunks, des Internetzugangs, des E-Mail-Verkehrs und der Internet-Telefonie schematisch dargestellt und die anfallenden Verkehrsdaten identifiziert.

A) Verkehrsdaten im Bereich der Festnetztelefonie

Die Vermittlung von Kommunikationsverbindungen im Bereich öffentlicher leitungsgebundener Telefonnetze (*PSTN*) beruht auf der Technik der sog. Leitungsvermittlung. Durch das Wählen einer Rufnummer durch den Anrufer (*Quelle*) wird über mehrere Vermittlungsstellen hinweg eine Verbindung zum Angerufenen (*Senke*) aufgebaut. Diese Verbindung wird über einen bestimmten Zeitraum (z.B. den Zeitraum des Telefongesprächs) hinweg aufrecht erhalten und anschließend wieder abgebaut. Die folgende Abbildung zeigt ein mögliches Szenario, an dem sich die nachfolgende Darstellung orientiert.[66] Teilnehmer *Alice* wählt die Rufnummer des Teilnehmers *Bob*, wobei sich *Bob* im Zugangsnetz eines anderen Netzbetreibers, hier des *Netzbetreibers C* befindet.

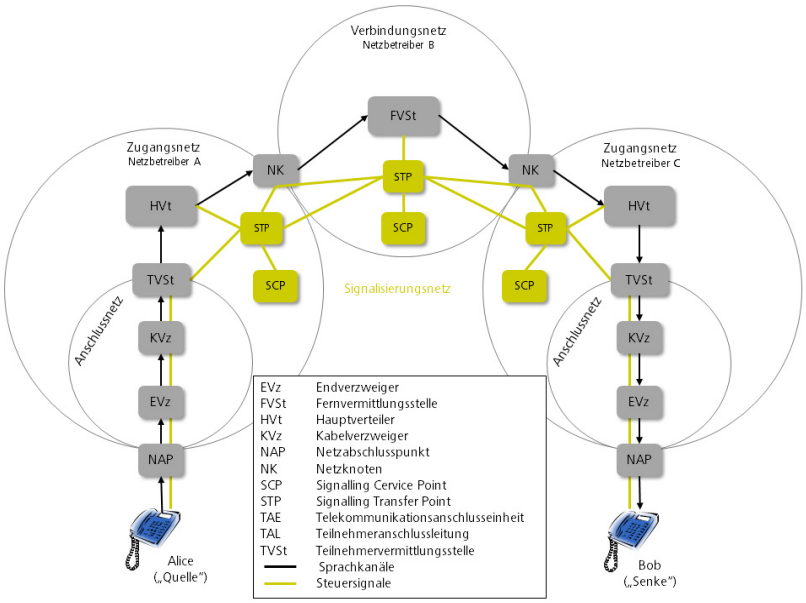


Abb. 3: Vermittlung einer Telefonverbindung über das leitungsgebundene Telefonfestnetz (schematisch)

Die Aufgabe der Festnetz- bzw. Telefondienstebetreiber ist es, den zu der Telefonnummer, die vom Endgerät von *Alice* übermittelt wird, gehörigen Anschluss von *Bob* zu identifizieren und die Verbindungsanfrage zu diesem oder zumindest – falls *Bob* sich im Netz eines anderen Betreibers befindet – jeweils bis zum Übergabepunkt (NK) zu weiteren Netzbetreibern zu leiten. Diese Aufgaben übernehmen verschiedene Vermittlungsstellen, die mit Hilfe von Routing-Tabellen, die seit der Digitalisierung des Festnetzes über ein separates Signalisierungsnetz[67] bereitgestellt werden, mit ausreichend Informa-

[66] Vgl. zum Aufbau eines Telefongesprächs den Wikipedia-Artikel „Telefongespräch", im Internet abrufbar unter der URL http://de.wikipedia.org/wiki/Telefongespr%C3%A4ch.
[67] Dieses ist für den Verbindungsaufbau, die Wegewahl durch das Netz, das Aufrechterhalten der Verbindung und den Verbindungsabbau zuständig, vgl. Konzepte der Internet-Technik, http://www.teialehrbuch.de/Kostenlose-Kurse/Internet-Technik/16074-Das-Telefonnetz.html.

tionen versorgt werden. Die Routing-Tabellen geben z.B. an, welche Aktionen die Vermittlungsstelle bei welcher Rufnummer bzw. welchen Rufnummernblöcken auszuführen hat.

Zu Beginn und Ende der Sprachverbindung wird von den Netzbetreibern ein sog. *Call Detail Record* (*CDR*) gespeichert. Dieser enthält alle rechnungsrelevanten Informationen wie Telefonnummer der Quelle und der Senke, die Uhrzeit des Verbindungsbeginns sowie die Dauer der Verbindung.[68] Diese als Verkehrsdaten einzustufenden Informationen werden in regelmäßigen Abständen aus den verschiedenen Vermittlungsstellen ausgelesen und anschließend zum Zwecke der Rechnungstellung von den Telefondiensteanbietern verarbeitet. Folgende Tabelle zeigt beispielhaft drei *CDR*s eines Kunden, die von einem Telefonanbieter gespeichert wurden:[69]

Kundennr.	Datum	Zeit	Tarif	Ziel	Gerufene Nr.	Dauer	Gebühr
A1727875117	20110310	1158	STD	Paris	2078063456	10.28	0.09
A1727875117	20110310	1415	STD	Paris	2078063456	7.88	0.07
A1727875117	20110310	1842	ECN	Regensburg	1923863456	0.85	0

Tab. 1: Exemplarischer DCR im Bereich der Festnetztelefonie

Die Angabe der Kundennummer erlaubt eine Verknüpfung dieser Daten mit den Kundendatenbanken der Telefondiensteanbieter, so dass jeder *CDR* exakt einem Kunden des Telefondiensteanbieters zugerechnet werden kann.

b) Verkehrsdaten im Bereich des Mobilfunks

Die Netzstruktur im Bereich der Mobilfunknetze ist im Kern vergleichbar mit der Struktur des Netzes im Festnetzbereich. Das Kernnetz des Mobilfunkbetreibers ist wie im Festnetzbereich drahtgebunden. Lediglich in Bezug auf die technische Ausgestaltung der sog. „letzten Meile“ unterscheiden sich die beiden Netze. Während im Bereich des Festnetzes der Anschluss zum Endkunden meist über ein Kupferkabel realisiert wird, erfolgt die Übertragung[70] von Daten zwischen Mobilfunkgerät des Kunden und Basisstationen des Netzbetreibers mittels Funkwellen, die nach bestimmten Standards (z.B. *GSM, UMTS* oder *LTE*) kodiert sind.[71] Die folgende Darstellung bezieht sich auf die Netzarchitektur eines *GSM*-Netzes und ist nahezu strukturanalog auf das *UMTS*- oder das *LTE*-Netz übertragbar.

[68] Vgl. Milford: The Data Retention Directive too fast, too fourious a response?, S. 10 f.
[69] In diesem Fall ist dieser schon verknüpft mit Abrechnungsdaten.
[70] Diese kann leitungs- oder paketvermittelt erfolgen. Für jede dieser Übertragungstechniken besteht ein separates Kernnetz.
[71] Vgl. hierzu die prägnante Darstellung der Netztechnologien im Mobilfunknetz im Konsultationsentwurf der Bundesnetzagentur zu Anrufzustellung in einzelnen Mobilfunknetzen, S. 5 ff. im Internet abrufbar unter der URL http://www.bundesnetzagentur.de/DE/DieBundesnetzagentur/Beschlusskammern/1BK-Geschaeftszeichen-Datenbank/BK1-GZ/2010/BK1-10-001/BK1-10-001_Marktdefinition.pdf?__blob=publicationFile.

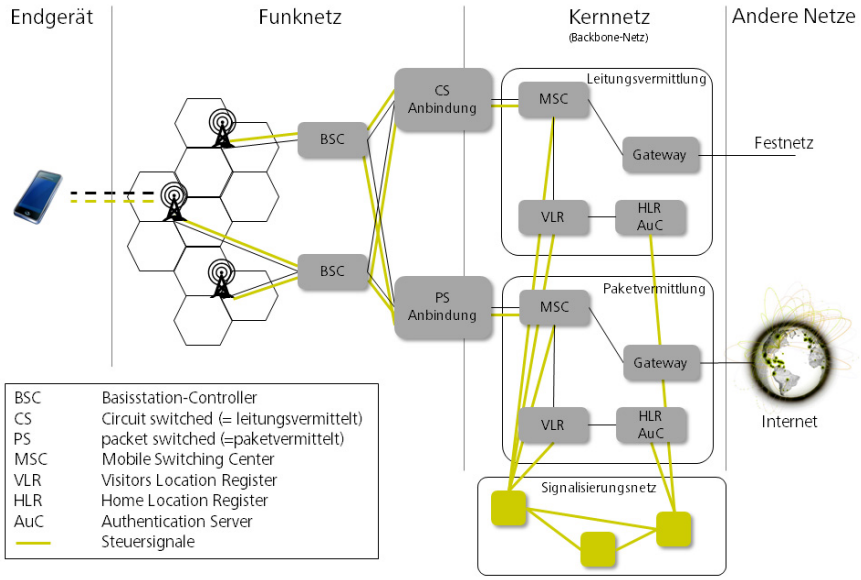


Abb. 4: Schematische Struktur des Mobilfunknetzes

Durch die Mobilität der Teilnehmer ergeben sich im Vergleich zum Festnetz zusätzliche Anforderungen an die Vermittlungsstellen (*Mobile Switching Center, MSC*). So muss zum Beispiel, um einen Anruf an ein Mobilfunktelefon zuzustellen, zunächst dessen Standort identifiziert werden, um den Anruf zur korrekten Basisstation zu leiten. Sofern sich ein Nutzer während eines Telefonats aus dem Empfangsbereich einer Basisstation entfernt und in den Empfangsbereich der nächsten Basisstation kommt, muss die Verbindung an diese übergeben werden. Das hierzu notwendige Mobilitätsmanagement wird mit Hilfe von zwei verteilten Datenbanken realisiert, die den einzelnen *MSC*s zugeordnet sind: Das *Home Location Register (HLR)* und das *Visitors Location Register (VLR)*.[72]

Das *HLR* enthält die zur Verbindungsherstellung notwendigen Daten aller Endnutzer, die mit dem Mobilfunknetz verbunden sind und führt die Authentifizierung der Teilnehmer durch. Das *VLR* enthält eine Abbildung aus dem *HLR*, beschränkt auf die Daten der Endnutzer, die sich im Zuständigkeitsbereich des jeweiligen *MSC* befinden. Sobald ein Teilnehmer mit einer Mobilfunkstation (z.B. einem Mobiltelefon) in den Einzugsbereich einer Basisstation kommt, baut das Mobilfunkgerät eine Verbindung zur Basisstation auf und versucht sich mit Hilfe des *Subscriber Identity Modules* (*SIM*) zu authentifizieren.[73] Hierzu werden auf Aufforderung der Basisstation verschiedene Informationen vom Endgerät übermittelt, darunter auch die *International Mobile Station Identity* (*IMSI*)[74], die zur eindeutigen Identifizierung des Teilnehmers herangezogen werden kann, und die *International Mobile Equipment ID* (*IMEI*), welche das Mobilfunkgerät des Teilnehmers eindeutig identifiziert.[75] Nach erfolgreicher Authentifizierung des Mobilfunkgeräts (eine Authentifizierung der Basisstation findet nicht statt) überträgt das Mobilfunkgerät bei Wechsel der Mobilfunkzelle Standortinformationen an die Basisstation, mit deren Hilfe die *HLR* und *VLR* auf aktuellem Stand gehalten werden können.

---

[72] Vgl. Walke, Bernhard: Mobilfunknetze und ihre Protokolle 1, S. 147.
[73] Zum Vorgang der Authentifizierung GSM-Netzen vgl. Freiling: Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, S. 10 f.
[74] Diese setzt sich zusammen aus einem Ländercode, einem Netzwerkcode, der Auskunft über den Netzanbieter des Teilnehmers liefert, und einer zehnstelligen Identifizierungsziffer.
[75] Vgl. Freiling: Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, S. 10 f.

Bei Nutzung von Telefonie-, SMS- oder MMS-Diensten werden wie im Festnetz *Call Detail Records* gespeichert, die zu Fakturierungszwecken ausgelesen werden.

c) Verkehrsdaten im Bereich des Internetzugangs

Hauptaufgabe sogenannter *Internet Service Provider* (*ISP*) ist die Übermittlung von Informationen in, im und aus dem Internet zu gewährleisten. Zur Verbindung mit einem *Internet Service Provider* bestehen verschiedene Möglichkeiten. Die meistgenutzten Zugangswege sind in der folgenden Abbildung schematisch dargestellt.

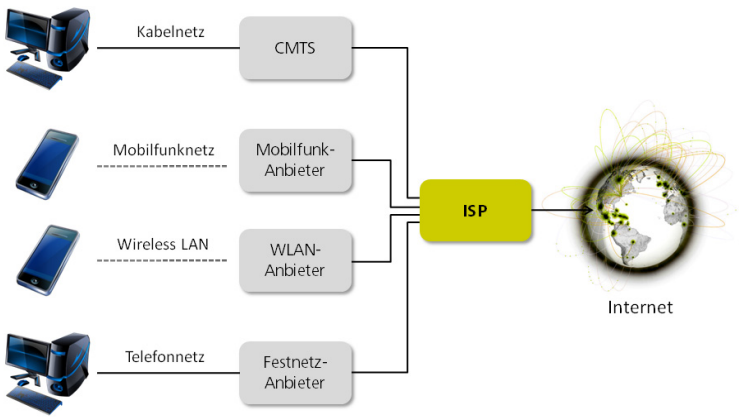


Abb. 5: Möglichkeiten des Zugangs zum Internet (schematisch)

Sofern über eine dieser Möglichkeiten eine Verbindung zwischen dem Endgerät des Nutzers und einem Zugangsserver des *ISP* (im folgenden Beispiel ein *RADIUS*-Server) hergestellt wurde, authentifiziert sich der Nutzer, soweit erforderlich, mit einer ihm zugewiesenen Benutzerkennung und dem dazugehörigen Passwort. Bei erfolgreicher Authentifizierung wird dem Nutzer eine *IP*-Adresse zugewiesen und dem entsprechenden Endgerät (Rechner oder Router) ein Zugang zum Internet gewährt. Der *RADIUS*-Server protokolliert daraufhin neben technischen Informationen zum Endgerät und zu der eröffneten Verbindung die Benutzerkennung des Internetnutzers, das Datum und die Uhrzeit der Einwahl sowie dessen zugewiesene *IP*-Adresse, die Version des verwendeten *IP*-Protokolls und eine Vielzahl weiterer Daten. Die folgende Abbildung zeigt beispielhaft einen *RADIUS*-Log bei erfolgreicher Einwahl:

```
1   Thu Apr 3 23:47:04 2008
2   User-Name = "154857895@adsl.newnet.co.uk"
3   Acct-Status-Type = Start
4   Acct-Session-Id = "FF10FFFF5876601D-47F55E68"
5   Service-Type = Framed-User
6   Framed-Protocol = PPP
7   NAS-Identifier = "Redback"
8   NAS-IP-Address = 212.87.xxx.xxx
9   NAS-Port = 1114112
10  NAS-Port-Type = Virtual
11  NAS-Port-Id = "L2TP LNS 7757853"
12  Medium-Type = DSL
13  Connect-Info = "8084000/8084000"
14  Platform-Type = 3
15  OS-Version = "2.6.7.0"
16  Acct-Authentic = RADIUS
17  Framed-Route = "80.175.xxx.xxx/28 80.175.xxx.xxx 1"
18  Framed-IP-Address = 80.175.xxx.xxx
19  Framed-IP-Netmask = 255.255.255.255
20  Source-Validation = 1
21  Client-DNS-Pri = 212.87.64.7
22  Client-DNS-Sec = 212.87.64.10
23  Tunnel-Type:0 = L2TP
24  Tunnel-Medium-Type:0 = IPv4
25  Tunnel-Server-Endpoint:0 = "212.87.xxx.xxx"
26  Tunnel-Client-Endpoint:0 = "212.87.xxx.xxx"
27  Tunnel-Server-Auth-Id:0 = "NEWNET"
28  Tunnel-Client-Auth-Id:0 = "NEWNET3"
29  Tunnel-Max-Sessions = 65535
30  Tunnel-Max-Tunnels = 5
31  Tunnel-Function = LNS-Only
32  Acct-Tunnel-Connection = "NEWNET3:22917:44995"
33  Event-Timestamp = "Apr 3 2008 23:47:04 BST"
34  Client-IP-Address = 212.87.xxx.xxx
35  Acct-Unique-Session-Id = "43e7e8aa0bd7fee2"
36  Timestamp = 1207262824
```

Abb. 6: Exemplarischer *RADIUS*-Log bei erfolgreichem Aufbau einer ADSL-Verbindung[76]

Die Kommunikation im „eigentlichen“ Internet (d.h. die Kommunikation mit Web- und Mailservern) basiert auf Kommunikationsprotokollen, die auf paketvermittelnden Techniken beruhen.[77] Informationen werden vom Sender in kleine Pakete zerlegt, die mit Hilfe einer Vielzahl von Protokollen mit unterschiedlichen Aufgaben über verschiedene Zwischenstationen zum Empfänger transportiert werden. Die verschiedenen Protokolle zur Regelung der Datenübertragung sind in einer hierarchischen Schich-

[76] Die IP-Adressen wurden anonymisiert.
[77] Vgl. hierzu und im Folgenden Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 17 ff.

tenstruktur realisiert. Vereinfachend kann man sich jede Schicht als einen Dienstleister vorstellen, der für eine bestimmte Aufgabe zuständig ist und der nächsthöheren Schicht seine Dienste anbietet.[78]

Je nach ihrem Aufgabenbereich sind die Protokolle einer der 7 Schichten des *OSI-Referenzmodells*[79] zugeordnet. Je niedriger die Schicht, desto größer ist der technische Bezug des Protokolls, je höher die Schicht, desto größer wird dessen Anwendungsbezug.

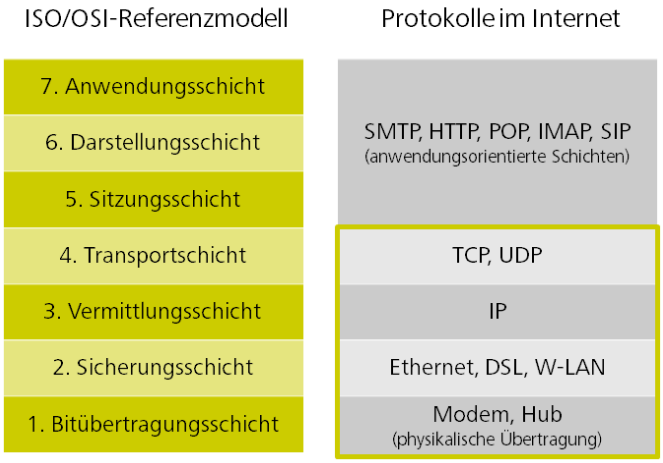


Abb. 7: OSI-Referenzmodell mit zugehörigen Protokolleschichten im Internetverkehr

Internetzugangsanbieter bieten Dienste auf den Ebenen 1-4 des *OSI-Referenzmodells* an. Die meist genutzte und damit wichtigste Protokollfamilie stellt der *TCP/IP-Protokollstapel* dar. Dieser arbeitet auf den Schichten 3 und 4 des *OSI-Referenzmodells* und baut auf den physikalischen Schichten – der Sicherungs- und Bitübertragungsschicht – auf.

Die physischen Schichten gewährleisten, dass elektronische Bits physikalisch, z.B. mit Hilfe einer Netzwerkkarte und entsprechenden Treibern, auf lokaler Ebene über ein bestimmtes Medium übertragen werden.[80] Hierzu werden die zu übertragenden Bits in Pakete aufgeteilt. Zur Adressierung wird den Paketen ein Protokollkopf vorangestellt, der die *MAC*-Adressen (*media access control*) des Senders und Empfängers enthält. *MAC*-Adressen (z.B. 00:14:6C:68:7A:8B) werden von den Herstellern von Netzwerkkarten nach einem bestimmten Codierungsschema[81] vergeben, so dass jede Netzwerkkarte eindeutig anhand ihrer *MAC*-Adresse identifizierbar ist.[82]

Da *MAC*-Adressen jedoch nur für die lokale Vernetzung konzipiert wurden und diese aus praktischen Gründen den Erfordernissen der Komplexität des weltweiten Datennetzes und dessen Adressierung nicht gerecht werden könnten[83], wurde für die Adressierung im Internet ein weiterer Mechanismus konzipiert: Das System der *IP*-Adressen. Jeder Rechner, der über seinen *ISP* erfolgreich mit dem Internet verbunden ist, ist über eine von seinem *ISP* zugewiesene *IP*-Adresse (z.B. 84.56.67.213) welt-

[78] Vgl. Freiling: Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, S. 4.
[79] Das Modell stammt von der Internationalen Organisation für Normung (ISO), definiert in ISO 7498-1, und dient als Designgrundlage für die technische Realisierung elektronsicher Kommunikation; vgl. ausführlich zu den einzelnen Schichten des Modells Tannenbaum: Computernetzwerke, S. 54 ff.
[80] Vgl. Freiling: Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, S. 3 ff.
[81] Die MAC-Adresse setzt sich zusammen aus einem Herstellercode und der Seriennummer der Netzwerkkarte.
[82] Vgl. Freiling: Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, S. 4.
[83] MAC-Adressen werden nur zur Adressierung bei der Übertragung zwischen den einzelnen Zwischenstationen (z.B. zwischen PC und Router) verwendet. Bei jeder Zwischenstation wird die MAC-Adresse des ursprünglichen Senders entfernt und die MAC-Adresse der entsprechenden Zwischenstation angehängt.

weit eindeutig identifizierbar. Die Zuweisung kann statisch erfolgen, d.h. einem bestimmten Rechner ist stets dieselbe *IP*-Adresse zugewiesen, oder dynamisch, so dass bei jeder Einwahl in das Internet eine erneute Zuweisung stattfindet (vgl. oben die Zuweisung der *IP*-Adresse nach erfolgreicher Authentifizierung an einem *RADIUS*-Server). Die Vergabe der *IP*-Adressen erfolgt nach einem bestimmten Schema. Jede *IP*-Adresse enthält zwei Teile: Der erste Teil gibt an, in welchem Teilnetz des Internets sich der entsprechende Rechner befindet. Der zweite Teil identifiziert den Rechner eindeutig. Dies ermöglicht eine schnelle Wegewahl, so dass Datenpakete über eine Vielzahl von Routern und Zwischenstationen im Internet schnell das richtige Ziel erreichen (*Routing*). Jedem *IP*-Paket ist ein *Protkollkopf* vorangestellt, der die *IP*-Adressen des gewünschten Senders und Empfängers des Datenpakets enthält. Die folgende Abbildung zeigt schematisch die Daten im *Kopf* eines *IP*-Paketes (*IPv6*[84]):

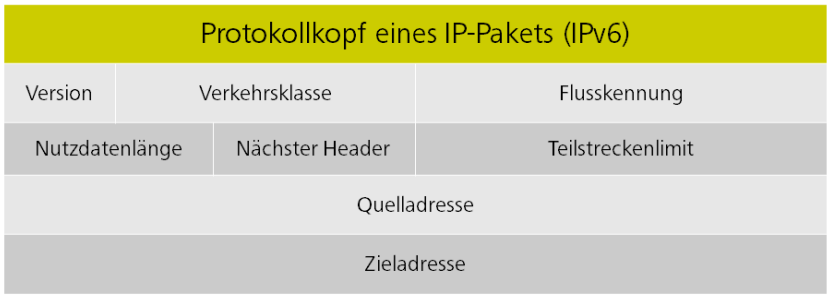


Abb. 8: Protokollkopf eines IP-Pakets (IPv6)

Um eine zuverlässige paketvermittelte Datenübertragung über das Internet zu gewährleisten, sind aufbauend auf den Routing- und Adressierungsfunktionen der Vermittlungsschicht zusätzliche Dienste erforderlich, die auf der Ebene der Transportschicht angeboten werden. So bestimmt das TCP-Protokoll die Standards für die Überprüfung, ob auch alle Datenpakete bei dem entsprechenden Empfänger angekommen sind. Zudem ermöglicht das *TCP*-Protokoll eine weitere Verfeinerung der Adressierung. Um spezielle Anwendungen auf einem Rechner anzusprechen, wäre die *IP*-Adressierung zu grob. Hierfür besteht die Möglichkeit, Ports zu definieren. Ein Port ist eine Nummer zwischen 0 und 65535. Auf einem mit dem Internet verbundenen Rechner sind den verschiedenen Ports Anwendungen zugewiesen, so dass die Inhalte der *IP*-Pakete mit Hilfe der Portnummer direkt an die entsprechende Anwendung auf dem Rechner übergeben werden können (z.B. an den Webbrowser oder an den E-Mail-Client).

Die Abgrenzung zwischen Verkehrs- und Inhaltsdaten in diesem Bereich gestaltet sich als nicht trivial. Angesichts der Aufteilung der Datenpakete im Internet in Kopf- und Inhaltsdaten böte sich diese Unterscheidung zur technischen Abgrenzung von Verkehrsdaten an. Die Interpretation von Verkehrsdaten als „Inhalte des Protokollkopfes von Datenpaketen“[85] ist jedoch im Rahmen der Schichtenstruktur des Internets nicht konsistent. Aufgrund der verschiedenen Schichten existieren mehrere Protokollköpfe. Protokollköpfe auf höheren Ebenen stellen stets Inhaltsdaten der darunterliegenden Ebenen dar (vgl. Abb. 9).[86] Um eine eindeutige Abgrenzung zwischen Verkehrs- und Inhaltsdaten zu ermöglichen,

[84] Version 6 des IP-Protokolls wird die derzeit hauptgenutzte Version 4 in den nächsten 10 Jahren ablösen.
[85] Freiling: Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, S. 14.
[86] So Freiling: Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, S. 14.

wäre die Festlegung einer bestimmten Schicht, auf der der Wechsel von Inhalts- zu Verkehrsdaten vollzogen würde, erforderlich. Die Daten der Protokollköpfe dieser und der darüberliegenden Schichten fielen dann unter den Begriff der Verkehrsdaten. Die genaue Betrachtung der Protokollköpfe der unterschiedlichen Ebenen zeigt jedoch, dass sich je nach herangezogener Schicht unterschiedliche Fehleinstufungen ergeben.

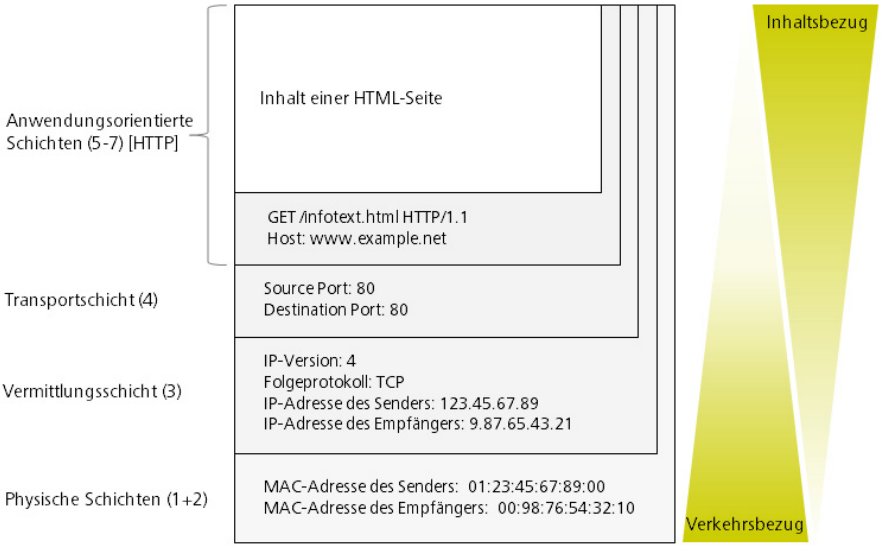


Abb. 9: Inhalte der Protokollköpfe auf den unterschiedlichen Schichten beim Versand einer E-Mail über das Internet

Differenziert man z.B. erst auf den anwendungsorientierten Schichten zwischen Verkehrs- und Inhaltsdaten, so dass alle in der Abbildung grau hinterlegten Protokollköpfe als Verkehrsdaten einzustufen wären, so würden die unzweifelhaft[87] als Inhaltsdaten einzustufenden *HTTP*-Protokollköpfe fälschlicher Weise als Verkehrsdaten eingestuft werden. Diese enthalten sog. *URI*s (*Uniform Resource Identifier*), die zur eindeutigen Identifizierung von Webseiten und Dateien im Internet verwendet werden und damit einen exakten Rückschluss auf die abgerufene Webseite oder Datei und damit dessen Inhalt ermöglichen.

Wählt man die darunterliegende Transportschicht als Übergangsschicht vom Inhalts- zum Verkehrsdatencharakter, so werden die Daten des *TCP*-Protokollkopfes, also die Ports der entsprechenden Anwendungen, noch mit unter den Begriff der Verkehrsdaten gefasst. Deren Informationsgehalt kann jedoch auch einen Rückschluss auf den Inhalt der Kommunikation eröffnen (z.B. wenn bestimmte Anwendungen für bestimmte Inhalte zuständig sind), auch wenn dieser schwächer als bei den URIs ausgeprägt ist.

Auch die Vermittlungsschicht eignet sich nicht als Abgrenzungsschicht zwischen Inhalts- und Verkehrsdaten. *IP*-Adressen weisen wie Portnummern eine gewisse Doppelnatur auf. Sie sind ebenso wie die physischen *MAC*-Adressen der Netzwerkkarten zwar zweifelsfrei als Verkehrsdaten einzustufen, können jedoch dadurch, dass sie im Rahmen des *HTTP*-Traffics Auskunft über besuchte Webseiten geben, auch als Inhaltsdaten eingestuft werden. Im Bereich des *SMTP*-Traffics (E-Mail-Verkehrs) fielen nach die Mailadressen des Absenders und des Empfängers (die im *SMTP*-Protokollkopf in den Anwendungsschichten des *OSI-Referenzmodells* zu verorten sind) auf Grundlage dieser Definition

[87] So auch Freiling, Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, S. 14.

fälschlicherweise nicht in den Bereich der Verkehrsdaten. Da die Protokollköpfe von *SMTP*- und *HTTP*-Traffic beiderseits auf der Anwendungsebene angesiedelt sind, jedoch unterschiedlich als Verkehrs- oder Inhaltsdaten einzustufen sind, ist eine randscharfe technische Definition des Begriffs der Verkehrsdaten über die Festlegung einer bestimmten Schicht nicht möglich.

D) Verkehrsdaten im Bereich des E-Mail-Verkehrs

Zur Übertragung von E-Mail-Nachrichten existieren unterschiedliche Protokolle (*SMTP, POP, IMAP, HTTP*). Diese haben gemeinsam, dass sie auf dem *TCP/IP-Protokollstapel* aufsetzen und im Rahmen des *OSI-Referenzmodells* auf den anwendungsorientierten Schichten zu verorten sind. Die Übertragung von E-Mails gestaltet sich dezentral. So kann eine E-Mail auf dem Weg zu ihrem Empfänger über mehrere Mailserver geleitet werden, bis sie am Zielserver ankommt. Die Übertragung von E-Mails zwischen den Mail-Servern erfolgt einheitlich mit Hilfe des *SMTP*-Protokolls, wohingegen sich der Zugang der Endnutzer zu ihren Mail-Servern heterogener gestaltet.[88] Dieser kann über die Kommunikationsvereinbarungen *SMTP, POP, IMAP* oder *HTTP* realisiert werden.

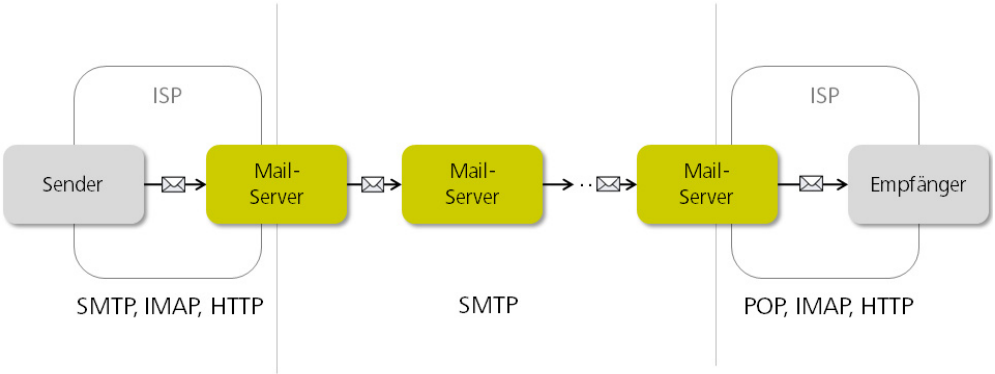


Abb. 10: Ablauf einer E-Mail-Kommunikation nach dem *store&forward*-Prinzip und der verwendeten Kommunikationsprotokolle

Das *Simple Mail Transfer Protocol* wird sowohl zur Kommunikation zwischen E-Mail-Clients (wie z.B. *Microsoft Outlook* und *Mozilla Thunderbird*) und Mailservern, als auch zur Kommunikation zwischen Mailservern benutzt und genießt dementsprechend die höchste Praxisrelevanz. E-Mails, die mit Hilfe des *SMTP*-Protokolls versendet werden, werden beim Absenden mit einem sog. *SMTP-Protokollkopf* versehen, der die notwendigen Verkehrsdaten zur Übermittlung der Nachricht beinhaltet.[89] Die eigentliche Nachricht wird im standardisierten *Internet Message Format* (IMF) formatiert und unterteilt sich in die Bereiche *Header* und *Body*.[90] Im *Header* der E-Mail sind Informationen über den Sender und den/die Empfänger (E-Mail-Adressen, Namen, etc.), eine eindeutige Message-ID, der

[88] Vgl. Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 80 ff.
[89] Alle Daten, die sich im SMTP-Umschlag, Header und Body der E-Mail befinden, können manuell mittels Terminal an Mail-Server übergeben und somit leicht manipuliert werden. Zur Kommunikation mit Mail-Servern mit Hilfe eines Terminals vgl. Damker/Federrath/Schneider: Maskerade-Angriffe im Internet, Eine Demonstration von Unsicherheit, S. 286 ff. sowie Stampfel/Gansterer/Ilger, Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 56 ff.
[90] Diese sind gleichzustellen mit dem im Rahmen von HTTP-Traffic übertragenen Inhalt von Webseiten oder Dateien, sind also im weißen Feld in Abb. 9 zu verorten.

Betreff der E-Mail und weitere Informationen wie z.B. die Daten der involvierten Mail-Server gespeichert.[91] Der Body der E-Mail enthält den eigentlichen Text der elektronischen Post.

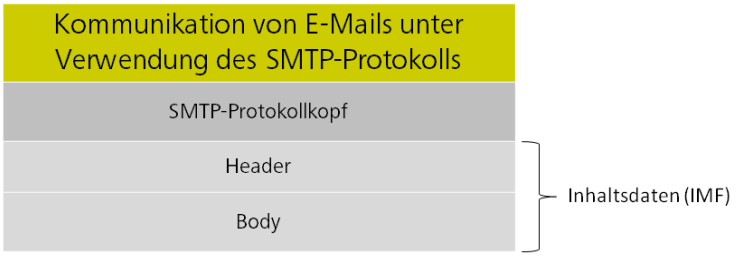


Abb. 11: Bestandteile der Übermittlung einer E-Mail unter Verwendung des SMTP-Protokolls

Die Zustellung der E-Mail bzw. deren Weiterleitung durch mehrere Mail-Server richtet sich nicht nach den Daten im *Header* der E-Mail (diese dienen nur der Information des Empfängers), sondern nach den Daten im sog. *SMTP-Protokollkopf*. Jeder Mail-Server, der an der Zustellung der E-Mail beteiligt ist, liest die Daten aus dem *SMTP-Protokollkopf* aus, entscheidet, ob und an welchen Mail-Server die E-Mail weitergesendet wird und fügt dem *Header* der E-Mail einen Datensatz mit Verkehrsdaten hinzu. Der Empfänger bekommt zuletzt nur die im *Header* enthaltenen Daten zu sehen, die Daten aus dem *SMTP-Protokollkopf* werden an diesen nicht übermittelt. Die folgende Abbildung zeigt exemplarisch einen mit Verkehrsdaten versehenen E-Mail-Header:

```
1  Subject: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
2  From: sender <sender.mail.address@btinternet.com>
3  Date: Fri, 11 Apr 2008 22:10:21 +0100
4  To: recipient <recipient@recipdomain.co.uk>
5  X-Account-Key: account2
6  X-UIDL: AHEMDNkAASHbR//Tjgnoo1CNVKY
7  X-Mozilla-Status: 0001
8  X-Mozilla-Status2: 00000000
9  X-Apparently-To: xxxxxxxx@btinternet.com via 217.12.12.113;
10 Fri, 11 Apr 2008 21:09:34 +0000
11 X-Originating-IP: [213.131.xxx.xxx]
12 Authentication-Results: mta816.mail.ukl.yahoo.com from=btinternet.com;
13 domainkeys=neutral (no sig)
14 Received: from 213.131.170.16 (EHLO sahasrar.ukisp.net) (213.131.170.16) by mta816.mail.ukl.yahoo.com
   with SMTP; Fri, 11 Apr 2008 21:09:34 +0000
15 Received: from relay2.post.newnet.co.uk (relay2.post.newnet.co.uk [212.87.80.26]) by sahasrar.ukisp.net
   (8.13.1/8.12.3) with SMTP id m3BL9VX6005557 for <recipient@recipdomain.co.uk>; Fri, 11 Apr 2008
   22:09:31 +0100 (BST) (envelope-from sender.mail.address@btinternet.com)
16 Received: (qmail 19271 invoked from network); 11 Apr 2008 21:09:31 -0000
17 Received: from <dns_reverse_lookup> (HELO ?80.175.xxx.xxx?) (80.175.xxx.xxx) by re-
   lay2.post.newnet.co.uk with SMTP; 11 Apr 2008 21:09:31 -0000
18 Message-ID: <47FFD3BD.3050700@btinternet.com>
19 User-Agent: Thunderbird 2.0.0.12 (Windows/20080213)
20 MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1; format=flowed Content-Transfer-
   Encoding: 7bit
```

Abb. 12: Exemplarischer mit Verkehrsdaten bestückter Header einer E-Mail-Nachricht (Betreff, aktuelle E-Mail und IP-Adressen wurden anonymisiert)

[91] Zu den Bestandteilen des E-Mail-Headers vgl. Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 74.

e) Verkehrsdaten im Bereich der Internet-Telefonie

Internet-Telefonie-Dienste (auch *VoIP*-Telefonie) setzen ebenso wie Maildienste auf dem *TCP/IP-Protokollstapel* auf und ermöglichen es mittels unterschiedlicher Protokolle[92] Sprachtelefonie über das paketvermittelte Internet abzuwickeln. Hierzu werden die Sprachinformationen auf dem Endgerät des Nutzers (z.B. einem PC) von der Software des *VoIP*-Dienstes digitalisiert und in Form von *IP*-Datenpaketen über das Internet versandt. Meist verfügt die entsprechende Software über Zusatzfunktionen, die z.B. Instant-Messaging-Dienste beinhalten. Die Identifikation von Nutzern erfolgt anhand von Nutzerkennungen, mit denen sich der Endnutzer bei dem entsprechenden *VoIP*-Dienst authentifiziert.

Ruft ein Nutzer einen Nutzer desselben *VoIP*-Dienstes an, so erfolgt die Telefonkommunikation ausschließlich paketvermittelt über das Internet. Zur Vermittlung der Gespräche zwischen zwei *VoIP*-Nutzern hält der *VoIP*-Dienst gewöhnlich einen Datenbankserver vor, auf dem die Nutzerkennungen, und die zugehörigen *IP*-Adressen angemeldeter Nutzer zur Verfügung stehen. Diese werden von den *VoIP*-Clients abgerufen. Die eigentliche Kommunikation zwischen den Nutzern erfolgt dann ohne Benutzung eines zentralen Servers. [93] Mittels *IP*-Adressen können sich *VoIP*-Clients nach dem *Peer-to-Peer*-Prinzip direkt mit anderen Clients im Internet verbinden. Der Server des *VoIP*-Dienstes ist hieran nicht mehr beteiligt. Zur Steuerung der Gespräche werden verschiedene Protokolle verwendet. Das folgende Beispiel zeigt den Header einer Gesprächsanfrage von *Alice* an *Bob* unter Verwendung des *SIP*-Protokolls.

```
1  INVITE sip:bob@ 192.0.2.4 SIP/2.0
2  Via: SIP/2.0/UDP server10.biloxi.com;branch=z9hG4bK4b43c2ff8.1
3  Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;branch=z9hG4bK77ef4c2312983.1;received=192.0.0.2
4  Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8;received=192.0.2.1
5  Max-Forwards: 68
6  To: Bob sip:bob@biloxi.com
7  From: Alice sip:alice@atlanta.com;tag=1928301774
8  Call-ID: a84b4c76e66710
9  CSeq: 314159 INVITE
10 Contact: sip:alice@pc33.atlanta.com
11 Content-Type: application/sdp
12 Content-Length: 142
```

Abb. 13: Exemplarischer Protokollkopf einer SIP-Gesprächsanfrage zur Telefonie über VoIP

Zudem ist es möglich, eine Sprachverbindung aus dem *VoIP*-Dienst mit einen Teilnehmer des leitungsvermittelnden Fest- oder des Mobilfunknetzes herzustellen, sofern der *VoIP*-Dienstanbieter Übergabeschnittstellen (sog. Gateways) zu diesen Infrastrukturen bereithält. Hierbei fallen bei dem Festnetz- oder Mobilfunkbetreiber die in den Abschnitten a) und b) beschriebenen Verkehrsdaten an.

[92] Vgl. die Übersicht der verwendeten Protokolle in Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 106 ff.
[93] Vgl. Bundesnetzagentur: Konsultationsentwurf zu Anrufzustellung in einzelnen Mobilfunknetzen, S. 11 f.

4. Bestandsdaten

Bestandsdaten sind „Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden“ (vgl. § 3 Nr. 3 TKG). Bestandsdaten beziehen sich demnach nicht wie Verkehrsdaten auf eine bestimmte Kommunikation, sondern auf einen bestimmten Nutzer, der in einem Vertragsverhältnis zum Telekommunikationsdiensteanbieter steht. Welche Daten konkret zu den Bestandsdaten zu zählen sind, richtet sich nach dem Inhalt des zugrunde liegenden Vertragsverhältnisses.[94] Beispiele für Bestandsdaten sind Name, Anschrift, Geburtsdatum, Rufnummer, E-Mail-Adresse, Passwörter sowie Bank- und Zahlungsdaten.

5. Standortdaten

Nach Art. 2 lit. c) EDSRL[95] fallen unter den Begriff Standortdaten alle „Daten, die in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben“. Standortdaten gewinnen vor allem im Bereich mobiler Geräte zunehmend an Bedeutung. Sog. *Location Based Services* liefern mit Hilfe des Standorts des Nutzers zusätzliche Dienste, wie z.B. Informationen über die Umgebung des Nutzers oder Auskunft über sich in der Nähe befindende Freunde oder Bekannte. Der Standort kann abhängig von der verwendeten Technik mit unterschiedlichen Verfahren bestimmt werden. Die verwendeten Verfahren weisen unterschiedliche Genauigkeitsgrade auf. So kann im Bereich mobiler Geräte zum Beispiel mit Hilfe des *Global Positioning Systems* oder mit Hilfe von Funkzellenmessungen eine sehr genaue Bestimmung des Standorts möglich sein. Beim leitungsgebundenen Internetzugang stellt die zugewiesene *IP*-Adresse auch ein Standortdatum dar. Dies ergibt sich aus der Codierung dieser Adresse, so dass die *IP*-Adresse durch Verknüpfung mit zusätzlichen Informationen (bestimmten Regionen sind bestimmte Adressräume zugewiesen) durchaus den groben Standort des Endgeräts verraten kann.

6. Vorratsdaten

Vorratsdaten sind alle Daten, zu deren Speicherung TK-Diensteanbieter gesetzlich verpflichtet sind. Welche Daten der soeben beschriebenen Datenkategorien in die Kategorie der Vorratsdaten fallen, ergibt sich aus Art. 5 VDSRL. Neben Verkehrs- und Standortdaten sind dies alle Daten, die zur Feststellung der Teilnehmer an einem elektronischen Kommunikationsdienst erforderlich sind (vgl. Art. 1 II VDSRL). Hierzu zählen auch Bestandsdaten wie Name, Anschrift und Telefonnummer, sofern diese notwendig sind, um den Kommunikationsteilnehmer eindeutig zu identifizieren. Eine detaillierte Darstellung aller Daten, zu dessen Speicherung und Zurverfügungstellung die Vorratsdatenspeicherungsrichtlinie verpflichtet, erfolgt in Kapitel D. I.

---

[94] Ebenso im Bereich der Telemedien, vergleiche Kühling/Seidel/Sivridis, Datenschutzrecht, S. 233.
[95] 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. EG 2002, L 201, 37; zuletzt geändert durch die Richtlinie 2009/136/EG, ABl. EU 2009, L 337, 11.

7. Zusammenfassung

Die soeben dargestellten Datenkategorien sind in ihrem Zusammenspiel nicht disjunkt, sie weisen verschiedene Überschneidungen auf. So können Verkehrsdaten wie z.B. die Telefonnummer auch Bestandsdaten sein. Sofern Verkehrsdaten Aufschluss über den Inhalt einer Kommunikation geben, fallen diese nicht mehr in die Kategorie der Vorratsdaten (vgl. Art. 5 II VDSRL). Es stellt sich jedoch die Frage, ab welcher Schwelle von einem so großen Inhaltsbezug auszugehen ist, dass ein Verkehrsdatum in ein Inhaltsdatum überschlägt. So enthalten zum Beispiel aussagekräftige Domain-Names (wenn z.B. eine E-Mail an kontakt@schuldnerhilfe.de gesendet wird) teilweise schon ausreichend Anhaltspunkte, um auf den Inhalt der gesendeten E-Mail schließen zu können. *IP*-Adressen können je nach betrachteter Domäne einen Inhaltsbezug aufweisen oder nicht. So fehlt es einer *IP*-Adresse, die einen *VoIP*-Nutzer identifiziert, z.B. an einem Inhaltsbezug. Sofern die IP-Adresse jedoch einen Webserver identifiziert, der mittels *HTTP*-Protokoll aufgerufen wurde und ausschließlich Informationen zu einer speziellen Thematik enthält, ist diese zudem als Inhaltsdatum einzustufen. Die *IP*-Adresse ist zudem ein gutes Beispiel dafür, dass Verkehrsdaten auch Standortdaten darstellen können. Die folgende Abbildung visualisiert die Systematik der soeben definierten Datenkategorien:

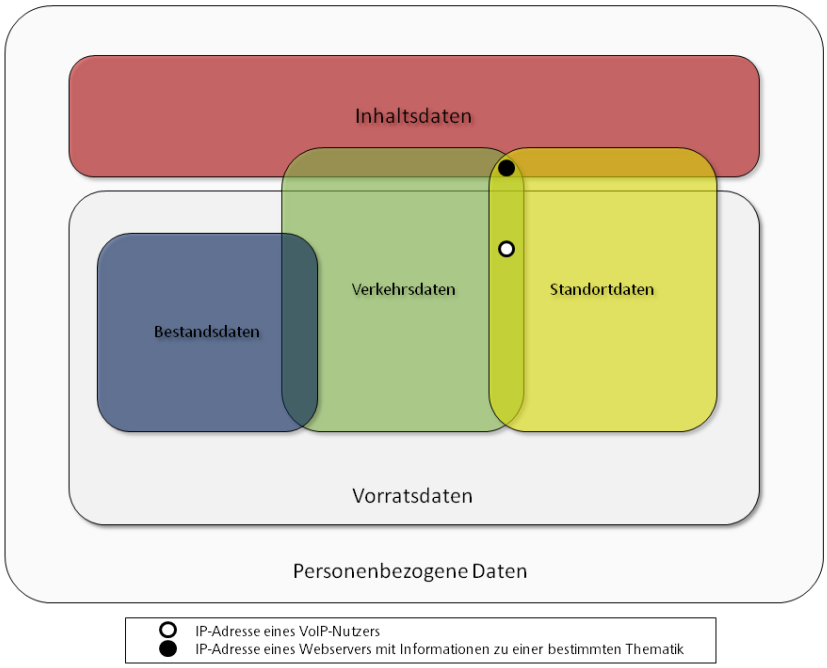


Abb. 14: Gesetzliche Datenkategorien und deren Überschneidungen mit Beispielen

C. Grundüberlegungen zum erforderlichen Schutzniveau

Die folgenden Überlegungen bilden den Ausgangspunkt und die Grundlage für die anschließende Beurteilung, ob und ggf. inwieweit die gesetzliche und praktische Ausgestaltung der technischen und organisatorischen Absicherung der Vorratsdaten dem tatsächlich erforderlichen Schutzniveau entspricht. Welches Schutzniveau aus Sicht der Datensicherheit zu gewährleisten ist und welche Schutzmaßnahmen somit konkret zu ergreifen sind, richtet sich hauptsächlich nach zwei Faktoren: Den Schutzinteressen der an der VDS beteiligten Entitäten und dem potentiellen Bedrohungsszenario. Dieses wird in Abschnitt II. exemplarisch anhand von verschiedenen Angriffsszenarien skizziert.

I. Schutzinteressen der beteiligten Akteure

Nach dem Prinzip der *Mehrseitigen Sicherheit* sind die Schutzinteressen aller an der Vorratsdatenspeicherung beteiligten Akteure zu berücksichtigen. Soweit diese miteinander konkurrieren, sind die resultierenden Schutzkonflikte auszutragen und in Analogie zur Grundrechtsdogmatik im Sinne einer praktischen Konkordanz[96] aufzulösen.[97] An der Vorratsdatenspeicherung beteiligte Akteure sind (1) die eigentlichen Kommunikationspartner, (2) die Telekommunikationsanbieter und (3) die zum Informationsabruf ermächtigten Ermittlungsbehörden. Die folgende Abbildung zeigt schematisch die beteiligten Entitäten (Organisationen und Personen) und deren Schutzinteressen.

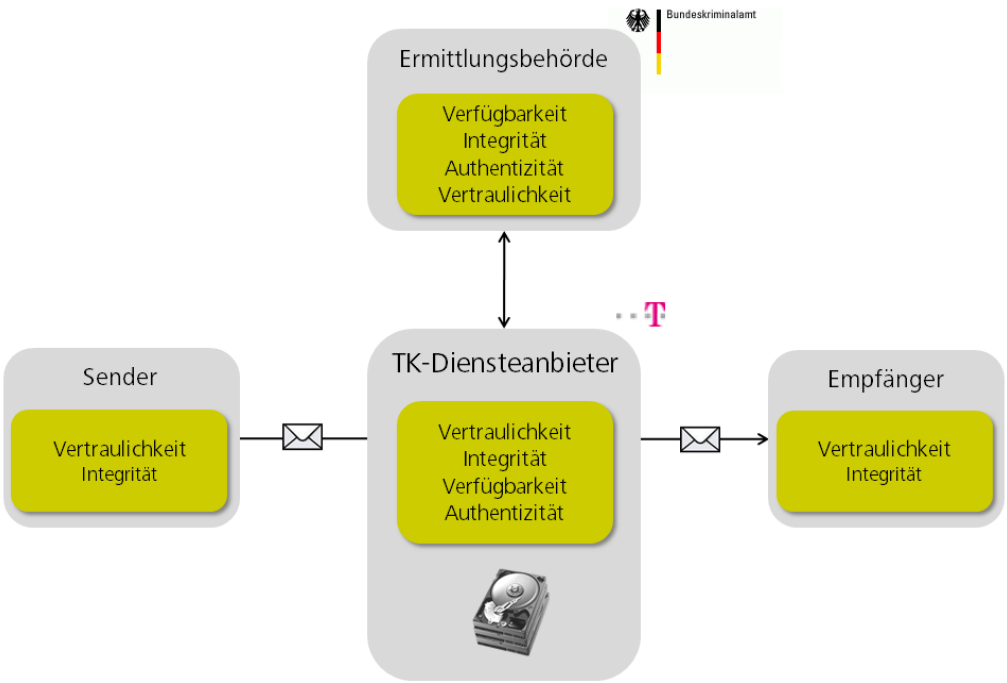


Abb. 15: Schutzinteressen der an der Vorratsdatenspeicherung beteiligten Akteure (exemplarisch am Beispiel Deutsche Telekom und Bundeskriminalamt)

[96] Das Prinzip der praktischen Konkordanz gebietet die Auflösung von Grundrechtskonflikten in einer Art und Weise, in der im Ergebnis die beiden konkurrierenden Grundrechtspositionen zu optimaler Wirksamkeit gelangen.
[97] Vgl. Rannenberg/Pfitzmann /Müller: IT Security and Multilateral Security in: Müller /Rannenberg (Hrsg.): Multilateral Security in Communications, S. 26.

1. Schutzinteressen der Telekommunikationsteilnehmer

Die Gruppe der Nutzer elektronischer Kommunikation (in Abb. 15 als Sender und Empfänger bezeichnet) geht nahezu vollständig in der gesamten Bevölkerung auf.[98] Jedes Individuum dieser Gruppe hat ein grundrechtlich geschütztes Interesse an der Vertraulichkeit seiner kommunizierten Inhalte und der diesbezüglichen Kommunikationsumstände.[99] Dementsprechend schützt z.B. in Deutschland das Telekommunikationsgeheimnis in Art. 10 I Var. 3 GG neben dem Kommunikationsinhalt auch die sog. Kommunikationsumstände vor einer Kenntnisnahme, Verarbeitung und deren Gebrauch durch die öffentliche Gewalt.[100]

Die im Rahmen der Vorratsdatenspeicherung zu speichernden Kommunikationsumstände ermöglichen einen Rückschluss auf Gewohnheiten und Vorlieben, Beziehungsgeflechte und Bewegungsprofile der kommunizierenden Person.[101] So gelang es zum Beispiel einer bekannten Online-Zeitung, anhand der Vorratsdaten des Grünenpolitikers Malte Spitz (durch Verknüpfung mit allgemein zugänglichen Daten) ein „klares Bild über Gewohnheiten und Vorlieben, ja über [sein] gesamte[s] Leben“[102] über einen Zeitraum von einem halben Jahr hinweg zu zeichnen. Durch Verknüpfung der auf Vorrat zu speichernden Daten wie z.B. Zeitpunkt, Dauer, Abfolge und Häufigkeit von Kommunikation könnte z.B. auf einen bestimmten Beziehungsstatus zwischen bestimmten Personen geschlossen werden. Das Vorhandensein von erfolglosen Anrufversuchen kann z.B. ein Indiz für Unstimmigkeiten zwischen diesen sein. Die Aggregation derartiger Daten ermöglicht die Aufdeckung des gesamten sozialen Umfelds. Bei Benutzung von Mobiltelefonen und der Internetnutzung werden die Verkehrsdaten zusätzlich mit Ortsdaten (*Cell-IDs* und *IP*-Adressen) angereichert. Internetfähige Handys hinterlassen z.B. bei Abruf von E-Mails im Push-Verfahren in regelmäßigen zeitlichen Abständen (teilweise im Sekundentakt) Datenspuren inklusive Ortsdaten, die mit in die Vorratsdaten bei den TK-Unternehmen einfließen. Durch Aggregation dieser Daten lassen sich nahezu vollständige Bewegungsprofile erstellen. Für die Auswertung derartiger Datenbestände existiert inzwischen eine größere Zahl an einfach zu bedienenden und zu beziehenden Softwarelösungen wie *i2 Analyst's Workstation 3*[103], *FMS-ASG Sentinel Visualizer*[104] oder *Maltego 3*[105].

Das Potential der Vorratsdaten zur Erstellung von Persönlichkeits-, Beziehungs- und Bewegungsprofilen[106] führt zu einer erhöhten Schutzbedürftigkeit im Hinblick auf die Vertraulichkeit der gespeicherten Daten. Die Existenz neuartiger Verknüpfungsmöglichkeiten, Analysemethoden und Profiling-Algorithmen verstärkt diese zusätzlich. Der Schutz der beim TK-Diensteanbieter gespeicherten Vorratsdaten vor unbefugtem Informationsgewinn stellt damit das zentral zu verfolgende Schutzziel dar.

---

[98] Ende 2009 verfügte z.B. jeder Bundesbürger in Deutschland im Durchschnitt über 1,3 Mobilfunkanschlüsse, vgl. Bundesnetzagentur: Jahresbericht 2010, S. 85, im Internet abrufbar unter der URL http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/Jahresbericht2010pdf.pdf?__blob=publicationFile.

[99] Vgl. BVerfG, Urteil vom 2.3.2006, Az: 2 BvR 2099/04.

[100] Vgl. BVerfGE 100, 313 (358 f.).

[101] Zu den Möglichkeiten der modernen Verkehrsdatenanalyse vgl. Kurz/Rieger: Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung, S. 5, im Internet abrufbar unter der URL http://www.ccc.de/de/vds/VDSfinal18.pdf sowie den Artikel „Das neue Profil des Menschen“ von Bernd Graff in der Süddeutschen Zeitung vom 5./6.6.2011, S. 14.

[102] Artikel „Was Vorratsdaten über uns verraten“ von Kai Biermann, in: ZEIT ONLINE, 24.2.2011, im Internet abrufbar unter der URL http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz.

[103] http://jb.warinteractive.com/products/analysts_workstation/default.asp.

[104] http://www.fmsasg.com/.

[105] http://www.paterva.com/web5/client/download.php.

[106] Zum Informationsgehalt der Verkehrsdaten vgl. auch Hensel: Die Vorratsdatenspeicherung aus datenschutzrechtlicher Sicht, DuD 9/2009, S. 527 ff.

Ebenso sind die Telekommunikationsteilnehmer an der inhaltlichen Korrektheit[107] und Integrität ihrer Verkehrsdaten interessiert. Die Gewährleistung dieser Schutzziele schützt vor einer falschen Verdächtigung aufgrund falscher Vorratsdaten und sichert die Möglichkeit unschuldiger Personen ab, sich mit Hilfe der Vorratsdaten zu exkulpieren.

2. Schutzinteressen der Ermittlungsbehörden

Die Schutzziele staatlicher Ermittlungsbehörden orientieren sich an dem durch die Nutzung der Vorratsdaten erzeugten Mehrwert für die Bewältigung präventiver und repressiver Ermittlungstätigkeiten. Um die gespeicherten Vorratsdaten möglichst fruchtend zu Ermittlungszwecken nutzen zu können, sind gleichermaßen fünf Schutzziele zu gewährleisten: die inhaltliche Korrektheit, Integrität und Verfügbarkeit der Vorratsdaten, die Zurechenbarkeit bzw. Authentizität bei der Übermittlung der Daten an die Ermittlungsbehörde und die Vertraulichkeit der Datenabfragen. Mit diesen steht bzw. fällt der eventuelle[108] Zusatznutzen für die Ermittlungstätigkeit.

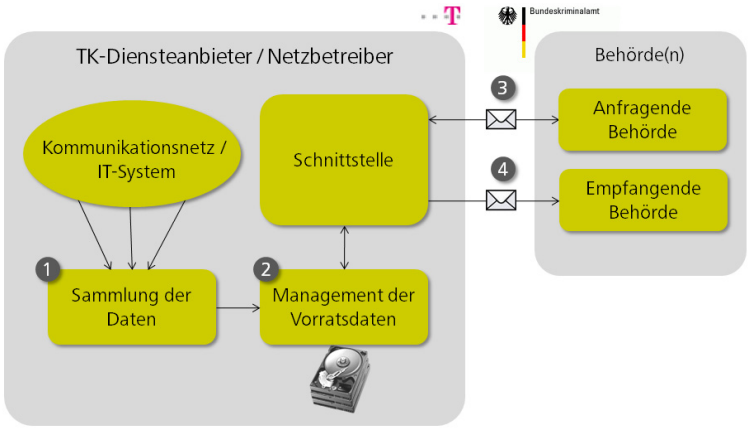


Abb. 16: Schematische Darstellung des Wegs der Vorratsdaten aus den Kommunikationsnetzen / IT-Systemen der TK-Diensteanbieter / Netzbetreiber zu den Ermittlungsbehörden[109]

Voraussetzung für die Sammlung und Aggregation der Vorratsdaten aus den Kommunikationsnetzen und IT-Systemen der Diensteanbieter und Netzbetreiber (1) ist, dass die entsprechenden Daten in den Systemen der Dienstanbieter und/oder Netzbetreiber überhaupt vorhanden sind. Aufgrund der großen Vielzahl an unterschiedlichen Telekommunikationsinfrastrukturen und deren Verbindungen untereinander sowie den unterschiedlichen Geschäftsmodellen, die sich seit der Liberalisierung der Telekommunikationsmärkte entwickelt haben, ist davon auszugehen, dass nicht jeder Netzbetreiber bzw. Diensteanbieter über alle erforderlichen Daten verfügt. So verfügt z.B. ein Reseller von Flatrate-DSL-Internetzugängen über keinerlei Verkehrsdaten seiner Nutzer, sondern lediglich über die Bestandsdaten seiner Kunden. Die Verkehrsdaten fallen bei den Netzbetreibern an, die jedoch mangels vertragli-

[107] Die inhaltliche Korrektheit ist zwar kein Schutzziel im Rahmen der in Kapitel B. I. 2. aufgezeigten Schutzzieldogmatik, wird aber der Vollständigkeit halber mit aufgeführt.
[108] Es gibt keine statistisch belegbaren Nachweise, wonach die Vorratsdatenspeicherung die Aufklärungsrate bisher erhöht hätte, vgl. zum Beispiel die Analyse der Aufklärungsquoten vom Arbeitskreis Vorratsdatenspeicherung, im Internet abrufbar unter der URL http://www.vorratsdatenspeicherung.de/images/schaubilder_wirksamkeit_vorratsdatenspeicherung_2011-01-26.pdf.
[109] Die anfragende und empfangene Behörde sind normalerweise gleich, können jedoch in bestimmten Fällen auch unterschiedliche Behörden sein (z.B. wenn die Anfragen durch Gerichte oder Staatsanwaltschaften und nicht durch die Ermittlungsbehörden an die TK-Diensteanbieter oder Netzbetreiber übermittelt werden.

cher Verbindung mit dem TK-Nutzer über keinerlei Bestandsdaten verfügen. Dementsprechend könnte es z.B. notwendig sein, zur Aufklärung der Identität des Senders Vorratsdaten bei mehreren Betreibern und Diensteanbietern abzufragen und diese dann miteinander zu verknüpfen.

Sofern die entsprechenden Daten im System des jeweiligen TK-Diensteanbieters verarbeitet werden, ist bei der Erhebung der Daten deren inhaltliche Korrektheit zu gewährleisten. Nur bei Übereinstimmung der Daten mit der Realität sind diese verlässlich und verwertbar. Falsche Daten führen zu falschen Verdächtigungen und können die Ermittlungstätigkeiten behindern. Im Hinblick auf Verkehrsdaten könnte man diese Forderung als überflüssig bezeichnen, weil deren inhaltliche Korrektheit als Grundlage des funktionierenden Kommunikationsnetzes ohnehin gewährleistet werden muss. Im Hinblick auf Bestandsdaten ist diese Forderung jedoch nicht obsolet.

In der Folgezeit müssen die abgespeicherten Daten über den gesamten Zeitraum der Speicherung hinweg vor unbefugter Modifikation geschützt und verfügbar gehalten werden (2), so dass die Daten bei Abruf durch die Ermittlungsbehörden in verwertbarer Form zur Verfügung stehen. Im Falle einer Anfrage (3) und Übermittlung (4) der Daten an eine öffentliche Stelle muss letztendlich sichergestellt werden, dass die übermittelten Daten auch tatsächlich von dem angeforderten Telekommunikationsunternehmen stammen und nicht von einem außenstehenden Angreifer z.B. über einen *Man-in-the-Middle*-Angriff[110] eingespielt oder verändert wurden.

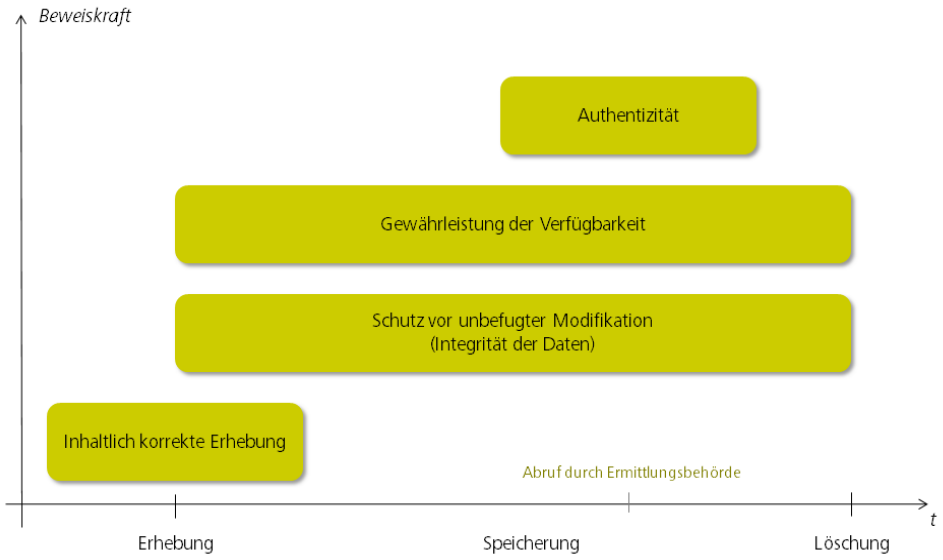


Abb. 17: Schutzinteressen der Ermittlungsbehörden (mit Ausnahme der Vertraulichkeit)

Die in Abb. 17 skizzierten Schutzziele (mit Ausnahme der Verfügbarkeit) sind tragende Säulen der Beweiskraft der abgerufenen Daten. Sofern diese nicht verlässlich gewährleistet sind, spricht der Grundsatz *in dubio pro reo* gegen eine Verwertung der Daten zu Lasten eines Beschuldigten in einem Strafprozess.

[110] Unter einem *Man-in-the-middle*-Angriff versteht man eine Angriffsform in Rechnernetzen, bei der sich der Angreifer unbemerkt zwischen zwei kommunizierende Entitäten setzt und diesen vortäuscht, der jeweilige Gegenüber zu sein, so dass der Angreifer die vollständige Kontrolle über den Datenverkehr zwischen den Kommunikationspartnern hat und diesen nach Belieben einsehen oder verändern kann.

Zudem ist im Interesse der Ermittlungstätigkeit sicherzustellen, dass die Anfragen der Ermittlungsbehörden vertraulich behandelt werden und nicht von unberechtigten Personen Kenntnis über diese erlangt wird.

3. Schutzinteressen der Telekommunikationsdiensteanbieter

Die Telekommunikationsdiensteanbieter verfolgen in nur geringem Ausmaß originäre Schutzinteressen. Aufgrund des vertrauenswürdigen Charakters ihres Endkundengeschäfts sind diese jedoch darauf bedacht, den Schutzinteressen ihrer Endkunden nachzukommen und deren Privatsphäre bzw. Fernmeldegeheimnis zu schützen. Hierzu finden sich gesetzliche Verpflichtungen, wie zum Beispiel § 88 im deutschen Telekommunikationsgesetz, der die Telekommunikationsunternehmen zur Einhaltung des Fernmeldegeheimnisses verpflichtet.

Den hauptsächlichen Treiber zur Gewährleistung der Schutzinteressen der TK-Nutzer und Ermittlungsbehörden durch die Telekommunikationsanbieter und dementsprechender Implementierung von Schutzmechanismen stellen rechtliche Verpflichtungen dar. Aufgrund ihrer Stellung als Verantwortliche über die Datensammlungen sind die TK-Diensteanbieter die Adressaten der rechtlichen Sicherheitsvorgaben. Inwieweit diese alle Schutzinteressen der Beteiligten abdecken, wird in den Kapiteln E. V. 2. und F. III. untersucht.

II. Bedrohungspotential

Neben den Schutzinteressen der Beteiligten ist die Stärke potentieller Angreifer ein mitentscheidendes Kriterium für die Auswahl konkreter Sicherheitsmaßnahmen. Das Angreifermodell beschreibt die „Stärke eines Angreifers, gegen den ein bestimmter Schutzmechanismus […] gerade noch sicher ist.“[111] Neben natürlichen Personen können auch Organisationen, ganze Staaten und Naturereignisse potentielle Angreifer darstellen. Obwohl mögliche Intentionen des Angreifers im Rahmen des Angreifermodells normalerweise keine Rolle spielen, soll im Rahmen dieses Abschnitts auch auf mögliche Motive eingegangen werden, um das vorherrschende Bedrohungsszenario möglichst nachvollziehbar zu skizzieren. Diese Motive können vielfältiger, z.B. persönlicher, wirtschaftlicher, gesellschaftspolitischer oder schlicht destruktiver Natur sein. Die potentiellen Angriffsszenarien lassen sich unterteilen in beabsichtigte und unbeabsichtigte, aktive und passive sowie Angriffe von innen und außen.[112] Im Folgenden werden die in Abb. 18 visualisierten Angriffsszenarien den in Abschnitt I. beschriebenen Schutzzielen zugeordnet und anhand von Beispielen konkret dargestellt.

[111] Federrath/Pfitzmann in Roßnagel(Hrsg.): Handbuch Datenschutzrecht, S. 64.
[112] Vgl. hierzu Federrath: Technische Aspekte des neuen Computergrundrechts, in: Uerpmann-Wittzack (Hrsg.): Das neue Computergrundrecht, S. 53 ff.

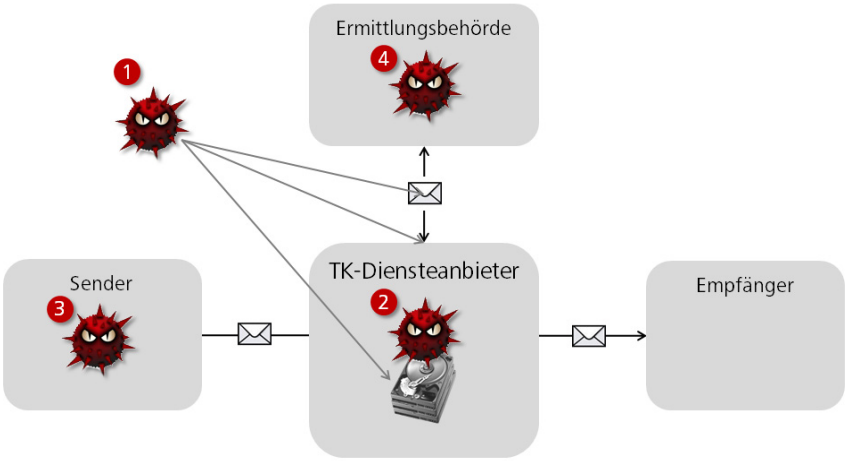


Abb. 18: Potentielle Angriffsszenarien

1. Angriffe auf die Schutzinteressen der TK-Nutzer

Motive zur unberechtigten Kenntnisnahme und damit Verletzung der Vertraulichkeit der Vorratsdaten könnten wirtschaftlicher, persönlicher und gesellschaftspolitischer Natur sein. Der Datenpool der Vorratsdaten enthält in seiner Gesamtheit eine Vielzahl an sensiblen Daten, die inhaltlich z.B. den zentralen Produktionsfaktor für Online-Portale darstellen und damit einen nicht zu vernachlässigenden Wert innehaben. Gerade weil die Daten auch in Bezug auf ein einzelnes Individuum sehr aussagekräftig sind, könnten auch persönliche Interessen zu Versuchen führen, die Vorratsdaten einer entsprechenden Person unberechtigterweise zur Kenntnis zu nehmen. Zudem kann nicht ausgeschlossen werden, dass gesellschaftspolitisch motivierte Hacking-Gruppen, wie zum Beispiel *Anonymous*, versuchen, durch Kenntnisnahme und Veröffentlichung der Daten eine mangelnde sicherheitstechnische Absicherung der Vorratsdaten aufzuzeigen.

Ein Angriff auf die Vertraulichkeit der gespeicherten Vorratsdaten ist grundsätzlich von innen und außen denkbar. So könnte zum Beispiel ein außenstehender Angreifer (Variante 1) versuchen, mit Hilfe von *IP-Sniffing*[113] über das Internet an die Ermittlungsbehörden übermittelte Vorratsdaten abzufangen und einzusehen. Dies würde z.B., falls die Vorratsdaten mittels unverschlüsselter E-Mails übertragen werden, abgesehen von der Ermittlung der *IP*-Adressen der kommunizierenden Server, keinen größeren Aufwand erfordern. Dementsprechend müssen die Vorratsdaten auf dem Übermittlungsweg durch ein dem aktuellen Stand der Technik entsprechendes Verschlüsselungsverfahren[114] abgesichert werden (z.B. durch die Verwendung von *SSL*-Protokollen). Ein außenstehender Angreifer könnte zudem versuchen, von außen durch Überwindung von technischen und physischen Sicherheitshürden (Firewalls, Authentifizierung, physischen Zutrittskontrollen) Zugriff auf die bei den TK-Diensteanbietern gespeicherten Daten zu erhalten. Dies erfordert die Entkoppelung der Datenbestände von öffentlichen Kommunikationsnetzen und die Installation robuster physischer und logischer Zutritts-, Zugangs- und Zugriffsschranken. Mit Hilfe kreativer Angriffsmethoden wie *Man-in-the-Middle*- oder *Maskerade*-Angriffen[115] könnten Angreifer zudem versuchen, sich gegenüber dem TK-

[113] Unter IP-Sniffing versteht man Techniken, mit denen Pakete in IP-basierten Netzwerken eingesehen werden können.
[114] Hierfür kommen vorrangig asymmetrische Verschlüsselungsverfahren in Betracht.
[115] Vgl. z.B. zum Vortäuschen eines falschen Absenders im E-Mail-Verkehr Damker, Federrath, Schneider: Maskerade-Angriffe im Internet, Eine Demonstration von Unsicherheit, DuD 20/5 (1996), S. 286 ff.

Diensteanbieter als berechtigte Ermittlungsbehörde auszugeben und Vorratsdaten abzufragen. Um dies zu verhindern, sind elektronische Anfragen von Ermittlungsbehörden mit einer qualifizierten – d.h. von einer vertrauenswürdigen Stelle zertifizierten – elektronischen Signatur zu versehen. So kann die Authentizität der Anfrage von den angefragten Unternehmen überprüft werden.

Aber auch das beim TK-Diensteanbieter und bei den Ermittlungsbehörden beschäftigte Personal (sog. Innentäter) könnte in Versuchung geraten, bestimmte Datensätze unbefugt zur Kenntnis zu nehmen (Variante 2 und 4). Bei vollständiger Automatisierung der Speicherung und Abfrage der Daten könnte dieses Bedrohungsszenario nahezu ausgeschlossen werden. Lediglich Systemadministratoren könnten dann noch eine potentielles Sicherheitslücke darstellen. Spätestens aber im Rahmen der Verwertung der Daten durch die Ermittlungsbehörden fallen die Vorratsdaten in Menschenhände. Eine automatisierte Beauskunftung ist zudem nicht vorgesehen.

Um die Vertraulichkeit der Vorratsdaten möglichst weitgehend technisch und organisatorisch abzusichern, ist der Zugang zu den Daten mit robusten physischen und logischen Sicherheitsmaßnahmen (vgl. oben) auf einen kleinen Kreis von speziell ermächtigten, geschulten und vertrauenswürdigen Personen zu beschränken. Dies erfordert die physische oder logische Trennung der Vorratsdaten von den restlichen Daten wie z.B. den Verkehrsdaten, die zu Rechnungszwecken verarbeitet werden sowie eine den verschiedenen Rollen der Mitarbeiter gerecht werdende Benutzer- und Rechteverwaltung. Zudem ist in Betracht zu ziehen, die zu speichernden Verkehrsdaten getrennt von den Bestandsdaten aufzubewahren und eine Verknüpfung der beiden Datenkategorien nur unter Beachtung des *Vier-Augen-Prinzips*[116] im Rahmen der Beantwortung spezieller Anfragen zu erlauben. Um einen Missbrauch der Daten im Nachhinein aufklären zu können, sind alle Zugriffe auf die Vorratsdaten revisionssicher zu protokollieren. Sobald die gesetzlich vorgeschriebene Speicherpflicht abgelaufen ist, müssen die gespeicherten Daten unwiderruflich gelöscht werden.

2. Angriffe auf die Schutzinteressen der Ermittlungsbehörden

Angriffe auf die Schutzinteressen der Ermittlungsbehörden kommen vor allem aufgrund persönlicher Motive in Betracht, die zu Versuchen führen könnten, Verkehrsdaten zu manipulieren, deren Verfügbarkeit zu beeinträchtigen oder Kenntnis von Abfragen zu erlangen. Die Verhinderung der Aufklärung eigener begangener Straftaten oder die Lenkung des Verdachts auf andere Personen durch Manipulation der Verkehrsdaten könnten mögliche Beweggründe sein.

Ein Angriff auf die Integrität der gespeicherten Vorratsdaten ist von innen und außen denkbar. Theoretisch denkbar ist zudem eine Manipulation der Verkehrsdaten auf dem Übertragungsweg zu den Ermittlungsbehörden mittels *Man-in-the-Middle-* oder *Maskerade*-Angriffen. Diesen ist durch die Verwendung qualifizierter Signaturverfahren zuvorzukommen. In Bezug auf das bei den Ermittlungsbehörden und TK-Diensteanbietern beschäftigte Personal gilt das unter Kapitel I. Gesagte. Zudem sollten die Verkehrsdaten bei deren automatisierter Sammlung aus den Telekommunikationssystemen mit einer unveränderbaren Signatur versehen werden, die die Echtheit der Daten bestätigen kann und damit Veränderungen der gespeicherten Daten aufzeigt. Abgesehen von Fehlerkorrekturverfahren ist eine Modifikation der gespeicherten Verkehrsdaten ohnehin aus keinem denkbaren Grund notwendig. Dementsprechend empfiehlt sich die Verwendung von *WORM*-Medien.

[116] Das Vier-Augen-Prinzip besagt, dass sicherheitskritische Vorgänge von mindestens zwei Personen durchgeführt werden müssen.

Angriffe auf die Verfügbarkeit der Vorratsdaten könnten mittels *Denial of Service*-Angriffen[117] auf die Übertragungsschnittstellen der TK-Diensteanbieter und Ermittlungsbehörden (soweit die Übertragung der Vorratsdaten über ein öffentliches Kommunikationsnetz erfolgt) erfolgen. Diesen dürfte nur geringe Relevanz zuzubilligen sein, weil sie die Übertragung der Daten bei Blockade der elektronischen Schnittstellen auf alternativen Wegen (z.B. Speichermedien, die per Post versendet werden) übermittelt werden können. Ebenso sind potentielle Naturkatastrophen und technische Defekte zu berücksichtigen, und die Vorratsdaten mit Backups ausreichend gegen diese abzusichern.

Von größerer Relevanz sind Techniken, die von vornherein das Anfallen von aussagekräftigen Vorratsdaten bei den TK-Diensteanbietern verhindern, die sich also primär gegen eine inhaltlich vollständige oder korrekte Erhebung von Vorratsdaten richten und im Ergebnis mittelbar auch das Schutzziel der Verfügbarkeit beeinträchtigen (Variante 3 in Abbildung 18). Welche Techniken hierzu geeignet sind, differiert je nach konkreter Ausgestaltung der VDS in den einzelnen Mitgliedstaaten und der zugrunde liegenden Kommunikationstechnik. Ein sehr einfacher Angriff im Bereich der Mobiltelefonie ist die Verwendung von Prepaid-Handys unter Angabe falscher Bestandsdaten.[118] Hierdurch wird verhindert, dass die in der Folge anfallenden Verkehrsdaten dem tatsächlichen Nutzer des Endgeräts zugeordnet werden können, weil in der Bestandsdatenbank des Mobilfunkanbieters falsche Daten hinterlegt sind. Die Angabe von falschen Bestandsdaten bei E-Mail-Anbietern ist ebenso ohne Hürden realisierbar.[119] Im Bereich des Internetzugangs bestehen unterschiedliche Möglichkeiten, um die eigenen Verkehrsdaten nicht in die Datenpools der TK-Diensteanbieter einfließen zu lassen. Anonymisierungsdienste wie z.B. *JonDonym*[120] oder *Tor*[121] ermöglichen es, innerhalb einer sog. Anonymitätsgruppe im Internet anonym zu bleiben.[122] Folgende Abbildung zeigt schematisch, wie sich Internetverbindungen, die über einen Anonymisierungsdienst abgewickelt werden, im Unterschied zur „normalen“ Internetverbindung des *Internetnutzers 1* gestalten.

[117] Denial of Service-Angriffe sind Angriffe auf Komponenten in Datennetzen. Es wird versucht, diese durch beabsichtigte Überlastung in ihrer Verfügbarkeit zu beeinträchtigen.
[118] Die Anmeldung einer Prepaid-SIM-Karte beim entsprechenden Anbieter erfolgt zumeist ohne Kontrolle der Identität des Nutzers. In diesen Fällen bestehen keine großen Hürden, um einen falschen oder fiktiven Namen sowie eine falsche und fiktive Adresse anzugeben.
[119] Eine Identifikation des E-Mail-Nutzers könnte hier zusätzlich mit Hilfe der IP-Adresse erfolgen, von der aus mit dem entsprechenden Mailserver kommuniziert wurde, sofern diese im Rahmen des E-Mail-Verkehrs von den E-Mail-Anbietern zu speichern ist. Hierzu wäre eine zusätzliche Auskunft bei dem Internetzugangsanbieter notwendig, der dem Nutzer die entsprechende IP-Adresse zugewiesen hat.
[120] http://www.jondos.org/.
[121] http://www.torproject.org/.
[122] Die Entwicklung dieser Techniken wurde teilweise mit öffentlichen Fördermitteln unterstützt. Es handelt sich um legitime Techniken, um einen gewissen Grad an Anonymität im Internet zu gewährleisten und sich damit z.B. vor unrechtmäßiger Datenerhebung durch Werberinge zu schützen. Die Tatsache, dass diese im Rahmen der vorliegenden Arbeit als potentielle Angriffe auf die Verfügbarkeit der Vorratsdatenspeicherung zu werten sind, verdeutlicht den durch die Einführung der Vorratsdatenspeicherung vollzogenen Paradigmenwechsel im Datenschutzrecht, der sich auch im Bereich der Datensicherheit widerspiegelt.

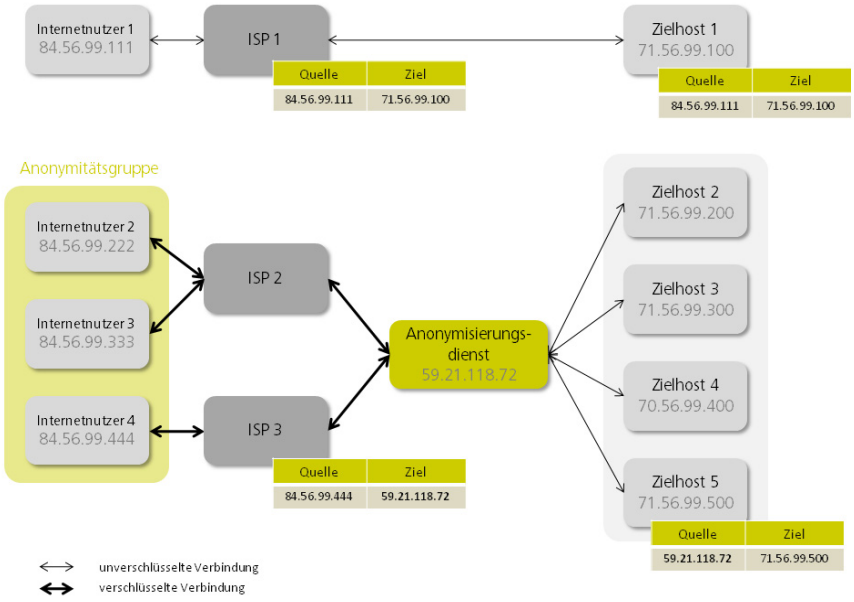


Abb. 19: Verschleierung von Verkehrsdaten durch die Nutzung von Anonymisierungsdiensten

Internetnutzer 1 ist mit seinem *ISP 1* verbunden und besucht ohne die Verwendung eines bestimmten Anonymisierungsdienstes eine bestimmte Website, den *Zielhost 1* mit der *IP*-Adresse 71.56.99.100. In diesem Fall können sowohl der *ISP 1* als auch der Zielhost die *IP*-Adressen des *Internetnutzers 1* und des *Zielhosts 1* „sehen" und entsprechend protokollieren. Die Nutzung eines Anonymisierungsdienstes führt bei ausreichender Größe der Anonymitätsgruppe[123] im Ergebnis zu einer Einschränkung des Sichtfeldes der *ISP* und der Zielhosts. *ISP 3* kann z.B. nur nachvollziehen, dass *Internetnutzer 4* mit der ihm zugewiesenen *IP*-Adresse 84.56.99.444 mit dem Anonymisierungsdienst unter der *IP*-Adresse 59.21.118.72 verbunden ist. Mit welchem Zielhost dieser kommuniziert, bleibt für *ISP 3* unsichtbar. Ebenso ist es für den Zielhost nicht möglich, die *IP*-Adresse des Internetnutzers zu bestimmen. Der Zielhost sieht lediglich die *IP*-Adresse des Anonymisierungsdienstes. Obwohl die Verwendung von Anonymisierungsdiensten nicht verhindern kann, dass der *ISP* weiß, welche *IP*-Adressen seinen Nutzern im Internet zugewiesen sind, führen die Verschleierung der Nutzer-*IP* gegenüber den Zielhosts sowie die Verschleierung des Zielhosts gegenüber dem *ISP* jedoch dazu, dass die beim *ISP 3* und *Zielhost 5* gespeicherten Verkehrsdaten nicht ausreichen, um die Kommunikation zwischen *Internetnutzer 4* und dem *Zielhost 5* im Nachhinein aufzudecken. Um die Verbindung dennoch aufzudecken, werden Daten der Anonymisierungsdienste benötigt, die die unterschiedlichen Anfragen an die Zielhosts den verschiedenen Nutzern des Anonymisierungsdienstes zuordnen.[124] Dementsprechend könnte der Umgehung der VDS mit Hilfe derartiger Anonymisierungsdienste durch eine Einbeziehung derselben in den Anwendungsbereich der Vorratsdatenspeicherung begegnet werden. Sofern die Server

[123] Befinden sich zu wenige Nutzer in der Anonymitätsgruppe, können deren Identitäten mit Hilfe von Schnittmengenangriffen aufgedeckt werden.

[124] Die „Deanonymisierung" bestimmter Nutzer von Anonymitätsdiensten ist technisch unter Wahrung der Anonymität der übrigen Nutzer des Anonymitätsdienstes möglich. Vgl. hierzu das die Privatsphäre der übrigen Nutzer schützende Modell in Köpsell/Wendolsky/Federrath: Revocable Anonymity in in: Müller (Hrsg.): Proc. Emerging Trends in Information and Communication Security: International Conference, ETRICS 2006, S. 206 ff.

dieser Dienste jedoch im außereuropäischen Ausland[125] beheimatet sind, scheidet dies aus. Nach demselben Prinzip ist die Umgehung der Vorratsdatenspeicherung durch Tunnelung des Datentransfers über einen angemieteten außereuropäischen *SSH*-Servers möglich, wie folgende Abbildung schematisch zeigt.[126]

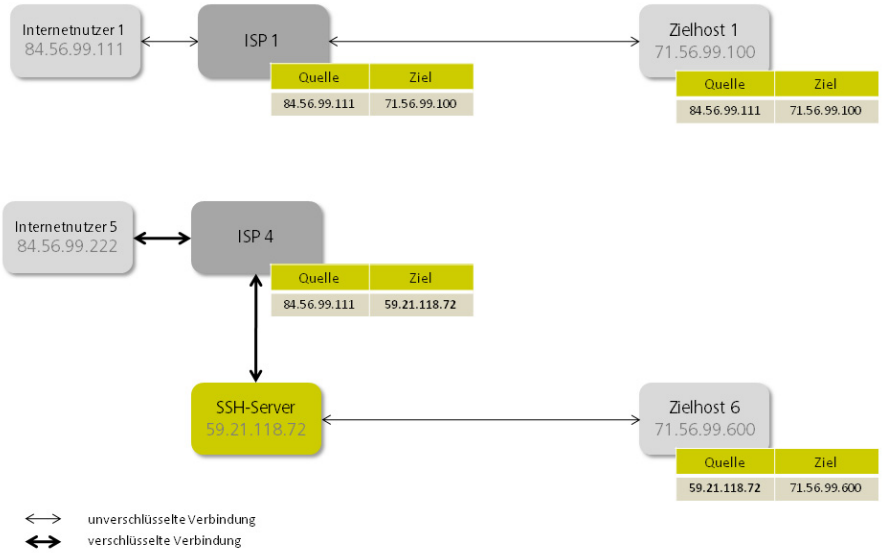


Abb. 20: Verschleierung von Verkehrsdaten durch die Nutzung eines SSH-Servers

Neben den soeben dargestellten Methoden existiert eine Vielzahl an weiteren Techniken, mit deren Hilfe die Vorratsdatenspeicherung umgangen werden kann.[127] Im Bereich des E-Mail-Verkehrs existieren ähnliche Techniken, um den anonymen Versand von E-Mail-Nachrichten mit Hilfe spezieller Mail-Server zu ermöglichen (z.B. *Cypherpunk-Remailer* oder *Mixmaster*). Des Weiteren könnten Mail-Server unter Angabe falscher Bestandsdaten oder unter Zwischenschaltung eines Anonymisierungsdienstes genutzt werden, bis hin zum Rückgriff auf außereuropäische Mailserver. Im Bereich der Telefonie könnten z.B. Einwahl-Telefon-Konferenzen genutzt werden. Bei Nutzung dieser fällt bei den Mobilfunkanbietern im Rahmen der Verkehrsdaten nur die 0180-Nummer des Telefonkonferenz-Dienstes an. Eine Aufdeckung der Kommunikationsteilnehmer ist in diesem Fall nur unter zusätzlicher Verwendung von Daten aus der Sphäre des Telefonkonferenz-Diensteanbieters möglich. Dementsprechend stellt sich auch hier die Frage der Einbeziehung solcher Telefonkonferenz-Diensteanbieter in den Anwendungsbereich der Vorratsdatenspeicherung.

Denkbar sind auch Kombinationen der soeben skizzierten Techniken. So könnte z.B. mit falschen Daten ein Benutzerkonto bei einem Mail-Server anlegt werden. Kontaktiert man diesen mit Zwischen-

[125] Vgl. hierzu auch den „Alvaro-Report“ vom 14.4.2005, EP-Dokument Prov. 2004/0813 (CNS), S. 7, im Internet abrufbar unter der URL http://www.statewatch.org/news/2005/may/ep-data-ret-alvaro-report.pdf.
[126] Videos zur erforderlichen Konfiguration eines derartigen Servers und des Client-PCs finden sich im Internet unter den URLs http://www.youtube.com/watch?v=1maZNx_ElKQ und http://www.youtube.com/watch?v=w6ww4sI06S4&feature=relmfu.
[127] Vgl. hierzu die Übersicht auf http://wiki.vorratsdatenspeicherung.de/VDS-umgehen#Internet-Zugang.

schaltung eines Anonymisierungsdienstes, so fallen bei dem Mail-Server selbst nahezu[128] keinerlei verwertbare Daten an.

Weitere Umgehungsmethoden sind die Nutzung von öffentlichen Münztelefonen und frei zugänglichen *WLAN*-Hotspots. Als Anknüpfungspunkt für die Identifizierung der Nutzer offener *WLAN*-Netze steht dabei einzig die *MAC*-Adresse der *WLAN*-Karte des Teilnehmers zur Verfügung.

Zusammengefasst kann in Bezug auf die Techniken zur Umgehung der Speicherung von Verkehrsdaten, die einen Angriff auf die Verfügbarkeit entsprechender Daten im weitesten Sinne darstellen, festgestellt werden, dass deren Erfolg hauptsächlich von zwei Faktoren abhängt: Dem Umfang und dem Adressatenkreis (auch Anonymisierungsdienste, Telefonkonferenz-Dienste etc.) der Speicherverpflichtung.

3. Mächtigkeit potentieller Angreifer

Die Mächtigkeit (auch: Stärke) potentieller Angreifer hängt maßgeblich von der verfügbaren Rechenleistung, den finanziellen Mitteln, der verfügbaren Zeit und der Verbreitung des Angreifers ab.[129] Diese Faktoren unterscheiden sich in Bezug auf die möglichen Angreifergruppen. Theoretisch in Betracht kommen Einzelpersonen, Personenvereinigungen, Unternehmen oder Staaten bzw. deren Regierungen oder Geheimdienste.[130] Inwieweit sich deren Mächtigkeiten unterscheiden, ist zur Abschätzung des erforderlichen Sicherheitsniveaus jedoch unbeachtlich. Entscheidend für dessen Höhe ist die maximal denkbare Mächtigkeit des Angreifers.

Die dem Angreifer verfügbare Rechenleistung sowie dessen finanzielle Mittel sind als nahezu unbeschränkt anzusehen. Vor allem staatliche Organe wie z.B. Geheimdienste verfügen über derzeit physikalisch maximal erreichbare Rechenleistungen, die diese vermutlich auch zu Spionagezwecken einsetzen.[131] Hinzu kommt eine zunehmende Organisierung und Kommerzialisierung[132] von Hackern. Betreiber sog. *Botnetze*[133] verkaufen temporär zum Beispiel die Kontrolle über tausende illegal kontrollierbarer Rechner im Internet oder deren Rechenleistung. Die enorm verfügbare Rechenleistung ergibt sich in diesem Fall aus der Kumulation der Rechenleistung aller *Bots*, so dass mit deren Hilfe z.B. effektive *Denial of Service*-Attacken ausgeführt werden können. Hacker organisieren sich zudem vermehrt in Gruppen, wie z.B. *Anonymous*, deren Mitglieder zusammen gezielte Attacken ausführen und so z.B. bereits Online-Portale wie *E-Bay* und Finanzinstitute wie *VISA* und *MasterCard* lahmlegen konnten.[134]

---

[128] Als Anknüpfungspunkt zu weiteren Ermittlung stehen nur die IP-Adresse des Anonymisierungsdienstes und die E-Mail-Adressen der Empfänger zur Verfügung.
[129] Vgl. Federrath/Pfitzmann in: Roßnagel (Hrsg.): Handbuch Datenschutzrecht, S. 65.
[130] Vgl. die Gruppeneinteilung potentieller Täter von Pierrot in Ernst (Hrsg.): Hacker, Cracker & Computerviren, S. 5.
[131] Vgl. Artikel „Bislang größte Serie von Hacker-Angriffen entdeckt“, in: FAZ.NET vom 3. August 2011, im Internet abrufbar unter der URL http://www.faz.net/artikel/C31158/72-regierungen-firmen-und-einrichtungen-betroffen-bislang-groesste-serie-von-hacker-angriffen-entdeckt-30478537.html.
[132] Vgl. Artikel „Geschäftsmodell Hacker“ in der Frankfurter Allgemeinen Sonntagszeitung vom 1. Mai 2011, S. 36.
[133] Ein Botnetz ist eine Gruppe von mit einer Schadsoftware infizierten Computern, die über das Internet vernetzt sind und von dem sog. Botnetz-Betreiber gesteuert werden können.
[134] Vgl. auch die Ankündigung von Anonymous, das Social Network Facebook am 5. November zu „zerstören“, Artikel „Anonymous nimmt Facebook ins Visier“, in: FAZ.NET vom 10. August 2011, im Internet abrufbar unter der URL http://www.faz.net/-02275h.

III. SCHUTZBEDARFSFESTSTELLUNG

Auf Grundlage der vorangegangenen Ausführung kann festgestellt werden, dass sich unter Berücksichtigung aller Schutzziele der beteiligten Entitäten und möglicher Angriffsszenarien ein immenser Bedarf zum Schutz der Vorratsdaten feststellen lässt. Um die Speicherung und Weiterleitung der Daten an Ermittlungsbehörden in rechtstaatlich konformen Bahnen ablaufen zu lassen, ist die Einhaltung aller dieser Schutzziele unabdingbar.

Eine Gewichtung der verschiedenen Schutzziele fällt schwer. Diese beinhaltet zwangsläufig eine Bewertung und Abwägung der kollidierenden Interessen der TK-Nutzer mit denen der Ermittlungsbehörden, die im Rahmen der vorliegenden Magisterarbeit nicht geleistet werden kann. Es kann jedoch festgestellt werden, dass aufgrund des Vorliegens dieser Vielzahl unterschiedlicher Schutzziele ein bunter Strauß an sicherheitstechnischen und organisatorischen Maßnahmen notwendig ist, um im Ergebnis alle Schutzinteressen ausreichend zu berücksichtigen und in angemessenem Maße zu gewährleisten. Diese Gewährleistung hat, betrifft sie doch Sicherheitsmaßnahmen zum Schutz der Verkehrsdaten der nahezu gesamten Bevölkerung, auf einem hohen Qualitätsniveau mit hoher technischer Aktualität zu erfolgen, um die datenschutzrechtlichen Vorschriften und das grundrechtlich geschützte Fernmeldegeheimnis nicht bis zur vollständigen Erschöpfung zu strapazieren.

Während eine Verletzung der Schutzziele der Verfügbarkeit, inhaltlichen Korrektheit, Integrität und Authentizität durch verschiedene Mechanismen (wie z.B. eine Nachprüfung der Daten anhand weiterer Ermittlungen) im Rahmen der Ermittlungstätigkeiten korrigiert werden kann, führt eine Verletzung der Vertraulichkeit der Daten zwangsläufig zu intensiven und ggf. streubreiten Eingriffen in die Privatsphäre. Dementsprechend wird im Rahmen der vorliegenden Arbeit ein höheres Gewicht auf das Schutzziel der Vertraulichkeit gelegt.

	Niedrig bis mittel	hoch	sehr hoch
Vertraulichkeit			X
Verfügbarkeit		X	
Inhaltliche Korrektheit		X	
Integrität		X	
Authentizität		X	

Tab. 2: Gewichtung der Schutzinteressen[135]

[135] Die Unterteilung der Schutzbedarfsklassen orientiert sich an der Einteilung im Grundschutzhandbuch des BSI, vgl. Ernestus in Roßnagel (Hrsg.): Handbuch Datenschutzrecht, S. 283 f.

D. Europarechtliche Vorgaben

In diesem Kapitel werden die einen sicherheitstechnischen Bezug aufweisenden europarechtlichen Vorgaben der Vorratsdatenspeicherung dargestellt. Hierzu sind auch die Vorgaben in Bezug auf die Kategorien der zu speichernden Daten und die Vorgaben in Bezug auf die Speicherdauer und die Zugriffsschwelle zu zählen. Diese enthalten relevante sicherheitstechnische Rahmenbedingungen wie z.B. die Größe des Kreises der rechtlich Zugriffsberechtigten und die Größe und Art der Datenbestände, die einen Rückschluss auf die Sensibilität und den notwendigen Speicherplatz zulassen.

Anschließend folgt die Darstellung der europarechtlichen Normierung der expliziten sicherheitstechnischen Anforderungen. Vorgaben zur Datensicherheit der auf Vorrat gespeicherten Daten finden sich in der europäischen Richtlinie zur Vorratsdatenspeicherung (VDSRL)[136], der Datenschutzrichtlinie für elektronische Kommunikation (EDSRL)[137] und der allgemeinen Datenschutzrichtlinie (DSRL)[138]. Diese weisen als Bestandteile der europäischen Sekundärrechtsebene einen hohen Abstraktionsgrad auf und bilden den äußeren Rahmen einer europarechtlich zulässigen Umsetzung der Vorratsdatenspeicherung auf nationaler Ebene.[139]

Die technische Konkretisierung der Vorgaben aus den Richtlinien erfolgt über technische Spezifikationen des *Europäischen Instituts für Telekommunikationsnormen* (*ETSI*). Diese Standards haben keine originäre Bindungswirkung, können jedoch z.B. durch Einbindung in nationale Gesetze oder Verwaltungsvorschriften in den Status der Rechtsverbindlichkeit gehoben werden.

I. Vorgaben in Bezug auf die Datenkategorien, Speicherfrist und Zweckbindung

1. Kategorien der zu speichernden Daten

Gemäß der Definition in Art. 1 II und 2 I lit. a) VDSRL sind die Anbieter öffentlich zugänglicher Telekommunikationsdienste verpflichtet, „Verkehrsdaten und Standortdaten sowie alle damit in Zusammenhang stehende[n] Daten, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind“ zu speichern.

Nach dem Richtlinienvorschlag der Europäischen Kommission sollten die Kategorien der zu speichernden Daten im Rahmen der Richtlinie nur grob beschrieben werden. Welche Daten genau unter

---

[136] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU 2006, L 105, 54.

[137] 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. EG 2002, L 201, 37; zuletzt geändert durch die Richtlinie 2009/136/EG, ABl. EU 2009, L 337, 11.

[138] 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. EG 1995, L 281, 31.

[139] Art. 15 I EDSRL, der den Mitgliedstaaten einräumt, auch darüber hinausgehende Regelungen zu treffen, gilt nicht für die in Art. 5 VDSRL aufgeführten Datentypen und Datenkategorien (vgl. Art. 15 Ia EDSRL). Damit sind die Regelungen in der VDSRL in Bezug auf die in der VDSRL genannten Daten als abschließend zu interpretieren.

diese Kategorien fallen (sog. Datentypen), sollte im Anhang der Richtlinie festgelegt werden.[140] Dies hätte eröffnet, die zu speichernden Datentypen nachträglich im Rahmen eines Komitologieverfahrens zu ändern und den Umfang der Vorratsdatenspeicherung auf diesem Wege ohne Mitwirkung des Europäischen Parlaments auszuweiten.[141] Um dies zu verhindern, wurde der Anhang in den Richtlinientext aufgenommen, so dass die Vorratsdatenspeicherungsrichtlinie in Art. 5 I der verabschiedeten Fassung eine ausdifferenzierte und abschließende[142] Aufzählung der auf Vorrat zu speichernden Datentypen enthält.

Zudem enthält Art. 5 II i.V.m. Art. 1 II 2 VDSRL das Verbot der Speicherung von Daten, die Aufschluss über den Inhalt einer Kommunikation geben. Eine trennscharfe Abgrenzung von Verkehrs- und Inhaltsdaten lässt sich jedoch praktisch nicht gewährleisten (vgl. Kapitel B. II. 3. c), so dass sich die Frage stellt, ab welchem inhaltlichen Gehalt Verkehrsdaten als Inhaltsdaten anzusehen und folglich nicht mehr von der Vorratsdatenspeicherung umfasst sind.

Je nach den informationellen Rückschlüssen, die aus den Daten gewonnen werden können, werden die Daten in Art. 5 I VDSRL in die Kategorien „Identifizierung der Quelle einer Nachricht“, „Identifizierung des Adressaten einer Nachricht“, „Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung“, „Bestimmung der Art einer Nachrichtenübermittlung“, „Bestimmung der Endeinrichtung von Benutzern“ und „Bestimmung des Standorts mobiler Geräte“ unterteilt. Welche Daten dies konkret sind, richtet sich nach der jeweils verwendeten Telekommunikationstechnologie. So unterteilt die Richtlinie die genannten Kategorien auf einer zweiten Ebene in die Bereiche Telefonfestnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie (*VoIP*) und benennt für jeden dieser Bereiche die zu speichernden Datentypen. Etwas unglücklich erscheint die Zusammenfassung der zu speichernden Datentypen in den Bereichen des Internetzugangs, des E-Mail-Verkehrs und der *VoIP*-Telefonie. Da die Telekommunikationsdienste dieser Bereiche auf unterschiedlichen Technologien beruhen, die auf unterschiedlichen Schichten des *OSI-Referenzmodells* anzuordnen sind (vgl. Kapitel B. II. 3. c), sind die Begrifflichkeiten der verschiedenen Bereiche oft nicht aufeinander übertragbar. Dies erschwert eine technisch eindeutige Benennung der zu speichernden Daten.

Im Folgenden wird versucht, mit Hilfe verschiedener Kommunikationsszenarien die nach Art. 5 I VDSRL zu speichernden Daten aus technischer Sicht möglichst eindeutig zu identifizieren und ein Datenbankschema[143] vorzuschlagen, dessen Struktur den Anforderungen der Vorratsdatenspeicherungsrichtlinie gerecht wird. Diese Datenbankschematas könnten unter Hinzuziehung weiterer Einflussgrößen[144] zur Abschätzung des erforderlichen Speicherbedarfs[145] für die Vorratsdaten genutzt werden, dessen Bereithaltung durch das Schutzziel der Verfügbarkeit gefordert wird.

---

[140] Vgl. Kommission: Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rats über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, KOM(2005) 438.

[141] Kritisch hierzu der Europäischen Wirtschafts- und Sozialausschusses in seiner Stellungnahme zum Vorschlag der Europäischen Kommission zur Vorratsdatenspeicherungsrichtlinie vom 19. Januar 2006, Abschnitt 2.4.6, im Internet abrufbar unter der URL http://eescopinions.eesc.europa.eu/eescopiniondocument.aspx?language=EN&docnr=0035&year=2006

[142] Vgl. Szuba: Vorratsdatenspeicherung, S. 52.

[143] Die Datentypen und der erforderliche Speicherplatz beziehen sich auf SQL-Datenbanken.

[144] Durchschnittliches Kommunikationsverhalten der Dienstenutzer, Anzahl der Dienstenutzer und zusätzliche Einflussgrößen wie z.B. SPAM.

[145] Eine Schätzung des erforderlichen Speicherbedarfs findet sich z.B. in Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 124 ff.

a) Vorratsdaten im Bereich des Festnetzes

Im Bereich des Festnetzes ist der Umfang zu speichernder Daten im Vergleich zu den anderen Bereichen am Geringsten. Nach ausdrücklichem Wortlaut in Art. 5 I lit. a) Nr. 1, lit. b) Nr. 1, lit. c) Nr. 1, lit. d) Nr. 1 und lit. e) Nr. 1 VDSRL sind die Rufnummern der Teilnehmer eines Telefonats (bzw. Telefaxes) sowie deren Namen und Anschriften, der Beginn und das Ende der Kommunikation sowie der in Anspruch genommene Telefondienst zu speichern. Zwar nicht ausdrücklich im Wortlaut verankert, aber in dessen Systematik angelegt, erscheint zudem die Speicherung der „Richtung" der Verbindung verpflichtend zu sein, um feststellen zu können, welcher der Teilnehmer die *Quelle* und welcher der Teilnehmer die *Senke* der Verbindung darstellt. Bereits diese explizit zu speichernden Daten können Aufschluss über den möglichen Inhalt der Kommunikation geben, sofern z.B. ein Teilnehmer der Kommunikation typischerweise mit der Erbringung bestimmter Dienstleistungen betraut ist (z.B. Psychologen, Anwälte, etc.), und damit mit dem Verbot der Speicherung von Inhaltsdaten in Art. 5 II VDSRL kollidieren.[146]

Name	Typ	Bytes	Beispiel
ID	INT	4	5897
Rufnummer des rufenden Teilnehmers	INT	4	49941123456
Rufnummer des gerufenen Teilnehmers	INT	4	49941654321
Beginn	DATETIME	8	13.1.2011 - 13:56:45
Ende	DATETIME	8	13.1.2011 - 14:36:12
Dienst[147]	TINYINT	1	1

Tab.3: Exemplarisches Schema eines Datensatzes, der entsprechend Art. 5 VDSRL im Festnetzbereich zu speichern ist

Die ID ist eine automatisch vergebene Zahl, über die jeder Eintrag in der Datenbank eindeutig identifizierbar ist. Die übrigen Daten des Datenbankeintrags können aus den sog. *CDR*s aggregiert werden, über die jeder Festnetzbetreiber zum Zwecke der Rechnungstellung verfügt (vgl. oben Kapitel B. II. 3. a).

Über die Rufnummern können die jeweiligen Telekommunikationsdiensteanbieter die Verkehrsdatensätze eindeutig mit den Bestandsdaten (Name und Anschrift) ihrer Kunden verknüpfen.[148] Die jeweiligen Bestandsdaten sind jedoch nur bei den entsprechenden Vertragspartnern der jeweiligen Telekommunikationspartner vorhanden. Falls ein Anbieter z.B. über keine Bestandsdaten eines Gesprächsteilnehmers verfügt, weil dieser z.B. Vertragspartei im Netz eines anderen Netzbetreibers ist, so trifft diesen keine Erhebungspflicht in Bezug auf diese Daten. Wie in Art. 3 I und Erwägungsgrund 23 der VDSRL klargestellt wird, sind in derartigen Fällen nur solche Daten zu speichern, die „im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt

[146] Für diese Fälle könnten eine VDS-Blacklist an die die Telekommunikationsdiensteanbieter und Netzbetreiber verteilt werden, die Listen der Telefonnummern der Berufsgeheimnisträger enthält, deren Verkehrsdaten nicht mit erfasst werden sollen.
[147] 1 = Telefoniedienste, 2 = Telefaxdienste, 3 = Verbindung zu einem ISP.
[148] Es wird davon ausgegangen, dass jeder Telekommunikationsdiensteanbieter über eine Kundendatenbank verfügt, in der die Bestandsdaten seiner Kunden enthalten sind.

oder verarbeitet werden“. Im Beispielszenario in Abbildung 21 könnten die Telekommunikationsdiensteanbieter (*Netzbetreiber A, B* und *C*)[149] folgende Datensätze speichern:

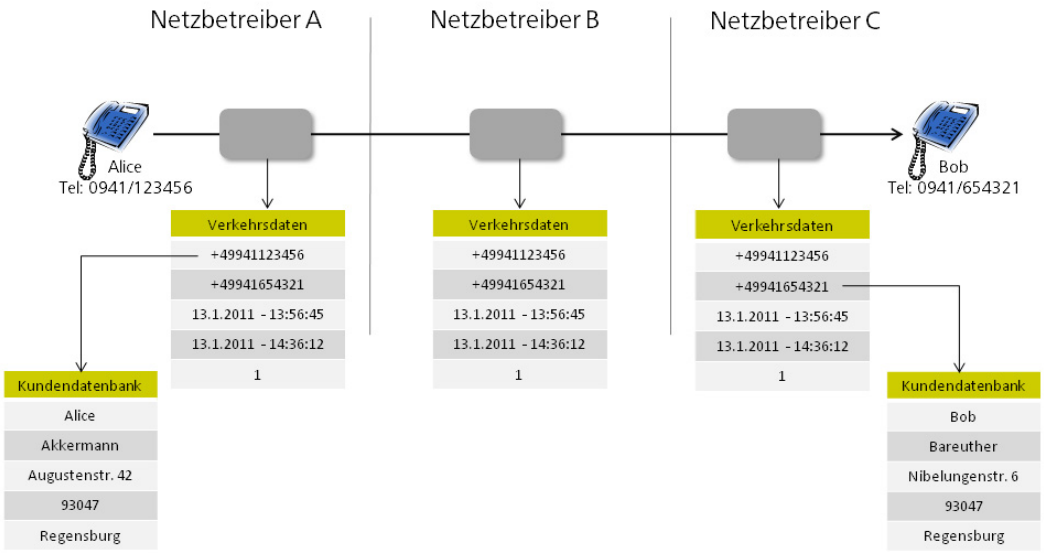


Abb. 21: Nach Art. 5 I VDSRL zu speichernde Verkehrsdaten im Falle des Telefonanrufs von Alice an Bob im Festnetz[150]

Eine Verknüpfung mit Bestandsdaten ist nur *Netzbetreiber A* und *Netzbetreiber C* möglich, der Verbindungsnetzbetreiber *B* hat nur vertragliche Vereinbarungen mit *Netzbetreiber A* und *C*. Dementsprechend ist fraglich, ob der *Verbindungsnetzbetreiber B* neben *Netzbetreiber A* und *C* auch verpflichtet ist, einen Datensatz zu speichern. Angesichts dessen, dass zur Aufdeckung der Identität von *Alice* und *Bob* ohnehin Anfragen bei den *Netzbetreibern A* und *C* erforderlich sind, ist die redundante Speicherung der Verkehrsdaten bei *Netzbetreiber B* überflüssig.

B) Vorratsdaten im Bereich des Mobilfunks

Im Bereich des Mobilfunks sind gem. Art. 5 I lit. e) Nr. 2 und lit. f) VDSRL zusätzlich zu den Daten, die auch im Festnetzbereich zu speichern sind, die *IMSI* und *IMEI* der Teilnehmer sowie die *Cell-IDs* bei Beginn der Verbindung zu speichern. Ob hierunter auch die *Cell-ID* des gerufenen Teilnehmers fällt, lässt Art. 5 I lit. f) Nr. 1 VDSRL nicht zweifelsfrei entnehmen. Der Singular „die Standortkennung“ könnte einerseits darauf hindeuten, dass nur die *Cell-ID* des rufenden Teilnehmers zu speichern ist. Art. 5 I lit. f) VDSRL bezieht sich jedoch generell auf die „Bestimmung des Standorts mobiler Geräte“ und unterscheidet nicht zwischen *Quelle* und *Senke* der Verbindung wie z.B. lit. a) und lit. b). Dementsprechend bezieht sich die Pflicht zur Speicherung der *Cell-ID* auf alle Telekommunikationsteilnehmer mit mobilen Telekommunikationsgeräten. Die hierfür notwendigen Daten können aus den *CDRs* und dem *HLR* der Mobilfunkbetreiber ausgelesen werden (vgl. Kapitel B. II. 3. b). Für die Be-

[149] Zur Vereinfachung wird davon ausgegangen, dass die Telefoniediensteanbieter von Alice und Bob zugleich Netzbetreiber der entsprechenden Zugangsnetze sind. Wäre dies nicht der Fall (sog. Reselling), würde sich zudem die Frage stellen, über welche Daten der Reseller und über welche Daten der Netzbetreiber verfügt.
[150] Vgl. hierzu auch Abbildung 3.

standsdaten gilt das unter Abschnitt a) Gesagte. Diesen Vorgaben entsprechend ergibt sich folgendes Datenbankschema:

Name	Typ	Bytes	Beispiel
ID	INT	4	256
Rufnummer des rufenden Teilnehmers	INT	4	4917612345678
Rufnummer des gerufenen Teilnehmers	INT	4	49176987654321
Beginn	DATETIME	8	13.1.2011 - 13:56:45
Ende	DATETIME	8	13.1.2011 - 14:36:12
Dienst[151]	TINYINT	1	1
IMSI des rufenden Teilnehmers	INT	4	262019876543210
IMEI des rufenden Teilnehmers	INT	4	012537458615879
Cell-ID des rufenden Teilnehmers	INT	4	458798525
IMSI des gerufenen Teilnehmers	INT	4	262019875689216
IMEI des gerufenen Teilnehmers	INT	4	01253745812345
Cell-ID des gerufenen Teilnehmers	INT	4	875903032

Tab. 4: Exemplarisches Schema eines Datensatzes, der entsprechend Art. 5 I VDSRL im Mobilfunkbereich zu speichern ist

Überträgt man das Beispiel aus dem Festnetzbereich (vgl. Abb. 21) auf den Mobilfunkbereich, so dass *Alice* und *Bob* über zwei unterschiedliche Mobilfunkanbieter mit dazwischengeschaltetem Verbindungsnetzbetreiber miteinander kommunizieren, so kann das Datenschema in Tab. 4 bei den jeweiligen Anbietern mit folgenden Daten gefüllt werden:

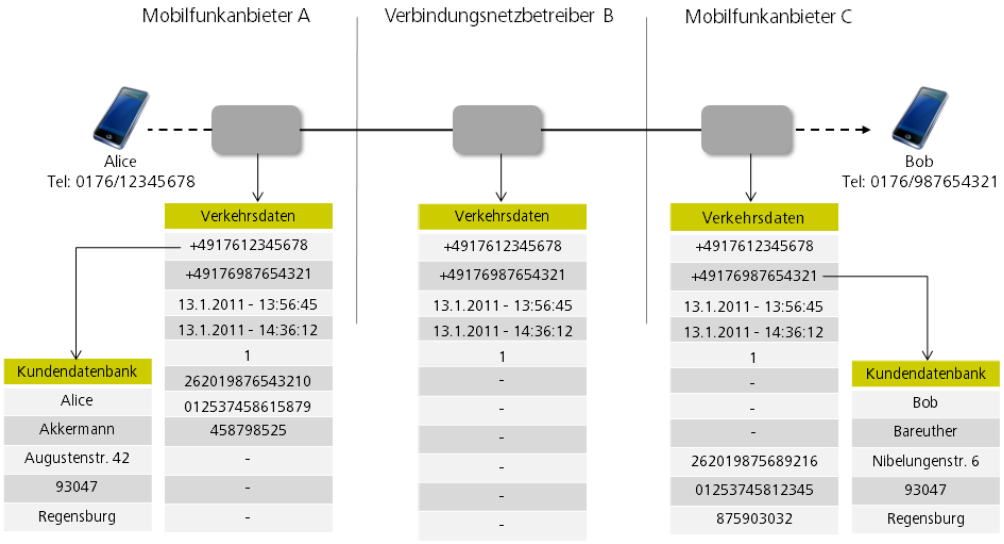


Abb. 22: Nach Art. 5 I VDSRL zu speichernde Verkehrsdaten im Falle des Telefonanrufs von Alice an Bob im Mobilfunknetz[152]

[151] 1 = Telefoniedienst, 2 = SMS-Dienst, 3 = MMS-Dienst, 4 = GPRS-Dienst, 5 = UMTS-Dienst, 6 = LTE-Dienst, 7 = Erste Aktivierung eines anonymen Dienstes (vgl. Art. 5 I lit. e) Nr. 2 vi) VDSRL).

[152] Es wird davon ausgegangen, dass der Mobilfunkanbieter A, der das Gespräch seiner Kundin Alice über das Verbindungsnetz B in das Netz des Mobilfunkbetreibers C leitet, keine Kenntnis von der IMSI, IMEI und Cell-ID von Bob hat. A weiß lediglich, dass sich der Teilnehmer mit der Rufnummer, die Alice gewählt hat, im Netz des Betreibers C befindet, das über das Verbindungsnetz des Betreibers B erreichbar ist. Analog dazu gestaltet sich der nicht abgebildete Datensatz bei dem Mobilfunkanbieter C (hier fehlen die technischen Daten sowie die Bestandsdaten in Bezug auf Alice).

Auch in diesem Fall ist die redundante Speicherung der Verkehrsdaten bei *Verbindungsnetzbetreiber B* überflüssig und damit nicht als verpflichtend anzusehen.

c) Vorratsdaten im Bereich des Internetzugangs

Die Konkretisierung der von den Internetzugangsanbietern zu speichernden Daten gestaltet sich etwas schwieriger. Art. 5 I lit. a) Nr. 2 VDSRL zählt drei Datentypen auf, die von Internetzugangs-Anbietern, E-Mail-Anbietern und Internet-Telefonie-Anbietern zu speichern sind. Dies sind (1) „die zugewiesene(n) Benutzerkennung(en)", (2) „die Benutzerkennung und die Rufnummer, die jeder Nachricht im öffentlichen Telefonnetz zugewiesen werden", sowie (3) der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine Internetprotokoll-Adresse (*IP*-Adresse), Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war".

Dem Begriff der „Benutzerkennung" in Art. 5 I lit. a) Nr. 2 i) VDSRL ist jedenfalls zu entnehmen, dass eine den entsprechenden Internetteilnehmer eindeutig identifizierende Kennziffer zu speichern ist. Vor dem Hintergrund der unterschiedlich verwendeten Zugangstechniken (vgl. Abb. 5) kann dies im Festnetz- oder Mobilfunkbereich die Rufnummer des Anschlusses sein. Diese ist im Falle des Zugangs in das Internet über einen Wählanschluss ohnehin zu speichern (vgl. Art. 5 I lit. e) Nr. 3) i) VDSRL). Im Bereich des Kabelnetzes, in dem die Adressierung nicht anhand von Rufnummern erfolgt, ist ein dementsprechendes Äquivalent (z.B. eine Benutzerkennung) zu speichern. Erfolgt der Zugang über ein freies *WLAN*, bleibt dem *ISP* nur die Speicherung der *MAC*-Adresse des *WLAN*-Clients als Benutzerkennung. Alternativ könnte technikübergreifend die zugewiesene *IP*-Adresse zusammen mit dem entsprechenden Zeitraum, in dem sie dem jeweiligen Teilnehmer zugewiesen war, als eindeutiges Identifikationsmerkmal dienen.[153] Die *IP*-Adresse ist zusammen mit dem Zeitraum, in dem sie dem entsprechenden Nutzer zugewiesen war, ohnehin gem. Art. 5 I lit. c) Nr. 2 i) VDSRL zu speichern. Erforderlich ist jedenfalls, dass das identifizierende Merkmal mit den Bestandsdaten der Kunden (vgl. Art. 5 I lit. a) Nr. 2 ii) VDSRL) eindeutig verknüpfbar ist, so dass jeder *IP*-Adresse im Internet eindeutig eine bestimmte Person zugeordnet werden kann. Die Vorgabe in Buchstabe ii) erscheint gemäß dieser Auslegung im Bereich des Internetzugangs als überflüssig.[154]

Nicht zu speichern sind die *IP*-Adressen oder gar *URI*s (*Uniform Resource Identifier*) der Kommunikationspartner, mit denen der Internetnutzer über das *HTTP*-Protokoll kommuniziert.[155] Deren Speicherung würde das in Art. 5 II VDSRL enthaltene Verbot verletzen. Vor allem die Kenntnis des *URI* ermöglicht weitreichende Blicke in den Inhaltsbereich der Kommunikation, so dass dessen Speicherung die Grenze des Art. 5 II VDSRL überschreiten würde.[156] Mit Ausnahme der seinen Kunden zugewiesenen *IP*-Adressen darf der *ISP* folglich keine Daten des verursachten Internetverkehrs speichern.

---

[153] Vgl. Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 50.
[154] Es wird angenommen, dass die Vorgabe in Art. 5 I lit. a) Nr. 2 ii) VDSRL nur für den Bereich der Internet-Telefonie gilt, vgl. Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 51.
[155] Ebenso wenig fallen von einem Suchmaschinendienst generierte Server-Protokolle, die die getätigten Suchanfragen enthalten, in den Anwendungsbereich der Richtlinie, vgl. hierzu Artikel-29-Datenschutzgruppe: Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, S. 13.
[156] Der *URI* ist ein Identifikator zur Bezeichnung von Webseiten, Dateien und weiteren Ressourcen im Internet. Er verweist z.B. auf ein spezielles *PDF*-Dokument, das der Internetnutzer abgefragt hat.

Zur Bestimmung des Endgeräts ist zudem eine Information über den Endpunkt des Urhebers des Kommunikationsvorgangs zu speichern. Der Endpunkt stellt den letzten Knoten der Internetverbindung auf Seiten des Nutzers dar, an dem die Daten an das Gerät des Endnutzers übergeben werden. Abhängig von der verwendeten Technologie (Endpunkte können mittels Wählanschluss, ISDN, DSL, Kabel, Mobilfunk oder WLAN realisiert werden), sind zur Identifikation des Endpunkts unterschiedliche Daten notwendig. Wird die Internetverbindung z.B. über das Festnetz hergestellt, so reicht die Angabe der Telefonnummer oder der *DSL*-Kennung aus.

Diesen Vorgaben entsprechend ergibt sich folgendes Datenschema der von den Internetzugangsanbietern zu speichernden Daten (die Daten können z.B. aus den *RADIUS*-Logs (vgl. Abb. 6) entnommen werden):

Name	Typ	Bytes	Beispiel
ID	INT	4	5865
Kundennummer / Telefonnummer	INT	4	499421123456
Log-in	DATETIME	8	13.1.2011 - 13:56:45
Log-out	DATETIME	8	14.1.2011 - 13:56:44
IP-Adresse	INT	4	84.56.67.213
Endpunkt	INT	4	499421123456

Tab. 5: Exemplarisches Schema eines Datensatzes, der entsprechend Art. 5 VDSRL vom ISP zu speichern ist

Über die Kunden- bzw. Telefonnummer können die Verkehrsdaten mit dem entsprechenden Eintrag zum Vertragspartner in der Kundendatenbank verknüpft werden. Das folgende Beispiel zeigt, welche Daten im konkreten Fall von einem *ISP* zu speichern sind:

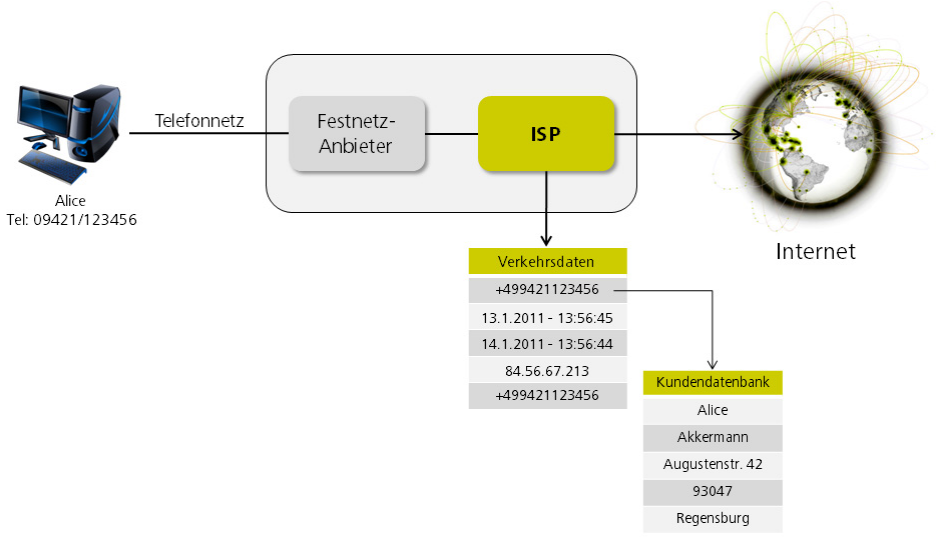


Abb 23: Nach Art. 5 I VDSRL zu speichernde Verkehrsdaten im Falle des Internetzugangs von Alice über das Telefonnetz[157]

D) Vorratsdaten im Bereich des E-Mail-Verkehrs

Im Bereich des E-Mail-Verkehrs müssen - soweit vorhanden - gem. Art. 5 I lit. a) Nr. 2 und lit. b) Nr. 2 VDSRL die E-Mail-Adressen des Absenders und des Empfängers sowie deren Namen und Anschrif-

[157] Vereinfachend wird davon ausgegangen, dass ISP-Provider zugleich der Festnetzbetreiber ist.

ten gespeichert werden. Gemäß Art. 5 I lit. c) Nr. 2 lit. ii) VDSRL umfasst die Speicherverpflichtung im E-Mail-Bereich zudem das „Datum und [die] Uhrzeit der An- und Abmeldung beim Internet-E-Mail-Dienst“. Die Speicherung des Zeitraums, in dem die Dienste des Mailservers in Anspruch genommen wurden, erscheint vor dem technischen Hintergrund, dass die Kommunikation mit dem Mailserver meistens eine automatisierte Datenübertragung darstellt (bei *SMTP-, IMAP-*, und *POP*-Verbindungen), deren Dauer von technischen Faktoren abhängt, als nicht zielführend.[158] Dementsprechend wird im vorliegenden Vorschlag nur der Zeitpunkt gespeichert, in dem die E-Mail an den Mailserver übergeben, also abgesendet wurde sowie der Zeitpunkt, in dem die E-Mail vom Mailserver des Empfängers abgerufen, also zugestellt wurde.

Fraglich ist, ob zudem die *IP*-Adressen des Senders und Empfängers der E-Mail gespeichert werden müssen, unter denen diese die Verbindung zu ihrem jeweiligen Mailserver aufbauen. Dem Wortlaut lässt sich dies aufgrund der Kumulation der Datentypen aus dem Internet, E-Mail- und *VoIP*-Bereich nicht eindeutig entnehmen. Über die gespeicherten *IP*-Adressen stünde den Ermittlungsbehörden neben den gespeicherten E-Mail-Adressen ein weiteres singularisierendes Anknüpfungsmerkmal zur Identitätsbestimmung zur Verfügung, sodass durch Anfrage beim entsprechenden *ISP* auf Daten aus einer weiteren Bestandsdatenbank zugegriffen werden könnte. Dies kann auch dazu dienen, den Verdacht von unschuldigen Personen abzulenken, deren E-Mail-Account z.B. gehackt wurde. Des Weiteren sind die bei den E-Mail-Anbietern gespeicherten Bestandsdaten oft untauglich zur Identitätsbestimmung, weil die von den Nutzern hinterlegten Bestandsdaten nicht verifiziert werden. Die *IP*-Adresse stellt dann die einzige Möglichkeit dar, den Sender oder Empfänger eine E-Mail zu identifizieren. Mit Blick auf Art. 1 II VDSRL wird im vorliegenden Vorschlag diesen Überlegungen gefolgt und folglich auch die *IP*-Adresse in das folgende Datenschema mit einbezogen.

Name	Typ	Bytes	Beispiel
ID	INT	4	2256
Sendezeit	DATETIME	8	13.1.2011 - 13:56:45
Zustellungszeit	DATETIME	8	13.1.2011 - 15:25:35
Absender-Mail-Adresse	VARCHAR	1 pro Buchstabe	alice@isp.de
Absender-IP	INT	4	84.56.67.213
Empfänger-Mail-Adresse	VARCHAR	1 pro Buchstabe	bob@mailservice.com
Empfänger-IP	INT	4	84.56.85.166
Internet-Dienst[159]	INT	1	5

Tab. 6: Schema eines Datensatzes, der entsprechend Art. 5 VDSRL vom E-Mail-Anbieter zu speichern ist

Im folgenden Szenario sendet *Alice* eine E-Mail an *Bob*. *Alice* kommuniziert hierzu über *SMTP* mit ihrem Mailserver, der von ihrem *ISP* betrieben wird (z.B. mit Mozilla Thunderbird). *Bob* hingegen ruft seine E-Mails über ein *HTTP*-Portal im Internet ab. Sein E-Mail-Anbieter betreibt eigene Mailserver und ist nicht identisch mit seinem *ISP*.

[158] Vgl. Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 85 f.
[159] ID zur eindeutigen Bestimmung des Internetzugangsanbieters.

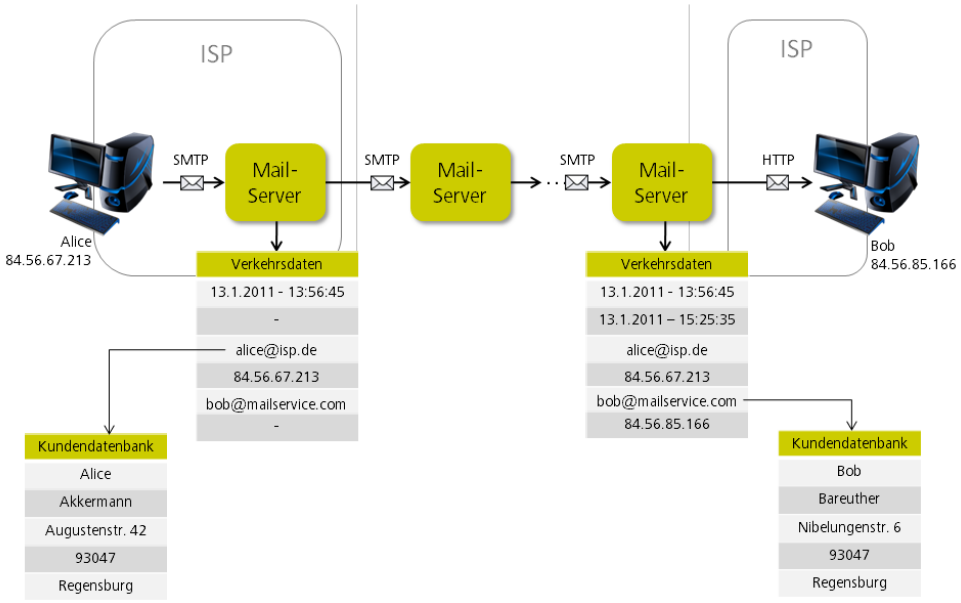


Abb. 24: Nach Art. 5 I VDSRL zu speichernde Verkehrsdaten im Falle des E-Mail-Verkehrs zwischen Alice und Bob

Der Mailserver von *Alice* erhält die erforderlichen Daten aus dem *SMTP*-Dialog zwischen dem Mail-Client von *Alice* und dem Mailserver. Der Zeitpunkt, zu dem *Bob* die E-Mail aus seinem Postfach abruft, sowie dessen E-Mail-Adresse sind dem *ISP* von *Alice* jedoch unbekannt. Der Mailserver von *Bob* hingegen kennt alle Daten des vorgeschlagenen Datensatzes. Die *IP*-Adresse von *Alice* und die Sendezeit können aus dem *Header* der E-Mail entnommen werden (diese werden von dem Mailserver von *Alice* in den *Header* geschrieben, vgl. oben Kapitel B. II. 3. d). Sofern der Mailserver von *Bob* jedoch im außereuropäischen Ausland angesiedelt ist (z.B. *GMX* oder *Google*), wäre dieser nicht zur Speicherung der Verkehrsdaten verpflichtet.

e) Vorratsdaten im Bereich der VoIP-Telefonie

Im Bereich der *VoIP*-Telefonie müssen - soweit vorhanden - gem. Art. 5 I lit. a) Nr. 2 und lit. b) Nr. 2 VDSRL die Benutzerkennung bzw. Telefonnummer sowie die Namen und Anschriften der Kommunikationsteilnehmer[160] gespeichert werden. Gemäß Art. 5 I lit. c) Nr. 2 lit. ii) VDSRL umfasst die Speicherverpflichtung im *VoIP*-Bereich zudem das „Datum und [die] Uhrzeit der An- und Abmeldung beim […] Internet-Telefonie-Dienst“. Diese Vorgabe wird in Analogie zum Festnetzbereich als Beginn und Ende der Kommunikation zwischen zwei Gesprächspartnern unter Zuhilfenahme von *VoIP*-Telefonie verstanden.[161] Aufgrund der gleichen Erwägungen wie im E-Mail-Bereich sind die *IP*-Adressen der Kommunikationspartner ebenfalls zu speichern. Damit ergibt sich folgendes Datenschema:

[160] Fraglich ist, ob die Kommunikation mittels Instant-Messenger auch in den Anwendungsbereich der Richtlinie fällt.
[161] So auch Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 116.

Name	Typ	Bytes	Beispiel
ID	INT	4	2256
Beginn der Kommunikation	DATETIME	8	13.1.2011 - 13:56:45
Ende der Kommunikation	DATETIME	8	13.1.2011 - 15:25:35
Benutzerkennung / Telefonnummer des rufenden Teilnehmers	VARCHAR	1 pro Buchstabe	Bob@biloxi.com
IP des rufenden Teilnehmers	INT	4	84.56.67.213
Benutzerkennung / Telefonnummer des gerufenen Teilnehmers	VARCHAR	1 pro Buchstabe	Alice@pc33.atlanta.com
IP des gerufenen Teilnehmers	INT	4	84.56.85.166
Internet-Dienst[162]	INT	1	5

Tab. 7: Nach Art. 5 I VDSRL zu speichernde Verkehrsdaten im Falle eines *VoIP*-Telefonats zwischen Alice und Bob

Diese von Art. 5 I VDSRL geforderten Daten können z.B. aus dem Protokollkopf eines *SIP*-Requests entnommen werden (vgl. Abbildung 13).

Die Bestimmung des Adressaten der Verpflichtung zur Speicherung von *VoIP*-Verkehrsdaten gestaltet sich aufgrund der dezentralen Realisierung der Kommunikation schwierig. So verfügen die Betreiber der *VoIP*-Server oft nicht über die notwendigen Verkehrsdaten (vgl. Kapitel B. II. 3. e). Sie verwalten lediglich die Datenbanken, in denen die Benutzernamen der angemeldeten Benutzer mit deren *IP*-Adressen korreliert werden. Verkehrsdaten über einzelne Kommunikationsvorgänge liegen diesen nicht vor. Dementsprechend wird vorgeschlagen, die *ISP* zu verpflichten, *VoIP*-Verkehrsdaten in ihren Zuständigkeitsbereichen zu speichern. Dies könnte z.B. mit Hilfe von Filtern geschehen, die über deren Internet-Traffic gelegt werden um z.B. *SIP*-Protokollköpfe auszulesen und abzuspeichern (z.B. mittels *Deep Packet Inspection*[163]). Aufgrund der großen Vielzahl an *VoIP*-Protokollen würde dies jedoch einen größeren Aufwand erfordern. Zudem sind *VoIP*-Pakete teilweise mit proprietären Verschlüsselungsmechanismen versehen (wie z.B. bei *Skype*), so dass der *ISP* die von Art. 5 I VDSRL geforderten Daten teilweise technisch nicht auslesen kann. Einfacher gestaltet sich die Bestimmung des zur Speicherung verpflichteten Telekommunikationsdiensteanbieters, sofern Telefonanrufe aus dem Mobilfunknetz oder dem Festnetz an einen *VoIP*-Teilnehmer adressiert sind. In diesem Fall liegen die entsprechenden Daten bei den Festnetz- und Mobilfunkbetreibern vor.

Zudem stellt sich die Frage, ob auch die zumeist in *VoIP*-Software integrierten *Instand-Messaging*-Systeme in den Anwendungsbereich der Vorratsdatenspeicherung fallen. Angesichts der *Peer-to-peer*-Struktur derartiger Dienste käme als Speicherverpflichteter wiederum nur der *ISP* in Betracht. Dies würde jedoch implizieren, dass auch die Verkehrsdaten aller weiteren *Instant-Messaging*-Systeme zu speichern wären. Dies würde einen unverhältnismäßigen Aufwand für den *ISP* beinhalten, sofern es überhaupt technisch möglich wäre, alle hierzu verwendeten Protokolldaten auszulesen. Außerdem sind *Instant-Messaging*-Systeme in Art. 5 I VDSRL nicht mit aufgeführt. Dementsprechend ist davon auszugehen, dass diese der Vorratsdatenspeicherung nicht unterliegen.

[162] ID zur eindeutigen Bestimmung des verwendeten Internetzugangsanbieters.
[163] Als Deep Packet Inspection wird ein Verfahren bezeichnet, das es den Netzbetreibern ermöglicht, automatisiert Datenpakete im Internet auszulesen und zu filtern.

F) Zusammenfassung

Die nähere Betrachtung der Vorgaben des Art. 5 I VDSRL hat gezeigt, dass sich die Menge der von den jeweiligen Diensteanbietern zu speichernden Daten größtenteils in den Grenzen technischer Realisierbarkeit hält. Vor allem die Ausnahme des *HTTP*-Internettraffics von der Speicherpflicht reduziert den von den Internetzugangsanbietern bereitzuhaltenden Speicherplatz. So wird dieser für die Vorratsdaten bei einem Internetzugangsanbieter mit 500.000 Nutzern, der zugleich E-Mail- und Internettelefonie-Dienste anbietet z.B. bei Vorliegen einer sechsmonatigen Speicherfrist auf 706 GB (9 GB für Internetverkehrsdaten, 626 GB für E-Mail-Verkehrsdaten und 73 GB für Internet-Telefonie-Verkehrsdaten) geschätzt, wobei 60% dieser 706 GB auf die Speicherung der Verkehrsdaten von SPAM-E-Mails zurückzuführen sind.[164]

Dennoch umfassen die Daten alle modernen Telekommunikationsbereiche, enthalten Bestands-, Verkehrs- und Ortsdaten und sind dementsprechend als hoch sensibel anzusehen. Im Hinblick auf die Speicherung von *VoIP*-Verkehrsdaten bestehen einige Unsicherheiten im Hinblick auf die Benennung des Speicherverpflichteten und die generelle technische Realisierbarkeit der Speicherung der erforderlichen Daten. Die Benennung der Daten hat zudem gezeigt, dass verschiedene Bereiche und Konstellationen existieren, in denen die Vorratsdaten auf verschiedene Anbieter verteilt sein können oder bei Nutzung außereuropäischer Dienste erst gar nicht anfallen. In der folgenden Tabelle sind alle Datenkategorien und Datentypen aufgeführt, die entsprechend den obigen Ausführungen von der Speicherverpflichtung umfasst sind:

[164] Vgl. Stampfel/Gansterer/Ilger: Data Retention, The EU Directive 2006/24/EC from a Technological Perspective, S. 124 ff.

Typ	Quelle	Festnetz	Mobilfunk	Internetzugang	E-Mail-Verkehr	VoIP-Telefonie
Rufender Teilnehmer						
Kennung	Verkehrsdaten	Rufnummer	Rufnummer	Benutzerkennung oder Rufnummer und zugeordnete IP-Adresse	E-Mail-Adresse und zugeordnete IP-Adresse	Benutzerkennung oder Rufnummer und zugeordnete IP-Adresse
Identität	Bestandsdaten	Name und Anschrift	Name und Anschrift	Name und Anschrift	Name und Anschrift	Name und Anschrift
Gerufener Teilnehmer						
Kennung	Verkehrsdaten	Rufnummer(n) (bei Rufweiterleitung auch die Nummer(n), an die der Anruf geleitet wird)	Rufnummer(n) (bei Rufweiterleitung auch die Nummer(n), an die der Anruf geleitet wird)	Inhaltsdaten	E-Mail-Adresse	Benutzerkennung oder Rufnummer und zugeordnete IP-Adresse
Identität	Bestandsdaten	Name und Anschrift	Name und Anschrift		Name und Anschrift	Name und Anschrift
Weitere Daten						
Zeitstempel	Verkehrsdaten	Beginn und Ende der Kommunikation (Datum und Uhrzeit)	Beginn und Ende der Kommunikation (Datum und Uhrzeit)	An- und Abmeldung vom Internetzugangsanbieter (Datum und Uhrzeit)	Aufgabe- und Abruf der E-Mail (Datum und Uhrzeit)	Beginn und Ende der Kommunikation (Datum und Uhrzeit)
Dienst	Verkehrsdaten	In Anspruch genommener Telefondienst	In Anspruch genommener Telefondienst[165]		In Anspruch genommener Internetdienst	In Anspruch genommener Internetdienst
Endeinrichtung	Verkehrsdaten/ Bestandsdaten	Rufnummern der Teilnehmer	IMSI und IMEI beider Teilnehmer	Rufnummer oder Endpunkt[166]		
Position (bei Verwendung mobiler Geräte)	Verkehrsdaten/ Bestandsdaten		Cell-IDs (und Daten zur Ortung von Funkzellen)			

Tab. 8: Kategorien und Typen der zu speichernden Daten nach Art. 5 VDSRL

[165] Beispiele: Telefonie, SMS, MMS etc.
[166] Beispiel: Kennung des DSL-Anschlusses.

2. Speicherdauer

Die Einhaltung der Speicherdauer verbunden mit der unwiderruflichen Löschung der Daten am Ende der Speicherfrist ist im Interesse der Telekommunikationsteilnehmer zu gewährleisten (Schutzziel Vertraulichkeit). Zudem spielt die veranschlagte Speicherdauer eine Rolle für den einzuplanenden Speicherbedarf für die Vorratsdaten. Gem. Art. 6 VDSRL müssen die in Abschnitt 1. dargestellten Daten über einen Zeitraum von sechs bis 24 Monaten gespeichert werden. Die genaue Festlegung der Speicherdauer überlässt die Richtlinie den Mitgliedstaaten. Bei Umsetzung einer 24-monatigen Speicherfrist fällt im Vergleich zur Mindestspeicherpflicht von sechs Monaten die vierfache Menge an Daten an (im obigen Beispiel wären dies annähernd drei Terabyte). Beginn der Speicherfrist ist nach Art. 6 VDSRL der „Zeitpunkt der Kommunikation". Dieser kann als Ende des entsprechenden Kommunikationsvorgangs konkretisiert werden, der den Vorratsdaten entnommen werden kann. Die Anlage eines zusätzlichen Feldes ist damit nicht erforderlich.

3. Zugriffsschwelle

Gemäß Art. 1 I VDSRL sollen die Daten zum „Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen." Eine Übermittlung entsprechender Daten an anfragende Stellen ist demnach nur zulässig, wenn es um die Verhinderung oder Verfolgung schwerer Straftaten geht, nicht aber z.B. zu Urheberrechtsverletzungen oder Ordnungswidrigkeiten. Die Zweckbindung kann nicht mit technischen Verfahren gewährleistet werden. Sie schränkt jedoch die Anzahl der Datenübermittlungen zwischen Telekommunikationsdiensteanbieter und Ermittlungsbehörden sowie die Zahl potentieller Stellen, die Daten aus den Beständen abrufen können, ein. Je enger die Zweckbindung, desto größer ist folglich die Vertraulichkeit der abgerufenen Daten einzuschätzen.

II. Vorgaben in Bezug auf die Datensicherheit der Vorratsdaten

Vorgaben in Bezug auf die zu gewährleistende Sicherheit der gespeicherten Daten finden sich sowohl in der VDSRL, der EDSRL und der DSRL. Art. 7 und Erwägungsgrund 15 der VDSRL stellen klar, dass die Vorschriften der DSRL und der EDSRL auch in Bezug auf die nach der VDSRL gespeicherten Verkehrsdaten Anwendung finden. Diesen Rechtsgrundverweisen auf die Datenschutzrichtlinien ist lediglich klarstellende Wirkung zuzusprechen. Verkehrsdaten sind personenbezogene Daten i.S.d. beiden Datenschutzrichtlinien, so dass diese auch ohne Artikel 7 VDSRL zur Anwendung kämen. Die in der DSRL und EDSRL enthaltenen Standards zum Schutz der Privatsphäre sollen das Vertrauen in die Datenverarbeitung stärken und so die Schaffung eines freien innereuropäischen Informationsraums (vgl. Art. 1 II DSRL) unterstützen.[167] Neben der Harmonisierung von rechtlichen Zulässigkeitsschranken zur Verarbeitung personenbezogener Daten spielt hierbei auch die Harmonisierung der Vorgaben in Bezug auf die technische und organisatorische Absicherung der gespeicherten oder übertragenen Daten eine Rolle.

Im Folgenden werden die sicherheitstechnisch relevanten Regelungen dieser Richtlinien dargestellt.

[167] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 23.

1. Sekundärrechtliche Vorgaben

a) Vorgaben aus der VDSRL: Die vier Grundsätze der Datensicherheit

Die Verankerung von Vorgaben zur Datensicherheit der gespeicherten Vorratsdaten im Richtlinientext der VDSRL war bis zum Erlass der Richtlinie umstritten. Die Europäische Kommission argumentierte, dass sich Zusatzbestimmungen zur Datensicherheit der Vorratsdaten aufgrund der Anwendbarkeit der Vorschriften aus der DSRL und der EDSRL erübrigten. Das Europäische Parlament hingegen schlug die explizite Verankerung der Schutzziele der Vertraulichkeit, Integrität und Authentizität der Daten im Richtlinientext vor.[168]

Schließlich verständigten sich die widerstreitenden Parteien auf die Verankerung von vier abstrakten „Grundsätze[n] der Datensicherheit" in Art. 7 VDSRL. Diese sind als Mindestvorgaben anzusehen, deren kumulative Einhaltung durch die Mitgliedstaaten sicherzustellen ist.

Der ersten Mindestanforderung in Art. 7 lit. a) VDSRL zufolge müssen die Vorratsdaten den gleichen Qualitätsanforderungen und der gleichen Sicherheit unterliegen wie im Netz vorhandene Daten. Der Beitrag dieser Mindestanforderung zur Sicherstellung eines ausreichenden Sicherheitsniveaus der Daten erscheint durchaus fraglich. Anstelle der Rückkopplung an das Qualitäts- und Sicherheitsniveau sonstiger im öffentlichen Kommunikationsnetz vorhandener Daten – das sich durch starke Inhomogenität auszeichnet – und der damit verbundenen Relativierung des Sicherheitsniveaus sollten eher Kriterien wie die Sensibilität und Aussagekraft der Daten über das Sicherheitsniveau entscheiden. Dementsprechend scheint Art. 7 lit. a) VDSRL lediglich einen weiteren Verweis auf die allgemeinen datenschutzrechtlichen Vorschriften zu enthalten.

Die zweite Mindestanforderung wird etwas konkreter. Art. 7 lit. b) VDSRL fordert die Implementierung geeigneter technischer und organisatorischer Maßnahmen, um „die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen". Durch die Nennung dieser potentiellen Bedrohungsszenarien adressiert Art. 7 lit. b) VDSRL die Schutzziele der Verfügbarkeit, Vertraulichkeit und Integrität. Die Authentizität der TK-Diensteanbieter und Ermittlungsbehörden bei der Übermittlung der Daten sowie die Gewährleistung der inhaltlichen Korrektheit der Daten finden hingegen keine explizite Berücksichtigung. Lediglich durch extensive Auslegung des Wortlauts könnte unter den Schutz vor „unrechtmäßige[r] […] Zugänglichmachung" auch die Gewährleistung der Authentizität der anfragenden Ermittlungsbehörde bei Übermittlung der Daten subsumiert werden.

Mit der Relativierung der Verpflichtung auf die Vornahme „geeigneter" technischer und organisatorischer Maßnahmen statuiert Art. 7 lit. b) VDSRL ein sehr abstraktes Mindestniveau und überlässt den Mitgliedstaaten einen großen Umsetzungsspielraum im Hinblick darauf, welche Schutzmaßnahmen im konkreten Fall geeignet sind und damit vorgeschrieben werden müssen. Dem Wortlaut des Art. 7 lit. b) VDSRL lässt sich nicht entnehmen, ob dieser sowohl die Implementierung technischer als auch organisatorischer Vorkehrungen fordert, oder ob bei ausreichender Eignung auch Vorkehrungen in einem der zwei Teilbereiche genügen. Aufgrund teleologischer Erwägungen ist

[168] Vgl. Art. 3a lit. h) und i) in der Anmerkung 27 des Europäischen Parlaments im Gesetzgebungsbericht vom 28.11.2005, A6-0365/2005, S. 16 im Internet abrufbar unter der URL http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A6-2005-0365&language=EN.

Art. 7 lit. b) VDSRL jedoch dahingehend zu verstehen, dass er technische und organisatorische Maßnahmen kumulativ fordert. Dies ergibt sich aus den Abhängigkeiten zwischen den zwei Bereichen. Ein Authentifizierungsverfahren allein ohne organisatorische Einteilung von Benutzergruppen liefe beispielsweise in die Leere.

Die dritte Mindestanforderung in Art. 7 lit. c) VDSRL bezieht sich auf das Schutzziel der Vertraulichkeit und fordert die Errichtung geeigneter technischer und organisatorischer Maßnahmen, „um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist". Dies ist als Teil-Konkretisierung der allgemeinen Pflicht zur Gewährleistung der Vertraulichkeit der Daten aus lit. b) zu sehen. Während lit. b) allgemein geeignete technische und organisatorische Maßnahmen zum Schutz vor unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung fordert, also die Bedrohungsszenarien beleuchtet, konkretisiert Art. 7 lit. c) VDSRL einen Kreis möglicher Maßnahmen mit dem Ziel der Beschränkung des zugriffsberechtigten Personals, um einem Teil dieser Bedrohungen entgegenzuwirken. Die ausdrückliche Forderung nach der Beschränkung des Zugangs zu den Daten auf einen bestimmten Personenkreis ist positiv zu werten. Nur so kann das Risiko des Missbrauchs der Daten durch interne Mitarbeiter der Telekommunikationsdiensteanbieter minimiert werden. Wie groß der privilegierte Personenkreis sein darf, wird in Art. 7 lit. c) VDSRL jedoch nicht geregelt.

Um die Anforderungen des Art. 7 lit. c) VDSRL zu erfüllen, schlägt die *Artikel-29-Datenschutzgruppe* in einem nicht rechtsverbindlichen Bericht folgende Maßnahmen vor:[169]

- „Strenge Kontrolle des Zugriffs auf die auf Vorrat gespeicherten Daten im Rahmen der Festlegung von Benutzerpflichten und Benutzerprofilen mit unterschiedlichen Benutzerberechtigungen;
- strenge Authentifizierung für den Zugang zum betreffenden System, basierend auf doppelten Authentifizierungsmechanismen (d. h. Passwort + biometrischen Daten oder Passwort + Token), um die körperliche Anwesenheit der für die Verarbeitung der Verkehrsdaten verantwortlichen Person sicherzustellen;
- detailgenaue Rückverfolgung der Arbeitsgänge bei Zugriff und Verarbeitung im Wege der Log-Vorratsspeicherung mithilfe von Zugriffsprotokollen (Logs), die zumindest die Benutzeridentität, die Zugriffszeit und die vom Zugriff betroffene Datei aufzeichnen;
- Einsatz von Log-Management-Lösungen zur Gewährleistung der Log-Integrität mithilfe von Verschlüsselungstechnologie oder Maßnahmen, die ein gleichwertiges Schutzniveau bieten;
- logische Trennung von anderen Systemen, die Verkehrsdaten zu kommerziellen Zwecken verarbeiten;
- zusätzliche Maßnahmen, die unter Umständen zur Sicherstellung der Vertraulichkeit von Daten nötig sind." [170]

[169] Berichte der Artikel-29-Datenschutzgruppe sind nicht rechtsverbindlich. Dementsprechend verpflichtet die folgende Aufzählung die Mitgliedstaaten nicht zur Sicherstellung der Implementierung der aufgezählten Maßnahmen. Die Aufzählung kann jedoch als Auslegungshilfe (i.S.v. Fallbeispielen) herangezogen werden, die helfen, die europarechtlichen Vorgaben zu konkretisieren.

[170] Artikel-29-Datenschutzgruppe: Bericht 01/2010, S. 15.

Zudem wird empfohlen, diese Maßnahmen in ein Sicherheitszertifizierungsprogramm, das Aufschluss über die Robustheit der eingeführten Maßnahmen gibt, einzubetten. Es wird zudem auf eine verstärkte Notwendigkeit der Kontrolle der Systemadministratoren hingewiesen.[171]

Nach Art. 7 lit. d) VDSRL (der vierten Mindestanforderung) müssen die nicht von den Ermittlungsbehörden abgerufenen Vorratsdaten am Ende der Vorratsspeicherfrist vernichtet werden. Dies erfordert die Implementierung automatisierter Datenlöschverfahren, so dass einzelne Datensätze, sobald die Speicherfrist überschritten ist, unverzüglich gelöscht werden. Manuelle Löschverfahren genügen dieser Anforderung nicht, weil diese die fristgerechte Löschung nicht ausreichend garantieren können.[172] Ausgenommen von der Löschung sind die von den Ermittlungsbehörden abgerufenen Daten. Unter der derzeitigen Rechtslage können diese Daten „de facto für einen unbestimmten zusätzlichen Zeitraum gespeichert werden“[173]. In Anbetracht der noch weiter gesteigerten Sensibilität dieser Daten wäre eine Regelung in Bezug auf diese Daten wünschenswert.

Art. 8 der VDSRL flankiert das Schutzziel der Verfügbarkeit. Danach haben die Mitgliedstaaten sicherzustellen, dass die Daten so gespeichert werden, dass sie unverzüglich an die zuständigen Behörden auf deren Anfrage hin weitergeleitet werden können.

Zur Überprüfung der Einhaltung dieser Kriterien muss in jedem Mitgliedstaat eine öffentliche unabhängige Kontrollstelle benannt werden, Art. 9 VDSRL. Der vorsätzliche Zugang zu den oder die vorsätzliche Übermittlung der Vorratsdaten muss nach nationalem Recht mit wirksamen, verhältnismäßigen und abschreckenden verwaltungsrechtlichen und strafrechtlichen Sanktionen belegt sein, vgl. Art. 13 II VDSRL.

b) Vorgaben aus der EDSRL

Gemäß Art. 4 I S. 1 Hs. 1 EDSRL trifft die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste die Pflicht, geeignete technische und organisatorische Maßnahmen zu ergreifen um die Sicherheit der angebotenen Dienste zu gewährleisten.

Art. 4 Ia EDSRL konkretisiert diese abstrakte Verpflichtung, indem mögliche Bedrohungsszenarien und Maßnahmen beschrieben werden, die verschiedenen zu berücksichtigenden Schutzzielen zugeordnet werden können. Die Vorgaben der Spiegelstriche 1 und 2 sind abgesehen von unbedeutenden Begriffsänderungen („unbeabsichtigt“ anstelle von „zufällig“) weitestgehend identisch mit den Vorgaben in Art. 7 lit. b) und c) VDSRL. Insofern kann auf die Ausführungen in Abschnitt a) verwiesen werden. Zusätzlich fordert Art. 4 Ia Spiegelstrich 3 EDSRL die Sicherstellung der Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten.

Über die Vorgaben der VDSRL hinausgehend normiert Art. 4 I S. 2 EDSRL zudem die Höhe des zu erreichenden Sicherheitsniveaus. Diese muss „angemessen“ sein. Ob konkrete Sicherheitsmaßnahmen einen angemessenen Schutz gewährleisten, hängt nach den Vorgaben in Art. 4 I S. 2 EDSRL von drei Faktoren ab: Dem Stand der Technik, den Kosten der Durchführung der Maßnahmen und dem bestehenden Risiko. So können zum Beispiel technische Neuerungen, die einen Anstieg der verfügbaren Rechenleistungen bedingen, die Verwendung stärkerer Schlüssel zur Verschlüsselung der Vorratsda-

[171] Vgl. Artikel-29-Datenschutzgruppe: Bericht 01/2010, S. 15 f.
[172] Vgl. Artikel-29-Datenschutzgruppe: Bericht 01/2010, S. 10.
[173] Artikel-29-Datenschutzgruppe: Bericht 01/2010, S. 16.

ten erfordern. Ebenso sind Softwaresysteme sicherheitstechnisch auf dem aktuellen Stand zu halten. Sofern für veraltete Systeme keine Sicherheitsupdates mehr erhältlich sind, oder sich herausstellt, dass diese kein ausreichendes Sicherheitsniveau gewährleisten können, sind diese durch neue, ein angemessenes Sicherheitsniveau gewährleistende Systeme zu ersetzen. Das bestehende Risiko von Sicherheitsverletzungen, das sich aus Wahrscheinlichkeit und potentiellem Schaden einer Sicherheitsverletzung errechnet, steht in positiver Korrelation zum anzustrebenden Sicherheitsniveau: Je höher das Risiko einer Verletzung der IT-Sicherheit einzuschätzen ist, desto höher sind die Anforderungen an ein angemessenes Sicherheitsniveau. So kann z.B. auch eine sehr unwahrscheinliche aber nicht komplett auszuschließende Sicherheitsverletzung, die einen immensen Schaden anrichten kann, zur Erforderlichkeit eines hohen Schutzniveaus führen. Zudem sind die Kosten entsprechender Sicherheitsmaßnahmen zu berücksichtigen. Diese sollten jedoch v.a. in Bezug auf sensible Daten wie Vorratsdaten ein nur schwaches Kriterium darstellen, um deren Schutz nicht vollständig von Kosten- und Wirtschaftlichkeitsüberlegungen abhängig zu machen.

c) Vorgaben aus der DSRL

Art. 6 I lit. d) DSRL adressiert das Schutzziel der inhaltlichen Korrektheit der gespeicherten Daten. Gem. Art. 6 I lit. d) DSRL müssen die Mitgliedstaaten vorsehen, dass „personenbezogene Daten […] sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind". Hierzu sind „alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nichtzutreffende oder unvollständige Daten gelöscht oder berichtigt werden". Welche Maßnahmen hierunter konkret zu verstehen sind, gibt die Richtlinie nicht vor. Ob z.B. die Pflicht zur regelmäßigen Überprüfung von Bestandsdaten der Kunden von Telekommunikationsdiensteanbietern besteht, weil deren Aktualität für den Zweck der Vorratsdatenspeicherung – die Identifizierung des Telekommunikationsteilnehmers – erforderlich ist, liegt damit in der Hand der nationalen Gesetzgeber.[174]

Art. 6 I lit. e) DSRL ist im Hinblick auf die Löschpflicht der Vorratsdaten relevant. Gemäß Art. 6 I lit. e) DSRL müssen personenbezogene Daten, die für den Zweck, zu dem sie erhoben wurden, nicht mehr benötigt werden, anonymisiert werden.[175] In die gleiche Richtung zielend, aber mit schärferem Wortlaut statuiert Art. 7 lit. d) VDSRL (vgl. Abschnitt a), dass Vorratsdaten am Ende der Speicherfrist „vernichtet" werden müssen. Angesichts dessen ist davon auszugehen, dass der nach dem *lex posterior*-Grundsatz[176] im Kollisionsfall vorgehende Art. 7 lit. d) VDSRL eine Anonymisierung der Vorratsdaten nicht gelten lässt. Die Daten müssen am Ende der Speicherpflicht unwiderruflich gelöscht werden.

Art. 16 DSRL statuiert in Parallele zu Art. 7 lit. c) VDSRL und Art. 4 Ia Spiegelstrich 1 EDSRL das Erfordernis der Verantwortlichkeitsregelung[177] und komplettiert damit den Schutz der Vertraulichkeit der Vorratsdaten vor Angriffen durch Mitarbeiter bei den TK-Diensteanbietern. Während sich die Vorschriften in der VDSRL und EDSRL auf technische und organisatorische Aspekte des Zugangs zu

[174] Vgl. Ehmann/Helfrich: EG Datenschutzrichtlinie, Art. 6, Rn. 27.
[175] Vgl. Ehmann/Helfrich: EG Datenschutzrichtlinie, Art. 6, Rn. 30 f.
[176] Der lex posterior-Grundsatz besagt, dass im Falle der Kollision zweier rechtlicher Normen die später erlassene Norm anzuwenden ist.
[177] so auch die Interpretation von Art. 16 DSRL in Bauer/Reimer: Handbuch Datenschutzrecht, S. 72.

den Daten beziehen, bezieht sich Art. 16 DSRL auf organisatorische Maßnahmen zum Schutz der Vertraulichkeit bei der Verarbeitung.

2. Europaweite Technische Standards

Die Konkretisierung der in Kapitel D.II. aufgezeigten sekundärrechtlichen Vorgaben zur Sicherheit der Vorratsdaten erfolgt insbesondere im Rahmen von technischen Spezifikationen durch das *Europäische Institut für Telekommunikationsnormen* (*ETSI*).[178] Die vom *ETSI* verabschiedeten Standards sind zwar originär nicht rechtsverbindlich und dementsprechend als Empfehlungen anzusehen, können jedoch dadurch, dass nationale Gesetze und Verwaltungsvorschriften auf diese Bezug nehmen, in den einzelnen Mitgliedstaaten rechtsverbindlichen Status erlangen.

a) Technische Spezifikation 102 656 V1.2.1 (2008-12)

Die *Technische Spezifikation 102 656 V1.2.1 (2008-12)* enthält Anforderungen an die technische Ausgestaltung der Verarbeitung der Daten und der Übergabeschnittstelle, die sich aus den Schutzinteressen der Ermittlungsbehörden ergeben. Anforderungen an die Übermittlungsschnittstelle sind hiernach: Zuverlässigkeit, Fehlerfreiheit, geringe Kosten, schnelle Beantwortung, standardisierte Abläufe und Sicherheit.[179]

Die Spezifikation nennt folgende Schutzziele und Maßnahmen: [180]

- Schutz der Vertraulichkeit von Informationen über die Abfragen der Ermittlungsbehörden (welche Informationen wurden abgefragt, wie viele Anfragen, in welchem Zeitraum) (lit.a)
- Beschränkung der Anzahl der Mitarbeiter, die mit der Bearbeitung von Anfragen befasst sind (lit.b)
- Übermittlung über eine spezielle Übergabeschnittstelle (lit. c)
- Kein Zugriff unautorisierter Personen auf die Übergabeschnittstelle (lit. d)
- Schutz der Übergabeschnittstelle gegen Missbrauch (lit. e)
- Beantwortung der Anfrage nur in dem Umfang, in dem sie von Gericht/Staatsanwaltschaft autorisiert wurde (lit. f)
- Authentifizierungsmechanismus bei jeder Verbindung, falls keine eigenen abgeschotteten Übertragungskanäle verwendet werden (lit. g), h)
- Gewährleistung der Vertraulichkeit der Daten bei der Übermittlung (durch Verschlüsselung) (lit. i)
- Manipulationssichere Protokollierung von Anfragen (Anfragekriterien, Zeit und Zeitfenster der Anfrage, Empfängeradresse, beteiligte Mitarbeiter, Verweis auf die richterliche/staatsanwaltschaftliche Genehmigung) und Beschränkung des Zugangs zu den protokollierten Daten (lit. j), k)

[178] Zudem existieren Normungen weiterer Normungsorganisationen, wie z.B. CENELEC, CEN und CC
[179] Vgl. ETSI TS 102 656 V1.2.1 (2008-12), S. 4.
[180] Vgl. ETSI TS 102 656 V1.2.1 (2008-12), S. 12, Abschnitt 4.9.

Anforderungen im Hinblick auf die sicherheitstechnische Absicherung der eigentlichen Datenpools enthält die Spezifikation nicht. Sie verweist diesbezüglich auf nationale sicherheitstechnische Vorschriften.[181]

Kapitel 4.11 der Spezifikation enthält weitere technische Vorgaben in Bezug auf die Übergabeschnittstelle und das Format der zu übermittelnden Daten.[182] Die Daten sind hiernach in einem offenen Format zu kodieren, also in einem Format, das ohne rechtliche Einschränkungen genutzt werden kann (z.B. im XML-Format). Die Übergabeschnittstelle ist nach allgemeinen Standards, unter Nutzung der allgemein verfügbaren Übertragungswege, Protokolle und Codierungen zu gestalten. Welche Netzwerkschichten konkret genutzt werden, bestimmt sich nach nationalem Recht. Zudem muss ein Berichtswesen implementiert werden, das Fehler bei der Übertragung aufdeckt.

Der informative Anhang der Spezifikation enthält zudem Vorgaben in Bezug auf Geheimhaltungspflichten der die Vorratsdaten verarbeitenden Diensteanbieter und Netzbetreiber. Demzufolge sind Informationen über die konkrete technische Implementierung der Vorratsdatenspeicherung und Informationen über Anfragen von Vermittlungsbehörden geheim zu halten. Sofern Netzbetreiber und Diensteanbieter zur Beantwortung von Anfragen von Ermittlungsbehörden kooperieren, um die erforderlichen Informationen zu aggregieren, ist der Informationsaustausch zwischen diesen auf das zur Beantwortung der Anfrage erforderliche Maß zu beschränken.

b) Technische Spezifikation 102 657 V1.7.1 (2010-10)

Die *technische Spezifikation 102 657 V1.7.1 (2010-10)* konkretisiert eine mögliche technische Ausgestaltung der elektronischen Schnittstelle zur Anfrage von Vorratsdaten und deren anschließender Übermittlung an die Ermittlungsbehörden.[183] Sie enthält optionale[184] Vorgaben in Bezug auf mögliche Sicherheitsmaßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und Authentizität bei der Kommunikation zwischen Ermittlungsbehörde und Netzbetreiber bzw. Diensteanbieter. Hierbei wird zwischen Maßnahmen auf der Verbindungsschicht und der Anwendungsschicht unterschieden.[185]

Auf Ebene der Verbindungsschicht werden Maßnahmen zur gegenseitigen Authentifizierung sowie zur Gewährleistung der Vertraulichkeit und Integrität empfohlen (z.B. *TLS, IPSec* und *HTTPS*). Auf Ebene der Anwendungsschicht wird die Verwendung von digitalen Signaturen (z.B. *DSS/DSA*) und zertifikatbasierten Systemen empfohlen.

III. Fazit

Die in Abschnitt II. dargestellten verbindlichen europarechtlichen Vorgaben zur sicherheitstechnischen und organisatorischen Absicherung der Vorratsdaten gestalten sich sehr abstrakt, heterogen und lassen eine in sich schlüssige Dogmatik vermissen. So beziehen sich die Normen teilweise auf zu verhindernde Bedrohungsszenarien, teilweise auf zu gewährleistende Schutzziele und teilweise auf einen

---

[181] Vgl. ETSI TS 102 656 V1.2.1 (2008-12), S. 13, Abschnitt 4.10.
[182] Vgl. ETSI TS 102 656 V1.2.1 (2008-12), S. 13, Abschnitt 4.11.
[183] Im Anhang I der Spezifikation TS 102 657 V1.7.1 (2010-10), S. 103 finden sich Vorgaben zu manuellen Übermittlungsmethoden wie Telefon, Fax, E-Mail oder DVD.
[184] Vgl. ETSI TS 102 657 V1.7.1 (2010-10), S. 31, Abschnitt 8.1.
[185] Vgl. hierzu und im Folgenden ETSI TS 102 657 V1.7.1 (2010-10), S. 31 ff., Abschnitt 8.

konkreten Kreis von Maßnahmen. In den Generalklauseln (Art. 7 lit. b) VDSRL und Art. 17 I DSRL) reiht der Gesetzgeber eine Vielzahl von Bedrohungsszenarien aneinander und verlangt schlicht übergreifend angemessene Maßnahmen zum Schutz vor diesen Bedrohungen. Positiv zu bewerten ist, dass die europarechtlichen Vorschriften (bei weiter Wortlautauslegung) in ihrer Gesamtheit alle im Rahmen der Vorratsdatenspeicherung zu berücksichtigenden Schutzziele adressieren. Dies zeigt Tabelle 9, in der die sekundärrechtlichen Vorgaben den verschiedenen, im Rahmen der Vorratsdatenspeicherung zu berücksichtigenden Schutzzielen zugeordnet sind. Im Hinblick auf den Schutz der Vertraulichkeit besteht die größte Regelungsdichte. Die Verpflichtung zur Umsetzung eines Sicherheitskonzepts (Art. 4 Ia Sstr. 3 EDSRL) ist ebenfalls als positiv zu werten.

Die Regelungen in Art. 7 VDSRL, die speziell für die Sicherheit der Vorratsdaten gelten, enttäuschen aus sicherheitstechnischer Sicht. Abgesehen von der Pflicht zur Vernichtung der Vorratsdaten am Ende der Speicherfrist in Art. 7 lit. d) VDSRL verweisen die Regelungen auf die sicherheitstechnischen Vorgaben der allgemeinen Datenschutzrichtlinien, die allgemein für jegliche Verarbeitung von personenbezogenen Daten gelten. Damit wurde die gesetzgeberische Gelegenheit verpasst, ein explizites Sicherheitsniveau für die Vorratsdaten zu statuieren. Art. 7 DSRL hätte dafür ausreichend Raum geboten. Auch Forderung der *Artikel-29-Datenschutzgruppe*, die in Art. 7 VDSRL verankerten Grundsätze durch Mindeststandards (vgl. oben Kapitel D. II. 1. a) zu ergänzen, die genau regeln, welche technischen und organisatorischen Sicherheitsvorkehrungen die Anbieter treffen müssen[186], konnte den europäischen Gesetzgeber nicht zu einer über bereits bestehende Regeln hinausgehende Verankerung eines Sicherheitsniveaus bewegen.

Angesichts dessen bleibt zu fragen, inwiefern die allgemeinen Vorschriften aus den Datenschutzrichtlinien ein ausreichendes Sicherheitsniveau für die Absicherung der Vorratsdaten vorgeben. Diese knüpfen das zu gewährleistende Sicherheitsniveau an die Faktoren Technik, Kosten und Risiko (das sich aus der Natur der Daten und der Art der Verarbeitung der Daten ergibt). Das mit den Vorratsdaten zusammenhängende Risikoniveau spricht im Rahmen der Abwägung zwischen diesen drei Faktoren jedenfalls für die Anwendung strenger, risikogewichteter Sicherheitsstandards.[187] Dem gegenüber stehen die erforderlichen Aufwendungen für die Implementierung der Sicherheitsmaßnahmen, die je nach Unternehmensgröße und entsprechenden Skalenvorteilen mehr oder weniger belastend sind. Mit welcher Gewichtung diese einzelnen Faktoren in die Abwägung einzufließen haben, geben Art. 4 I 2 EDSRL und Art. 17 I 2 DSRL nicht vor. Vielmehr überlässt es der europäische Gesetzgeber den einzelnen Mitgliedstaaten, diese Abwägung rechtlich näher auszugestalten. Die technischen Spezifikationen des *ETSI* zur Vorratsdatenspeicherung können hierbei behilflich sein, auch wenn diese vorrangig nur die Schutzziele der Ermittlungsbehörden adressieren. Eine stärkere Berücksichtigung der Schutzziele der Telekommunikationsteilnehmer wäre in diesem Rahmen wünschenswert.

---

[186] Vgl. Artikel-29-Datenschutzgruppe: Stellungnahme 3/2006 zur Richtlinie 2006 des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, S. 3 f.

[187] Vgl. Artikel-29-Datenschutzgruppe: Bericht 01/2010, S. 13.

	Art. 7 VDSRL	Art. 8 VDSRL	Art. 4 EDSRL	Art. 6 DSRL	Art. 16 DSRL	Art. 17 DSRL
Vertraulichkeit	Schutz gegen unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung *(lit. b)* Zugang zu Daten ausschließlich durch besonders ermächtigten Personen *(lit c)* Vernichtung der Daten am Ende der Speicherfrist *(lit d)*		Schutz vor unbefugter oder unrechtmäßiger Speicherung, unbefugtem oder unberechtigtem Zugang oder unbefugter oder unrechtmäßiger Weitergabe *(Abs. 1a Sstr. 2)* Zugang nur durch ermächtigte Personen für rechtlich zulässige Zwecke *(Abs. 1a Sstr. 1)*		Verarbeitung nur auf Weisung des für die Verarbeitung Verantwortlichen	Schutz gegen unberechtigte Weitergabe oder unberechtigten Zugang und gegen jede andere Form der unrechtmäßigen Verarbeitung *(Abs. 1)*
Verfügbarkeit	Schutz gegen zufällige oder unrechtmäßige Zerstörung oder zufälligen Verlust *(lit. b)*	Unverzügliche Weiterleitung an die zuständigen Behörden	Schutz vor unbeabsichtigter oder unrechtmäßiger Zerstörung oder unbeabsichtigtem Verlust *(Abs. 1a Sstr. 2)*			Schutz gegen zufällige oder unrechtmäßige Zerstörung oder zufälligen Verlust *(Abs. 1)*
Inhaltliche Korrektheit				Sachliche Richtigkeit und wenn nötig auf den neuesten Stand gebracht *(Abs. 1 lit. d)*		
Integrität	Schutz gegen zufällige Änderung oder unberechtigte oder unrechtmäßige Speicherung *(lit. b)*		Schutz vor unbeabsichtigter Veränderung und unbefugter oder unrechtmäßiger Speicherung *(Abs. 1a Sstr. 2)*			Schutz gegen unberechtigte Änderung *(Abs. 1)*
Authentizität	Schutz gegen unrechtmäßige Zugänglichmachung (lit. b)[188]		Schutz vor unbefugtem oder unberechtigtem Zugang *(Abs. 1a Sstr. 2)*[188]			*(Abs. 1)*Schutz gegen unberechtigten Zugang[188]
Maßnahmen	Geeignete technische und organisatorische Sicherheitsmaßnahmen		Geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Dienste *(Abs. 1 Hs. 1)* Umsetzung eines Sicherheitskonzepts *(Abs. 1a Sstr. 3)*	Angemessene Maßnahmen zur Berichtigung oder Löschung nichtzutreffender oder unvollständiger Daten *(Abs. 1 lit. d)*		Geeignete technische und organisatorische Sicherheitsmaßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus *(Abs. 1)*
Berücksichtigung			Technik, Kosten, Risiko *(Abs. 1 S. 2)*			Technik, Kosten, Risiko *(Abs. 1 S. 2)*

Tab. 9: Europarechtliche Vorgaben mit datensicherheitstechnischem und -organisatorischem Bezug

[188] Die grau eingefärbten Vorgaben in diesem Bereich beschränken bei extensiver Wortlautauslegung auf die Gewährleistung der Authentizität der Ermittlungsbehörde bei Abfrage der Daten.

E. Vergleichende Betrachtung der einzelstaatlichen Umsetzungen

Für die einzelnen Telekommunikationsunternehmen in den Mitgliedstaaten sind die in Kapitel D. dargestellten Regelungen nicht unmittelbar verbindlich, vgl. Art. 288 III AEUV.[189] Europäische Richtlinie richten sich von ihrer rechtlichen Wirkung her zunächst an die zuständigen staatlichen Stellen der Mitgliedstaaten, die verpflichtet sind, die Vorgaben der Richtlinien innerhalb der Umsetzungsfrist in nationales Recht umzusetzen („gemeinschaftsrechtlicher Umsetzungsbefehl“[190]). Erst diese nationalen Vorschriften stellen für die Telekommunikationsunternehmen unmittelbar geltendes Recht dar. Damit drängt sich die Frage auf, ob und wenn ja in welcher konkreten Ausgestaltung die 27 Mitgliedstaaten die in Kapitel B dargestellten europarechtlichen Vorgaben zur Gewährleistung der Datensicherheit der Vorratsdaten in nationales Recht umgesetzt haben. Der Fokus der Betrachtung richtet sich dabei vor allem auf nationale Vorgaben, die über die europarechtlichen Vorgaben hinausgehen. Da erst die Gesamtschau der nationalen rechtlichen und praktischen Umsetzungen, die untereinander und mit den Vorgaben der Richtlinien inhaltlich verglichen werden können, Aussagen über das tatsächliche europaweit implementierte Sicherheitsniveau ermöglicht, wird im folgenden neben den rechtlichen Vorgaben zudem die praktische Umsetzung der einzelstaatlichen Vorgaben in den Telekommunikationsunternehmen beleuchtet.

I. Aktueller Umsetzungsstand

Aufgrund der breiten und zugespitzten gesellschafts- und rechtspolitischen Diskussionen um die Vorratsdatenspeicherung verlief deren Umsetzung auf nationaler Ebene nur schleppend. Nach Ablauf der Umsetzungsfrist am 15.9.2007 (vgl. Art. 15 I 1 VDSRL) hatten lediglich acht Mitgliedstaaten (Deutschland, Dänemark, Estland, Frankreich, Großbritannien, Lettland, Spanien und Tschechien) einzelstaatliche Durchführungsmaßnahmen ergriffen und die Vorgaben in nationales Recht umgesetzt.[191] Bis dahin war, soweit die Mitgliedstaaten von der Möglichkeit des Vorbehalts Gebrauch gemacht hatten (vgl. Art. 15 III 1 VDSRL), zumindest die Speicherpflicht in Bezug auf Mobilfunk- und Festnetztelefonie umzusetzen.[192] Nachdem die Vorgaben der VDSRL ein Jahr später von Griechenland, Irland, den Niederlanden, Österreich, Polen und Schweden noch nicht umgesetzt waren, leitete die Kommission ein Vertragsverletzungsverfahren gegen jeden dieser sechs Mitgliedstaaten ein.[193]

---

[189] Eine unmittelbare Geltung von Richtlinien kommt nur in Ausnahmefällen unter bestimmten Voraussetzungen (nach Ablauf der Umsetzungsfrist und bei Regelungen ohne Umsetzungsspielraum) in Betracht. Im Hinblick auf die Vorratsdatenspeicherungsrichtlinie scheidet diese aufgrund des bestehenden Umsetzungsspielraums (z.B. in Bezug auf die Speicherfrist zwischen 6-24 Monaten und in der Richtlinie fehlende Vorgaben zur Zweckbindung) aus.

[190] Szuba: Vorratsdatenspeicherung, S. 262.

[191] Vgl. Wimmer Andersson/ Buchinger u.a.: Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung, S. 6. Teilweise bestanden in verschiedenen Mitgliedstaaten schon vor Erlass der Richtlinie 2006/24/EG nationale Regelungen zur Speicherung von Verkehrsdaten, vgl. zur Rechtslage vor der VDSRL Büllingen/Gillet/Gries/Hillebrand/Stamm: Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich, im Internet abrufbar unter der URL http://www.humanistische-union.de/fileadmin/hu_upload/doku/vorratsdaten/info/Studie_VDS_final_lang.pdf.

[192] 16 Mitgliedstaaten haben den Vorbehalt gem. Art. 15 III 1 VDSRL erklärt, so dass diesen bezüglich der „Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail“ ein Aufschub der Umsetzung bis zum 15. März 2009 gewährt wurde. England und Tschechien haben den Vorbehalt nicht beansprucht.

[193] Vgl. Szuba: Vorratsdatenspeicherung, S. 263.

Griechenland, Irland, Österreich und Schweden konnten letztendlich die Feststellung einer Vertragsverletzung durch den EuGH nicht mehr abwenden.[194]

Bis zum Zeitpunkt der Einreichung dieser Arbeit (August 2011) haben alle nationalen Gesetzgeber – mit Ausnahme von Schweden – die Vorratsdatenspeicherung in ihrer jeweiligen einzelstaatlichen Rechtsordnung verankert.[195] Die Kommission hat dementsprechend am 31. Mai 2011 beantragt, Schweden unter anderem zu einer Strafzahlung von täglich 40947,20 € zu verurteilen, bis die Richtlinie umgesetzt und damit die Vertragsverletzung abgestellt wird.[196] Österreich hat das Gesetz zur Einführung der VDS[197] am 29. April 2011 beschlossen. Dieses tritt am 1. April 2012 in Kraft.

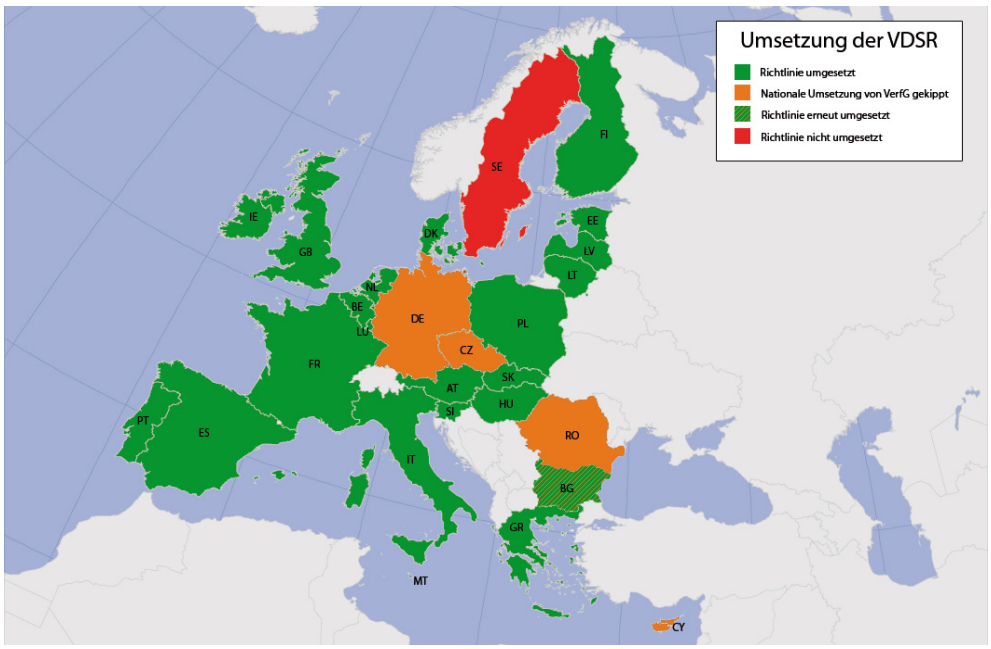


Abb. 25: Nationaler Umsetzungsstand der VDSRL im Vergleich[198]

In fünf Mitgliedstaaten (Bulgarien, Deutschland, Rumänien, Tschechien und Zypern) wurden die nationalen Regelungen von den jeweiligen höchsten Gerichten verworfen.[199] Nur eines dieser Länder

[194] Urteil des Gerichtshofes (Sechste Kammer) vom 4. Februar 2010 – Europäische Kommission/Schweden, Rechtssache C-185/09, Amtsblatt der Europäischen Union vom 27.3.2010, C 80/6; Urteil des Gerichtshofes (Siebte Kammer) vom 29. Juli 2010 – Europäische Kommission/Republik Österreich, Rechtssache C-189/09, Amtsblatt der Europäischen Union vom 11.9.2010, C 246/8; Urteil des Gerichtshofes (Achte Kammer) vom 26. November 2009 – Europäische Kommission/Irland, Rechtssache C-202/09, Amtsblatt der Europäischen Union vom 30.1.2010, C 24/16; Urteil des Gerichtshofes (Zweite Kammer) vom 26. November 2009 – Europäische Kommission/Griechenland, Rechtssache C-211/09, Amtsblatt der Europäischen Union vom 30.1.2010, C 24/16.

[195] Eine Übersicht über alle nationalen Umsetzungsgesetze findet sich unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72006L0024:DE:NOT.

[196] Vgl. Klage, eingereicht am 31. Mai 2011 — Europäische Kommission/Königreich Schweden - Rechtssache C-270/11, Amtsblatt der Europäischen Union vom 30.7.2011, C 226/17.

[197] Das österreichische Umsetzungsgesetz ist im Internet abrufbar unter der URL ftp://ftp.freenet.at/privacy/gesetze/vorratsdatenspeicherung.pdf.

[198] Die thematischen Karten wurden unter Zuhilfenahme eines Tools im Internet erstellt (http://geo.dianacht.de/makemap/) und anschließend mit Bildbearbeitungssoftware nachbearbeitet. Die Datenquellen der Abbildungen befinden sich im Anhang in den Abschnitten 1)-4).

[199] Urteil des Obersten Bulgarischen Verwaltungsgerichts vom 11. Dezember 2008, vgl. zudem die Meldung auf heise.de, im Internet abrufbar unter der URL http://www.heise.de/newsticker/meldung/Vorratsdatenspeicherung-in-Bulgarien-vorerst-gestoppt-192081.html; Urteil des Deutschen Bundesverfassungsgerichts vom 15. Dezember 2009, BVerfGE 125, 260, im Internet abrufbar unter der URL http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintVersion&Name=bv125260; Urteil des Rumänischen

(Bulgarien) hat seitdem rechtstechnisch nachgebessert und die Vorratsdatenspeicherung erneut mit Änderungen rechtlich implementiert.[200]

Belgien spielt gewissermaßen eine Sonderrolle. Obwohl Belgien die Richtlinie bisher nicht förmlich umgesetzt hat, geht die Kommission[201] aufgrund der dortigen Rechtslage und Praxis von einer (teilweisen) Umsetzung aus.[202]

Damit ist die VDS aktuell in 22 der 27 Mitgliedstaaten der EU rechtlich verbindlich umgesetzt. Auf diese Mitgliedstaaten beziehen sich die folgenden Ausführungen. Im Hinblick auf die nähere zukünftige Entwicklung bleibt der Ausgang aktuell anhängiger verfassungsrechtlicher Klagen in Irland, Polen und Ungarn abzuwarten.

II. Kategorien der zu speichernden Daten

Rechtlich betrachtet haben mit Ausnahme von Belgien[203] alle Mitgliedstaaten, die die Richtlinie bislang umgesetzt haben, die Speicherung der von der VDSRL vorgegebenen Datenkategorien und Datentypen (vgl. Kapitel D. I. 1.) vorgesehen.[204] Darüber hinausgehend zeigt die Betrachtung der nationalen Gesetzgebungsverfahren jedoch punktuelle (erfolgreiche) Versuche, auch Inhaltsdaten mit in die Vorratsdaten einfließen zu lassen. So verpflichtet die am 15. September 2007 in Kraft getretene dänische Verordnung die dänischen Internetzugangsanbieter zur Speicherung von *IP*-Protokollkopfdaten (*IP*-Adressen und *Port*-Nummern) des ersten, letzten und jedes 500sten *IP*-Pakets einer Internetsitzung.[205] Dies ermöglicht einen Rückschluss auf aufgerufene Internetseiten und verwendete Dienste und verstößt eindeutig gegen das Verbot der Speicherung von Inhaltsdaten aus Art. 5 II VDSRL. Über die dänische Regelung hinausgehend verpflichtete das ursprüngliche tschechische Umsetzungsgesetz sogar zur Speicherung der *URI*s, anhand derer aufgerufene Internetressourcen im Hinblick auf deren Art (Datei, Textseite, Bild, Programm) und deren Speicherort eindeutig identifiziert werden können.[206] In England fanden im Innenministerium Überlegungen zur Einbeziehung sozialer Netzwerke (insbe-

---

Verfassungsgerichtshofs vom 7. Oktober 2009, im Internet abrufbar unter der URL http://www.ccr.ro/decisions/pdf/ro/2009/D1258_09.pdf; Urteil des tschechischen Verfassungsgerichts vom 31. März 2011, im Internet abrufbar unter der URL http://www.concourt.cz/clanek/GetFile?id=5075; Urteil des Zypriotischen Verfassungsgerichts vom 1. Februar 2011, im Internet abrufbar unter der URL http://www.supremecourt.gov.cy/Judicial/SC.nsf/All/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf;

[200] Das bulgarische Gesetz ist im Internet abrufbar unter der URL http://lex.bg/laws/ldoc/2135553187.

[201] Vgl. Europäische Kommission, Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung, S. 6; Wimmer Andersson/Buchinger u.a.: Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung, S. 22 ff.

[202] Soweit Informationen zur Umsetzung in Belgien zur Verfügung standen, wurden diese in die folgende Betrachtung mit einbezogen.

[203] Keine Konkretisierung der zu speichernden Internet- und Telefoniedaten, vgl. Europäische Kommission, Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung, S. 6.

[204] In Belgien fehlt eine rechtliche Konkretisierung der zu speichernden Internet- und Telefoniedaten, vgl. Europäische Kommission, Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung, S. 15 f.

[205] Vgl. Szuba: Vorratsdatenspeicherung, S. 266; Wimmer Andersson/Buchinger u.a.: Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung, S. 12; Forgó/Jlussi/Klügel/Krügel: Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung, in: DuD 10/2008, S. 682 sowie den Artikel „Dänische Provider sollen Telefon- und Internetdaten ein Jahr speichern", in: heise.de, im Internet abrufbar unter der URL http://www.heise.de/newsticker/meldung/Daenische-Provider-sollen-Telefon-und-Internetdaten-ein-Jahr-speichern-143546.html.

[206] Vgl. Wimmer Andersson/Buchinger u.a.: Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung, S. 12 und 91 sowie Artikel-29-Datenschutzgruppe: Bericht 01/2010, Anhang, Tabelle 2, Zeile 4.

sondere *Facebook*) in die Vorratsdatenspeicherung statt, wurden jedoch bisher rechtlich nicht umgesetzt.[207]

Auch in der Praxis der Vorratsdatenspeicherung finden sich Beispiele für punktuelle Verstöße gegen das Verbot der Speicherung von Inhaltsdaten. So speicherte z.B. in Lettland ein Internetzugangsanbieter Inhaltsdaten von *IP*-Paketen über einen Zeitraum von einem Monat hinweg[208] und in Griechenland, Italien und Zypern speicherten Anbieter die *Header* von E-Mail-Nachrichten inklusive Betreffzeile[209]. In einem Fall wurde zudem die Inhalte von SMS-Mitteilungen über mehrere Monate auf Vorrat gespeichert und den Ermittlungsbehörden zugänglich gemacht.[210]

II. Speicherfristen

Der europarechtlich eröffnete Spielraum zur Festlegung von Speicherpflichten zwischen sechs und 24 Monaten spiegelt sich in erheblichen Abweichungen der national festgelegten Speicherfristen wider. Dies führt dazu, dass die Datenbestände in Hinblick auf Größe und Sensibilität in den unterschiedlichen Mitgliedstaaten stark variieren. So indiziert eine 24-monatige Speicherfrist z.B. die vierfache Menge an Vorratsdaten im Vergleich zu einer sechsmonatigen Speicherfrist.

Größtenteils geben die nationalen Rechtsordnungen einheitliche Speicherfristen für alle Kategorien von Daten vor. Es finden sich jedoch auch Differenzierungen, so dass teilweise für den Bereich des Internets kürzere Speicherfristen gelten.[211] In der folgenden Abbildung sind die aktuellen nationalen Höchstfristen bereichsübergreifend gegenübergestellt:

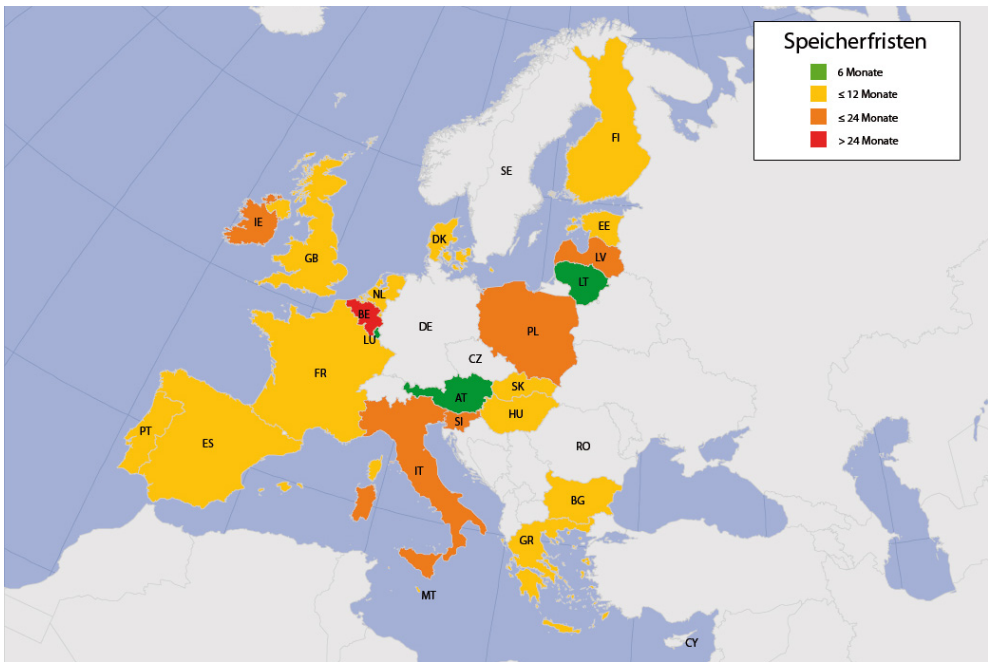


Abb. 26: Nationale Speicherfristen im Vergleich

[207] Vgl. Artikel „Briten wollen Facebook überwachen“, in: taz.de, 25.3.2009, im Internet abrufbar unter der URL http://www.taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/briten-wollen-facebook-ueberwachen/.
[208] Vgl. Artikel-29-Datenschutzgruppe: Bericht 01/2010, Anhang, Tabelle 2, Zeile 14.
[209] Vgl. Artikel-29-Datenschutzgruppe: Bericht 01/2010, Anhang, Tabelle 2, Zeilen 10,13 und 3.
[210] Vgl. Artikel-29-Datenschutzgruppe: Bericht 01/2010, S. 10.
[211] Vgl. die Darstellung der unterschiedlichen Speicherfristen in EU-Kommission: Bewertungsbericht über die Richtlinie zur Vorratsdatenspeicherung, S. 16 f.

Zudem setzen die nationalen Rechtsordnungen teilweise Möglichkeiten abgefragte Daten über einen zusätzlichen Zeitraum hinweg zu speichern. So enthält z.B. das bulgarische TKG eine Regelung, die es erlaubt abgefragte Vorratsdaten 6 Monate länger zu speichern (Art. 250a V bulgarisches TKG). In Frankreich werden abgerufene Vorratsdaten sogar weitere drei Jahre in Datenbanken des Innen- und Verteidigungsministeriums gespeichert.[212] Dies führt im Ergebnis dazu, dass die abgefragten Daten in Frankreich insgesamt über einen Zeitraum von vier Jahren gespeichert werden. Positiv fallen in diesem Kontext die Regelungen in Spanien und Estland auf: diese schließen die von Art. 7 lit. d) VDSRL eröffnete Lücke, indem sie die Ermittlungsbehörden zur Löschung von abgefragten Daten verpflichten, sobald diese nicht mehr für die konkrete Ermittlung benötigt werden. In Estland wird dem Betroffenen hierzu ein Antragsrecht eingeräumt.[213]

IV. Zugriffsschwellen

Ebenso heterogen gestalten sich die nationalen Regelungen, die die Zulässigkeitsschwelle zum Zugriff auf die Vorratsdaten normieren. Entsprechend der Vorgabe in Art. 1 I VDSRL dürfen die gespeicherten Daten nur zur Ermittlung und Verfolgung schwerer Straftaten abgerufen werden. Teilweise wird diese Regelung wortlautgetreu in die nationalen Rechtsordnungen übernommen, ohne konkret zu definieren, welche Straftaten darunter zu verstehen sind.[214] Neun Mitgliedstaaten erlauben jedoch – über die europarechtlichen Vorgaben hinausgehend – die Verwendung der Daten zum Schutz der öffentlichen Sicherheit, so dass die Vorratsdaten in diesen Ländern auch zur Verfolgung von Ordnungswidrigkeiten verwendet werden können.

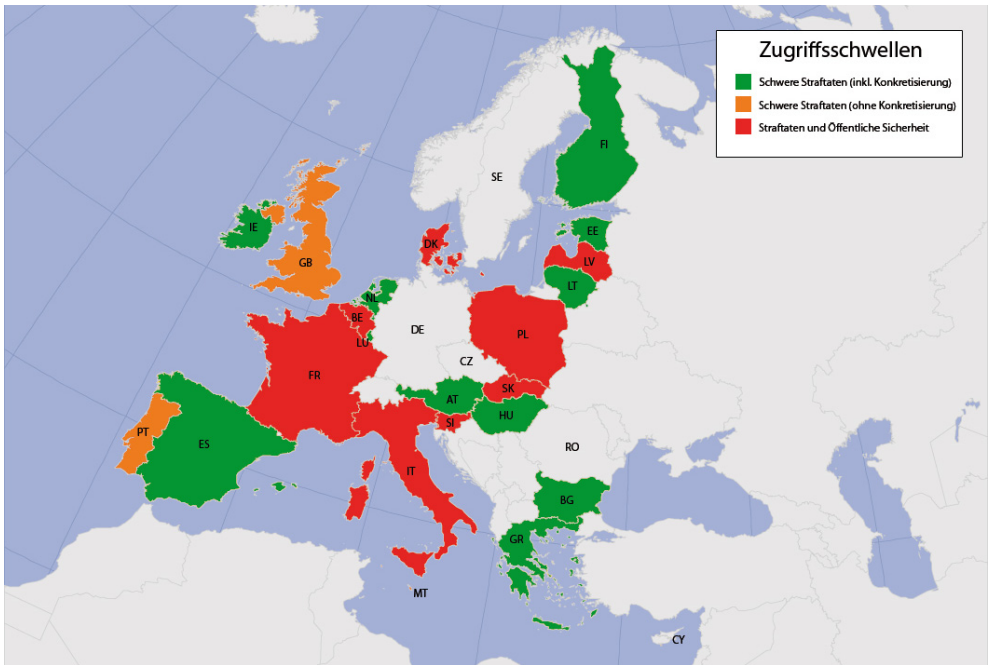


Abb. 27: Nationale Zugriffsschwellen im Vergleich

[212] Vgl. Szuba: Vorratsdatenspeicherung, S. 269.
[213] Vgl. Anhang, Abschnitt 2).
[214] Vgl. hierzu und im Folgenden EU-Kommission: Bewertungsbericht über die Richtlinie zur Vorratsdatenspeicherung, S. 7 ff.

Die Herabsetzung der Zugriffsschwelle in den rot markierten Ländern und die generalklauselartige Festlegung der Zugriffsschwelle in den orange markierten Ländern implizieren eine Vergrößerung des Kreises der Zugangsberechtigten und erhöhen das Risiko einer Verletzung des Schutzziels der Vertraulichkeit der TK-Nutzer. Vor allem in den Ländern Italien, Polen, Lettland und Belgien ist dies als sehr bedenklich einzustufen, zumal diese Länder zusätzlich eine relativ lange Speicherfrist vorgeben (vgl. Abb. 26).

V. Technische und organisatorische Sicherheitsvorkehrungen

1. Rechtliche Betrachtung

Die gesetzlichen Vorgaben in Bezug auf technische und organisatorische Sicherheitsvorkehrungen innerhalb der nationalen Rechtsordnungen verteilen sich zumeist – in Analogie zum Europarecht – auf mehrere unterschiedliche Rechtsakte. Dies erschwert die Identifizierung der entsprechenden Normen.[215] Da die in der VDSRL normierten Vorgaben in Bezug auf die Sicherheit der Vorratsdaten nicht über die schon seit 1998 umzusetzenden Vorgaben der DSRL hinausgehen (bis auf die Verpflichtung zur Vernichtung der Daten am Ende der Speicherpflicht aus Art. 7 lit. d) VDSRL), wird im Rahmen der folgenden rechtlichen Betrachtung versucht, zusätzliche, über die europäischen Vorgaben hinausgehenden Anforderungen in den Rechtsordnungen der Mitgliedstaaten zu identifizieren.[216]

Bulgarien, England, Irland und die Slowakei haben Art. 7 VDSRL wortlautgetreu in ihre Rechtsordnung übernommen. In nahezu allen untersuchten Rechtsordnungen werden – entsprechend Art. 7 lit. b) VDSRL, Art. 4 Ia Sstr. 2 EDSRL und Art. 17 I DSRL – generalklauselartig geeignete technische Maßnahmen zum Schutz unterschiedlicher Bedrohungsszenarien (Verlust, Zerstörung, unbefugte Veränderung, unrechtmäßige Zugänglichmachung und Verbreitung, etc.) gefordert. Diese sind wie im Europarecht teilweise mehrfach gesetzlich verankert. Bei großzügiger Auslegung dieser Generalklauseln sind damit alle zu berücksichtigenden Schutzziele (vgl. Kapitel C. I.) europaweit rechtlich adressiert. Teilweise unterscheiden sich die Generalklauseln in kleinen Nuancen. So wird z.B. in Luxemburg und Ungarn explizit auch der Schutz der Daten bei deren Übermittlung über ein Netzwerk angesprochen.[217] Die erforderliche Höhe des Schutzniveaus wird in Analogie zu den europarechtlichen Vorgaben zumeist von folgenden Faktoren abhängig gemacht: dem Stand der Technik, den Kosten der Sicherheitsmaßnahmen und der Natur und Art der Verarbeitung der gespeicherten Daten sowie dem daraus resultierenden Risiko einer Sicherheitsverletzung. Länderübergreifend wird das größte Gewicht auf das Schutzziel der Vertraulichkeit gelegt. Diesbezüglich herrscht europaweit die größte Regelungsdichte. Dies ist vor dem Hintergrund, dass dieses das einzige Schutzziel ist, dass sich auf Grundrechtspositionen stützen lässt, zu deren Schutz die entsprechenden Datenschutzgesetze gerade erlassen worden sind, auch nicht verwunderlich.

Im Hinblick auf darüber hinausgehende, die weiteren Schutzziele adressierende Vorgaben unterscheiden sich die einfachgesetzlichen Regelungen in den Mitgliedstaaten stark. Hieraus darf jedoch nicht auf divergierende rechtliche Schutzniveaus geschlossen werden, zumal der Großteil der sicherheits-

[215] Dementsprechend können die nachfolgenden Ausführungen keinen Anspruch auf Vollständigkeit erfüllen.
[216] Vgl. hierzu und im Folgenden Abschnitte 2) und 3) im Anhang.
[217] Der Schutz personenbezogener Daten bei der Übermittlung ist auch durch die Generalklauseln der übrigen Mitgliedstaaten gedeckt, die die Übermittlung nicht explizit ansprechen. Ansonsten wäre der Schutz vor dem Hintergrund zunehmender Vernetzung zu lückenhaft.

technischen Regelungen meist erst auf Verwaltungsebene konkretisiert wird.[218] Dementsprechend finden sich in den meisten Umsetzungsgesetzen Ermächtigungen an Exekutivorgane zum Erlass konkretisierender Verwaltungsvorschriften. Teilweise werden jedoch auch auf Ebene des einfachen Gesetzes detaillierte technische Vorgaben gemacht. Sofern dies gelingt, ist dies als positiv zu werten, weil nur so der demokratisch legitimierte Gesetzgeber eine größere Kontrolle über die tatsächliche Umsetzung der Vorgaben hat und diese nicht an Verwaltungsorgane abgibt. Es muss jedoch auch berücksichtigt werden, dass sich technische Vorgaben aufgrund deren Schnelllebigkeit oft nicht zur Implementierung in Gesetzestexte eignen und aufgrund des größeren Sachverstands oftmals besser durch entsprechende Fachleute in Ministerien zu konkretisieren sind als durch den Gesetzgeber.

Aus sicherheitstechnischer Sicht über die europäischen Vorgaben hinausgehend und dementsprechend positiv gestalten sich die rechtlichen Vorgaben in Italien, Luxemburg und Österreich.[219]

Italien regelt detaillierte sicherheitstechnische und organisatorische Minimalanforderungen in *Annex B* zum italienischen Datenschutzgesetz. Das Gesetz inklusive Annex verpflichtet die TK-Diensteanbieter und Netzbetreiber z.B. zur Verwendung wissensbasierter, hardwarebasierter oder biometrischer Authentifizierungs- und Autorisierungsmechanismen, die eine eindeutige Identifizierung des Zugriffsberechtigten ermöglicht. Sofern Passwörter verwendet werden, müssen diese mindestens acht Zeichen lang sein und in einem 3-Monats-Zyklus geändert werden. Backups der Daten sind in wöchentlichen Zyklen anzufertigen. Um ein ausreichendes Sicherheitsniveau zu gewährleisten fordert das italienische Recht zudem die periodische Überprüfung der betriebenen Sicherheitspolitik und dessen dokumentarische Niederschrift. So müssen z.B. in jährlichem Turnus die Zugriffsberechtigungen der Mitarbeiter überprüft und auf das erforderliche Maß für deren Tätigkeiten beschränkt werden. Die verwendete Sicherheitssoftware muss mindestens alle sechs Monate aktualisiert werden. Eine Verschlüsselung[220] der Vorratsdaten und eine Trennung der Daten wird jedoch nicht explizit gefordert.

Die einfachgesetzlichen Regelungen in Luxemburg gestalten sich noch ausdifferenzierter.[221] Insbesondere zum Schutz der Vertraulichkeit der Daten schreibt das luxemburgische Datenschutzgesetz physische Zutrittskontrollen, sowie den Schutz von Datenträgern und IT-Systemen vor unberechtigten Personen und unbefugtem Gebrauch vor. Dazu kommen logische Sicherheitsmaßnahmen, die den Zugriff auf die Daten auf speziell autorisierte Personen beschränken. Zudem sind alle Datenzugriffe zu protokollieren, so dass die zugreifende Person im Nachhinein identifiziert werden kann. Zum Schutz der Verfügbarkeit sind die Daten vor unbefugter Löschung zu schützen und Backups zu erstellen. Vorrangig zum Schutz der Integrität sind zudem entsprechende Schutzmechanismen zur Verhinderung einer unbefugten Eingabe von Daten in das Informationssystem zu treffen. Auch der Schutz der Daten bei der Übermittlung ist explizit angesprochen. Hierbei sind insbesondere Identifikations- und Authentifizierungsmechanismen sowie Sicherheitsmaßnahmen zum Schutz vor Veränderung auf dem Übermittlungsweg erforderlich. Die konkrete Ausgestaltung dieser Vorgaben wird der nationalen Datenschutzbehörde überlassen, die Empfehlungen über *Best Practices* abgibt.

---

[218] Im Rahmen der vorliegenden Untersuchung wurde hauptsächlich die Umsetzung auf einfacher Gesetzesebene untersucht. Konkretisierende Verordnungen, Verwaltungsakte, etc. konnten größtenteils nicht recherchiert werden.

[219] In Italien werden technische Vorschriften im Anhang zum Gesetz geregelt und waren dementsprechend gut recherchierbar.

[220] Diese wird in italienischem Recht nur für die Verarbeitung von Gesundheitsdaten vorgeschrieben, vgl. Abschnitt 34 Nr. 1 lit. h) des italienischen Datenschutzgesetzes (im Anhang unter Abschnitt 3).

[221] Vgl. vor allem Art. 23 des luxemburgischen Datenschutzgesetzes.

Die detailliertesten gesetzlichen Anforderungen bezüglich der technischen und organisatorischen Sicherheitsmaßnahmen zum Schutz der Vorratsdaten finden sich im österreichischen Recht. Zur Gewährleistung der Vertraulichkeit der Daten verpflichtet das österreichische Datenschutzgesetz die Telekommunikationsunternehmen samt Mitarbeiter zur Geheimhaltung und Übermittlung der Daten nur auf ausdrückliche Anordnung des Arbeitgebers hin. Gefordert wird eine klare Aufgabenverteilung und Regelung von Zutritts- und Zugriffsberechtigungen. Es müssen geeignete Vorkehrungen getroffen werden, um die Unterscheidung der Vorratsdaten von anderen Daten zu ermöglichen (physikalische oder logische Trennung). Der Zugriff auf die Vorratsdaten ist nur ausschließlich hierzu ermächtigten Personen unter Einhaltung des *4-Augen-Prinzips* erlaubt. Zur Gewährleistung der Verfügbarkeit verpflichten § 99 I und § 102b II des österreichischen TKG die TK-Diensteanbieter, die zur Auskunft über Vorratsdaten erforderlichen Einrichtungen bereitzustellen und die Daten so abzuspeichern, dass Anfragen unverzüglich beantwortet werden können. Die Übermittlung der Daten an die Ermittlungsbehörden hat in CSV-Format unter Verwendung einer technisch anspruchsvollen Verschlüsselung zu erfolgen. Zudem sind entsprechende Übertragungstechnologien zu verwenden, die sowohl die Datenintegrität als auch die Authentizität von Sender und Empfänger sicherstellen. Alle Operationen (Änderung, Abfrage, Übermittlung) in Bezug auf die Vorratsdaten sind zudem zu protokollieren und die Protokolldaten drei Jahre lang aufzubewahren. Bei der Verankerung dieser Vorgaben hat sich der österreichische Gesetzgeber stark an den Vorgaben der *Artikel-29-Datenschutzgruppe* orientiert (vgl. Kapitel D. II. 1. a).

2. Praktische Betrachtung

Im Folgenden werden die Ergebnisse einer europaweiten Erhebung von Sicherheitsmaßnahmen der *Artikel-29-Datenschutzgruppe* dargestellt.[222] Diese führte im Jahr 2009 in Zusammenarbeit mit den nationalen Datenschutzbehörden europaweit Befragungen und Inspektionen vor Ort bei den wichtigsten Telekommunikationsbetreibern und Diensteanbietern durch, um einen Überblick über die getroffenen technischen und organisatorischen Sicherheitsmaßnahmen zum Schutz der Vorratsdaten zu erlangen. Im Gegensatz zu den gesetzlichen Vorgaben, die europaweit als relativ homogen anzusehen sind (vgl. Abschnitt 1.), offenbarte die Untersuchung ein „Flickwerk an Durchführungsmaßnahmen“[223]. Während größere Betreiber, insbesondere die Marktführer, aufgrund von Skalenvorteilen umfangreiche Spitzen-IT-Sicherheitslösungen einsetzen können, bestimmen bei kleineren Anbietern vor allem Kostenminimierungsstrategien die Ausgestaltung der Sicherheitsmaßnahmen. Die IT-Sicherheit wird laut der Befragung in den Unternehmen größtenteils als innerbetriebliche Aufgabe angesehen, so dass nur 45 % der befragten Anbieter von TK-Dienstleistungen auf externe Audits und Sicherheitszertifizierungen durch unparteiische Dritte setzten.[224] Ebenso wurden Penetrationstests und Risikoanalysen nur bei einem Teil der untersuchten Unternehmen durchgeführt. Die folgenden Abschnitte zeigen – nach den einzelnen Mitgliedstaaten differenzierend – den Stand der Implementierung konkreter Sicherheitsmaßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Vorratsdaten. Hierbei werden einzelne Sicherheitsmaßnahmen exemplarisch herausgegriffen.

---

[222] Artikel-29-Datenschutzgruppe, Bericht 01/2010, im Internet abrufbar unter der URL http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_de.pdf; die erhobenen Daten sind im Anhang in Abschnitt 4 enthalten.
[223] Artikel-29-Datenschutzgruppe: Bericht 01/2010, S. 9.
[224] Artikel-29-Datenschutzgruppe: Bericht 01/2010, S. 14.

b) Maßnahmen zum Schutz der Vertraulichkeit und Integrität

Recht einheitlich gestaltet sich das Bild der physischen Sicherheitsmaßnahmen zum Schutz der Vertraulichkeit der Vorratsdaten. So erfolgt zumeist eine kontinuierliche Überwachung der EDV-Systeme und Gebäudekomplexe durch Videoüberwachungsanlagen, ein spezialisiertes Überwachungspersonal und Zugriffskontrollsysteme.[225] Wie wirksam die konkreten Maßnahmen bei den jeweiligen Unternehmen sind, kann aus den Daten des Untersuchungsberichts nicht entnommen werden.[226]

Im Hinblick auf die logischen Sicherheitsmaßnahmen zeigen sich – mit Ausnahme von logischen Authentifizierungsmechanismen mittels Benutzername und Passwort, die in jedem der untersuchten Unternehmen implementiert waren – größere Abweichungen. Teilweise werden die für Ermittlungszwecke bereitgehaltenen Vorratsdaten nicht (physisch oder) logisch von anderen Daten wie z.B. Verkehrsdaten, die zu Rechnungszwecken verwendet werden, getrennt. Ohne eine zumindest logische Trennung der Daten ist eine effektive Beschränkung des Zugriffs auf die Vorratsdaten auf einen kleinen Kreis von speziell berechtigtem Personal jedoch nicht realisierbar. Vor allem in den Ländern Irland, Finnland, Polen und Griechenland (aber auch den orange eingefärbten Ländern) ist dementsprechend von negativen Implikationen auf die Vertraulichkeit der Vorratsdaten auszugehen.

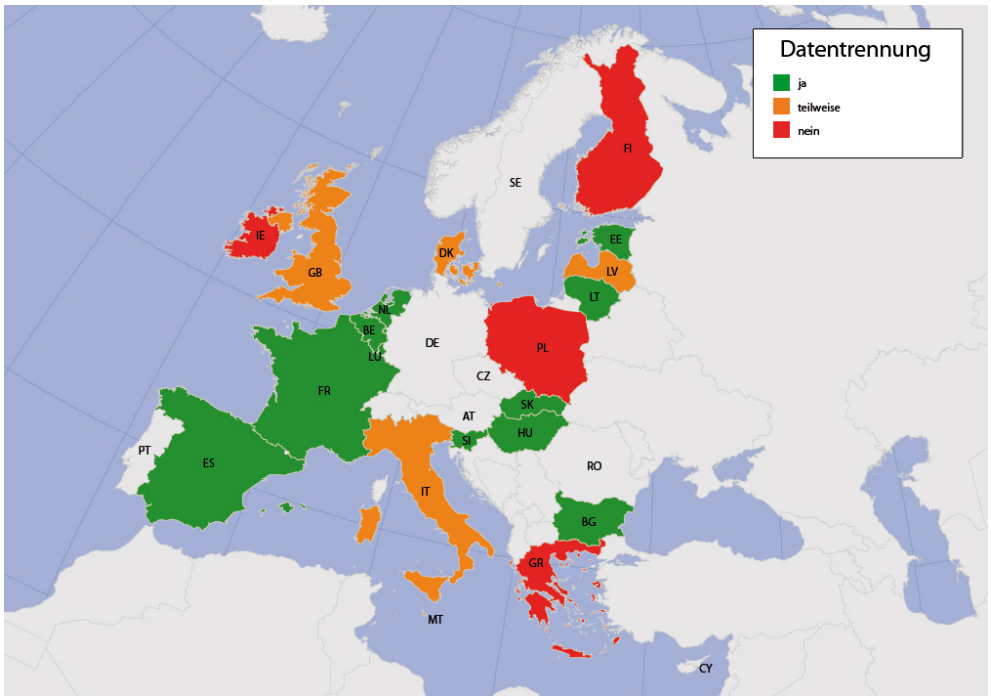


Abb. 28: Praktizierte Datentrennung im Vergleich

Auch im Hinblick auf die Verwendung von Verschlüsselungsverfahren zur Absicherung der Vorratsdaten gegen unerlaubte Zugriffe zeigten sich im Rahmen der Untersuchung Unterschiede. Größtenteils werden die Vorratsdaten nur bei elektronischer Übermittlung zu den Ermittlungsbehörden verschlüsselt. Nur in Luxemburg und Malta fanden sich Telekommunikationsanbieter, die die Vorratsdaten

[225] Artikel-29-Datenschutzgruppe: Bericht 01/2010, S. 13.
[226] Der Arbeitskreis-Vorratsdatenspeicherung bezweifelt die Wirksamkeit einer Vielzahl der von den Unternehmen eingesetzten physischen Sicherheitsmaßnahmen und hat dies anhand mehrerer erfolgreicher Versuche, diese zu überwinden, aufgezeigt, vgl. hierzu das Infoheft des AK-Vorratsdatenspeicherung „Es gibt keine sicheren Daten“, im Internet abrufbar unter der URL http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten.pdf.

komplett verschlüsselt in ihren IT-Systemen aufbewahren. Die fehlende Verschlüsselung der gespeicherten Vorratsdaten führt jedoch nicht zwangsläufig zu Einschränkungen der Vertraulichkeit. So können die Daten auch unverschlüsselt z.B. durch robuste Authentifizierungs- und Autorisierungsmechanismen ausreichend geschützt werden. Die Verschlüsselung ist angesichts der Sensibilität der Vorratsdaten aber trotzdem zu empfehlen, da diese ein zusätzliches Hindernis gegen unbefugte Kenntnisnahme darstellt. Unbedingt erforderlich ist die Verschlüsselung der Daten auf dem Übertragungsweg von den TK-Diensteanbietern zu den Ermittlungsbehörden, sofern diese über öffentlich zugängliche Telekommunikationsnetze erfolgt. In Belgien werden die Vorratsdaten dementsprechend nur per Brief und Fax an die Ermittlungsbehörden übermittelt.[227]

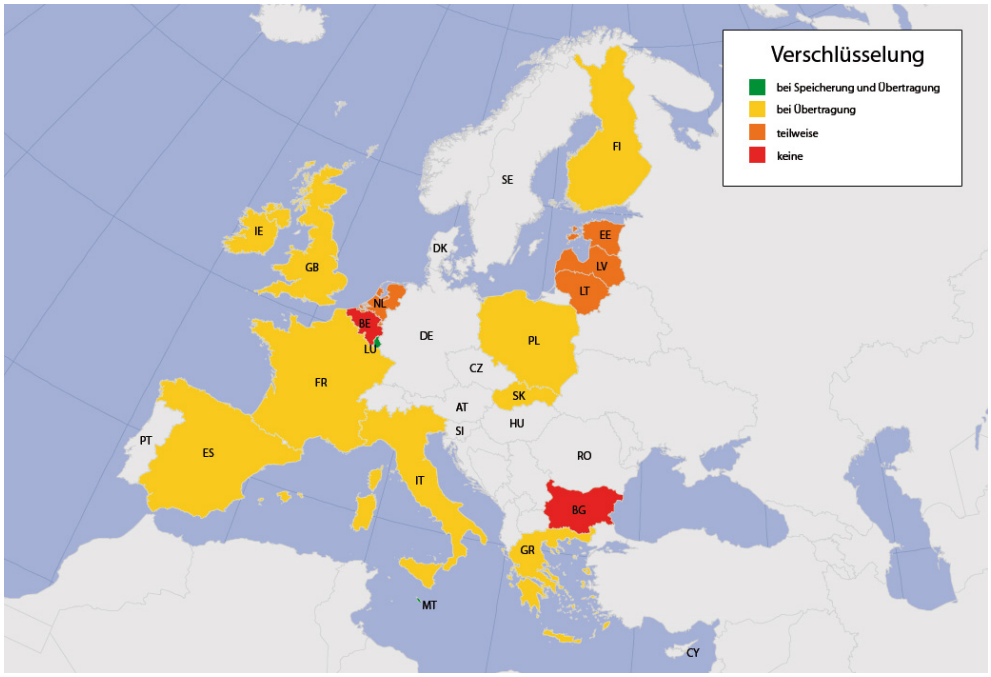


Abb. 29: Praktizierte Verschlüsselung der Vorratsdaten im Vergleich

Eine Protokollierung der Zugriffe auf die Vorratsdaten fand in nahezu allen untersuchten TK-Unternehmen statt. Die Untersuchung deckte jedoch auch Unternehmen in Dänemark, Estland, Finnland, Lettland, der Slowakei und Griechenland auf, die Zugriffe auf die Vorratsdaten nicht protokollierten. Zudem waren manche Systemadministratoren von der Protokollierung ausgeschlossen.[228]

[227] Zur Art der Übermittlung in Bulgarien finden sich in dem Bericht der Artikel-29-Arbeitsgruppe keine Informationen.
[228] Artikel-29-Datenschutzgruppe: Bericht 01/2010, S. 15 f.

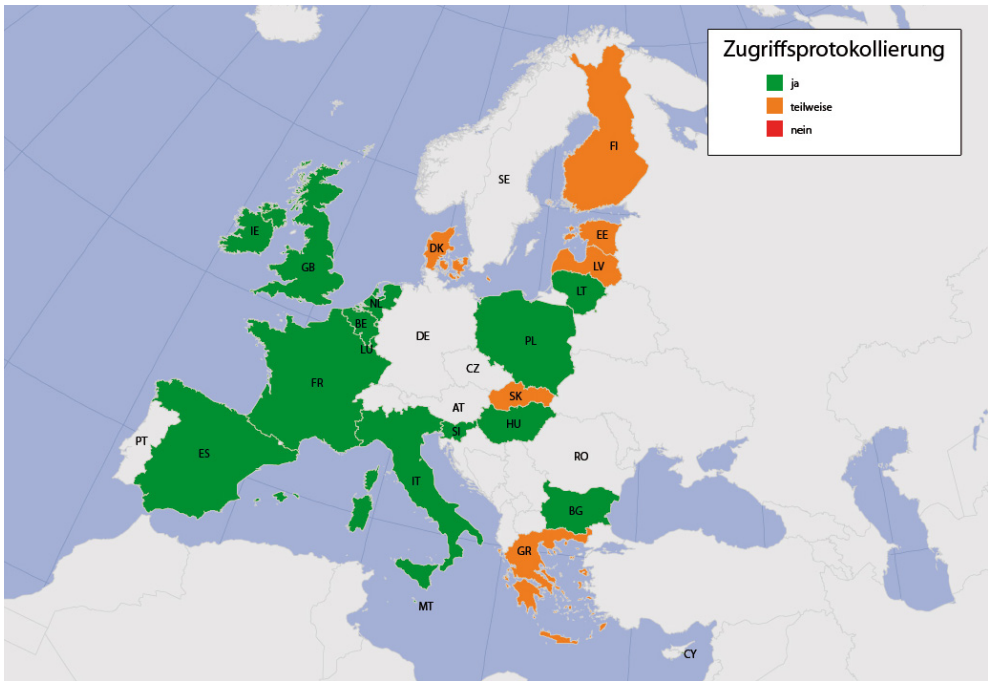


Abb. 30: Protokollierung des Zugriffs auf die Vorratsdaten im Vergleich

Welche Nutzeraktionen konkret protokolliert wurden, und wie die Protokolldaten aufbewahrt wurden lässt sich dem Bericht nicht entnehmen.

c) Maßnahmen zum Schutz der Verfügbarkeit

BackUp- und *Disaster Recovery*-Systeme zum Schutz der Verfügbarkeit der Vorratsdaten waren in nahezu allen untersuchten Unternehmen vorhanden. Lediglich kleinere Unternehmen in Lettland und Malta verfügten über keine *Backup*-Lösungen.

d) Konkrete Ausgestaltung des Übermittlungsverfahrens

Die praktische Ausgestaltung der Übermittlung der Daten an die Ermittlungsbehörden war zum Zeitpunkt der Untersuchung durch eine große Bandbreite an unterschiedlichen Lösungen geprägt.[229] Die praktizierten Übermittlungsmethoden reichen von handgeschriebenen Dokumenten, CDs, DVDs und USB-Sticks die in teils versiegelten Umschlägen mittels Kurierdienst oder Standardpostsendung übersandt werden, über Kommunikation per Fax oder unverschlüsselter E-Mail bis hin zur Verwendung verschlüsselungsgeschützter Übertragungskanäle (*PGP*, *HTTPS* und *SSL*, Authentifizierung mit öffentlichen Schlüsseln).[230] Vor allem bei der Versendung der Daten mittels unverschlüsselter E-Mail-Nachrichten besteht ein nicht kalkulierbares Risiko, dass die Daten auf dem Übertragungsweg ausgelesen oder vielleicht sogar mittels *Man-in-the-Middle*-Angriffen verändert werden. Dementsprechend birgt diese Methode ein nicht zu vernachlässigendes Potential zur Gefährdung der Schutzziele der Vertraulichkeit und Integrität der Vorratsdaten sowie der Authentizität der Kommunikationspartner bei der Übermittlung der Vorratsdaten.

[229] Vgl. Artikel-29-Datenschutzgruppe: Bericht 01/2010, S. 17 ff.
[230] Vgl. Artikel-29-Datenschutzgruppe: Bericht 01/2010, Anhang, Tabelle 3.

VII. Fazit

Angesichts der vorausgehenden Betrachtung kann nicht von einem europaweit ausreichenden Sicherheitsniveau zum Schutz der Vorratsdaten ausgegangen werden. Sowohl die rechtliche Ausgestaltung der Rahmenbedingungen und der expliziten sicherheitstechnischen Vorgaben, als auch die in der Praxis verwendeten Sicherheitsmaßnahmen beherbergen eine Vielzahl negativer Implikationen auf die zu verfolgenden Schutzziele. Vor allem das Schutzziel der Vertraulichkeit ist einem kaum kalkulierbaren Bedrohungsszenario ausgesetzt. In den Mitgliedstaaten Belgien, Italien, Polen und Lettland wird die Schutzbedürftigkeit der Vorratsdaten durch die Herabsetzung der Zugriffsschwelle, verbunden mit der Festsetzung einer langen Speicherfrist noch weiter verstärkt. Zudem bestehen teilweise Möglichkeiten, bereits abgerufene Vorratsdaten über einen längeren Zeitraum hinweg zu speichern. Auch diese Daten müssen ausreichend abgesichert werden.

Die rechtlichen Vorgaben zur sicherheitstechnischen Absicherung der Vorratsdaten in den einzelnen Mitgliedstaaten orientieren sich stark an den europarechtlichen Vorgaben. So finden sich die europarechtlichen Generalklauseln – in vielen Fällen wortwörtlich übernommen – in allen nationalen Rechtsordnungen in vielfältiger Ausfertigung wieder. Abstrakt sind damit alle Schutzziele europaweit abgedeckt, jedoch stets unter Berücksichtigung der Kosten der entsprechenden Sicherheitsmaßnahmen. Regeln zur Gewichtung der einzelnen Faktoren finden sich auch in den nationalen Rechtsordnungen nicht. Dementsprechend positiv zu werten sind vor allem die gesetzlichen Regelungen in Österreich, die – über die europäischen Vorgaben hinausgehend – konkrete Sicherheitsmaßnahmen formulieren, welche speziell auf die Vorratsdaten zugeschnitten sind (Einhaltung des 4-Augen-Prinzips, Datentrennung, etc.).

Auch wenn bisher noch kein Fall bekannt wurde, in dem Vorratsdaten entwendet wurden, lässt der bisherige Umgang mit den gespeicherten Vorratsdaten in der Praxis bezweifeln, dass deren Vertraulichkeit ausreichend gewährleistet wird. So trennt ein nicht zu vernachlässigender Teil der Telekommunikationsanbieter die Vorratsdaten nicht von den sonstigen im Geschäftsbetrieb verarbeiteten Daten und eine Verschlüsselung der gespeicherten Daten findet wenn dann nur auf dem Übertragungsweg statt. Teilweise werden die Daten jedoch auch unverschlüsselt per E-Mail an die Ermittlungsbehörden übertragen. In diesem Fall sind die übertragenen Daten einem *Man-in-the-middle*-Angriff schutzlos ausgeliefert. Ferner beherbergt die große Bandbreite an unterschiedlichen Übermittlungstechniken ein nicht zu vernachlässigendes Sicherheitsrisiko für die übermittelten Daten. Dementsprechend sollte in den verschiedenen Mitgliedstaaten, soweit dies noch nicht geschehen ist, ein standardisiertes Übermittlungsverfahren nach den Vorgaben der *Technischen Spezifikation 102 657 V1.7.1 (2010-10)* des *ETSI* (vgl. Kapitel D. II. 2. b) vorgeschrieben werden.

F. Die Umsetzung in der Bundesrepublik Deutschland

Im Folgenden verengt sich die Betrachtung auf die rechtliche und praktische Geschichte der Vorratsdatenspeicherung in der Bundesrepublik Deutschland. Betrachtungsgegenstand sind zunächst die rechtlichen sicherheitstechnischen Vorgaben, die die Telekommunikationsanbieter im Rahmen der Speicherung der Vorratsdaten in Deutschland zu beachten hatten. Anschließend erfolgt eine Darstellung der sicherheitstechnischen Aspekte des Urteils des Bundesverfassungsgerichts. Dieses hat die Vorratsdatenspeicherung unter anderem aufgrund mangelhafter gesetzlicher sicherheitstechnischer Vorgaben für nichtig erklärt. Um festzustellen, ob sich diese in der praktischen Absicherung der Vorratsdaten bei den Telekommunikationsunternehmen in Deutschland widerspiegelten, folgt anschließend die Untersuchung der implementierten Sicherheitsmaßnahmen bei drei in Deutschland und insbesondere in Bayern tätigen Telekommunikationsanbietern.

I. Die rechtliche Umsetzung der Vorratsdatenspeicherung in Deutschland

Nachdem der Deutsche Bundestag am 9. November 2007 mit 366 Ja-Stimmen für die Einführung der Vorratsdatenspeicherung in Deutschland gestimmt hatte, trat das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ nach dessen Verkündung im Bundesgesetzblatt am 1.1.2008 in Kraft.[231] Es verpflichtete Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer[232], die in § 113a II TKG aufgeführten Daten über einen Zeitraum von sechs Monaten zu speichern.

Neben Anbietern von Telefonie-, Internetzugangs-, E-Mail- und *VoIP*-Diensten verpflichtete § 113a VI TKG auch Anbieter von Anonymisierungsdiensten zur Speicherung der erforderlichen Daten, um die Identität der Nutzer derartiger Dienste im Nachhinein aufdecken zu können.[233] Nicht zur Speicherung verpflichtet waren Anbieter nicht-öffentlich zugänglicher Kommunikationsdienste wie z.B. Universitäten, die ihren Studierenden E-Mail-Dienste anbieten oder Unternehmen, die ihren Mitarbeitern ein unternehmensinternes Netz zur Verfügung stellen.[234]

Die zu speichernden Datentypen entsprachen den europarechtlichen Vorgaben (vgl. Kapitel D. I. 1.).[235] Im Bereich des E-Mail-Verkehrs waren Verkehrsdaten sowohl beim Ein- und Ausgang von E-Mails in elektronischen Postfächern, als auch beim Zugriff auf diese Postfächer jeweils mit *IP*-Adresse des verbundenen Teilnehmers zu speichern.[236] Die Speicherung von Inhaltsdaten und aufgerufene Internetseiten war explizit verboten (§ 113a VIII TKG).

---

[231] Vgl. BGBl. 2007 I, S. 3198, im Internet abrufbar unter der URL http://www.bgbl.de/Xaver/text.xav?bk=Bundesanzeiger_BGBl&start=%2F%2F*[%40attr_id%3D%27bgbl107s3307.pdf%27]&wc=1&skin=WC.

[232] Dementsprechend waren sog. Verbindungsnetzbetreiber in Deutschland nicht zur Vorratsdatenspeicherung verpflichtet.

[233] Vgl. Graf: Beck’scher Online-Kommentar StPO, § 113a TKG, Rn. 29; BT-Drucksache 16/5846, S. 71 f.

[234] Vgl. Wettern: Umsetzung der Vorratsdatenspeicherung an den Hochschulen, in: DuD 2009, S. 345.

[235] Die entsprechenden Datentypen wurden in Art. 5 II TKG für jeden einzelnen Bereich (Telefondienste, elektronische Post, Internetzugangsdienste) explizit benannt.

[236] Diesbezüglich weicht die Umsetzung im TKG von der Auslegung der VDSRL in Kapitel D. I. 1. d) ab.

1. Einfachgesetzliche Sicherheitstechnische Vorgaben

Vorgaben im Hinblick auf technische und organisatorische Sicherheitsmaßnahmen zum Schutz der Vorratsdaten finden sich im Telekommunikationsgesetz und im Datenschutzgesetz, wobei der Großteil der Vorschriften auf die EDSRL und die DSRL zurückgehen und dementsprechend schon vor der Vorratsdatenspeicherung existierten. Im Rahmen der Einführung der VDS wurden nur wenige zusätzliche Anforderungen gesetzlich implementiert.[237] Im Folgenden werden die rechtlichen Vorgaben, die die technische und organisatorische Ausgestaltung der Sicherheitsmaßnahmen zum Schutz der Vorratsdaten bei den TK-Diensteanbietern bestimmten, dargestellt und den einzelnen Schutzzielen zugeordnet (siehe Tabelle 10)

a) Vorgaben aus dem TKG

Speziell sich auf die Vorratsdaten beziehende Sicherheitsvorgaben fanden sich in § 113a TKG. In § 113 X TKG verpflichtete der Gesetzgeber die TK-Diensteanbieter, „betreffend die Qualität und den Schutz der gespeicherten Verkehrsdaten die im Bereich der Telekommunikation erforderliche Sorgfalt zu beachten“. Diese Generalklausel beschränkt sich nicht auf bestimmte Bedrohungsszenarien, sondern adressiert ganz allgemein alle zu berücksichtigenden Schutzziele. Insbesondere erfordert § 113a X TKG, wie auch Art. 7 lit. c) VDSRL die Beschränkung des Zugangs zu den Daten auf ausschließlich hierzu besonders ermächtigte Personen. Die Löschung der Vorratsdaten musste spätestens einen Monat nach Ablauf der Speicherfrist erfolgen, wodurch sich die faktische Speicherdauer auf sieben Monate verlängern konnte. Um die Verfügbarkeit der Daten zu gewährleisten, mussten die TK-Diensteanbieter die Daten so speichern, dass ein effektives und schnelles Retrieval möglich war und diese unverzüglich an die zuständigen Behörden weitergeleitet werden konnten.[238]

In Analogie zum Europarecht hebt auch das TKG den Schutz der Vertraulichkeit besonders hervor. Alle Anbieter von TK-Diensten (Netzbetreiber, virtuelle Netzbetreiber, Service-Provider und Reseller) sind dementsprechend gem. § 109 I TKG verpflichtet, angemessene technische Vorkehrungen oder sonstige Maßnahmen zu treffen, um das in § 88 TKG verbürgte Fernmeldegeheimnis und den Schutz personenbezogener Daten und der zugehörigen Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu gewährleisten. Bei der physischen und logischen Implementierung von entsprechenden Schutzmechanismen sind der Stand der technischen Entwicklung, der wirtschaftliche Aufwand und die Bedeutung der zu schützenden Einrichtungen zu berücksichtigen. Explizit die Netzbetreiber sind gem. § 109 III TKG zusätzlich zu einer Vielzahl organisatorischer Maßnahmen verpflichtet. Diese müssen einen Datenschutzbeauftragten benennen und ein Sicherheitskonzept[239] erstellen, das die eingesetzten Kommunikationsanlagen, potentielle Gefährdungen und technische Vorkehrungen oder sonstige Schutzmaßnahmen zur Begegnung von Gefährdungen beschreibt. Das Sicherheitskonzept ist der BNetzA vorzulegen und einer ständigen Anpassungs- und Aktualisierungspflicht unterworfen.

---

[237] Dies sind die Anforderungen, die sich aus § 113a TKG ergeben.
[238] Vgl. Graf: Beck’scher Online-Kommentar StPO, § 113a TKG, Rn. 12.
[239] Siehe hierzu BNetzA: Leitfaden zur Erstellung eines Sicherheitskonzeptes gemäß § 109 III TKG, im Internet abrufbar unter der URL
http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Bundesnetzagentur/AmtsblattPublikationen/DruckschriftenAllgemein/SicherheitTelekommunikation/LeitfadenSicherheitskonzeptId4552pdf.pdf?__blob=publicationFile.

b) Vorgaben aus dem BDSG

§ 5 BDSG statuiert das allgemeine Datengeheimnis. Dieses richtet sich direkt an die mit der Verarbeitung personenbezogener Daten beschäftigten Personen und verpflichtet diese, Daten nicht unbefugt zu erheben, zu verarbeiten oder zu nutzen. Konkret bedeutet dies im Rahmen der Vorratsdatenspeicherung zum Beispiel, dass Mitarbeiter ihre intern zugewiesenen Zugriffsberechtigungen nicht überschreiten dürfen[240] und, soweit diese im Rahmen ihrer Tätigkeiten Kenntnis von Vorratsdaten erhalten, auch nach Beendigung der Tätigkeit zur Geheimhaltung verpflichtet sind. Hiermit wird versucht, der Gefahr von Vertraulichkeitsverletzungen durch mit der Verarbeitung von personenbezogenen Daten beschäftigten Personen zu minimieren.

§ 9 BDSG verpflichtet alle Stellen, die personenbezogene Daten erheben oder verarbeiten, geeignete technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Datenschutzgesetzes zu gewährleisten. § 9 BDSG ist dementsprechend als zentrale Schaltnorm zwischen Datenschutz und Datensicherheit anzusehen. Sie fordert spiegelbildlich zu den vom Gesetzgeber im BDSG vorgegebenen Zielen die Ergreifung technischer und organisatorischer Maßnahmen. Eine Aufzählung von bestimmten Bedrohungsszenarien erfolgt in § 9 BDSG im Gegensatz zu seinem europäischen Pendant, Art. 17 DSRL nicht. Dafür enthält die Anlage zu § 9 BDSG „acht goldene Regeln“[241] zur Gewährleistung der IT-Sicherheit personenbezogener Daten. Diese sind in Form einer nicht abschließenden Liste mittels Zielvorgaben formuliert, die sich auf unterschiedliche Kontrollbereiche beziehen. Die folgende Aufzählung enthält die in der Anlage aufgeführten Kontrollbereiche mit beispielhaften Schutzmechanismen:[242]

- Physische Zutrittskontrolle (z.B. Schlüsselregelung, Chipkarten, Pförtner)
- Logische Zugangskontrolle (z.B. Benutzer- und Rechteverwaltung, Authentifikationsverfahren, Verschlüsselung)
- Logische Zugriffskontrolle (z.B. Berechtigungskonzept, Authentifizierungs- und Autorisierungsmechanismen, Verschlüsselung, Protokollierung),
- Weitergabekontrolle (z.B. Abschottung von Systemen vom Internet, Verschlüsselung auf Übertragungswegen, Taschenkontrollen),
- Eingabekontrolle (z.B. Protokollierung),
- Auftragskontrolle (z.B. Weisungen des Auftraggebers bei Auftragsdatenverarbeitung)
- Verfügbarkeitskontrolle (z.B. Backup, Katastrophenpläne)
- Trennung der zu unterschiedlichen Zwecken erhobenen Daten (z.B. physische Trennung, softwareseitiger Ausschluss, Trennung über Zugriffsregeln oder logische Separierung von Datenbanken).

Diese Regeln überschneiden sich mit allen im Rahmen der VDS zu beachtenden Schutzzielen (vgl. unten Tabelle 10). Welche Sicherheitsmaßnahmen konkret von einem TK-Diensteanbieter zu treffen sind, ergibt sich aus diesen Vorgaben noch nicht. Diesbezüglich wird den TK-Diensteanbietern ein

[240] Vgl. Gola/Schomerus: Bundesdatenschutzgesetz, § 5, Rn. 6.
[241] Vgl. Reinhard/Pohl/Capellaro: IT-Sicherheit und Recht, S. 59.
[242] Vgl. Reinhard/Pohl/Capellaro: IT-Sicherheit und Recht, S. 61 ff.; Gola/Schomerus: Bundesdatenschutzgesetz, § 9, Rn. 22 ff.

größerer Freiraum eingeräumt, wie die vom Gesetzgeber vorgegebenen Ziele erreicht werden. Der hierzu zu betreibende Aufwand wird in § 9 S. 2 BDSG dahingehend eingeschränkt, dass dieser in angemessenem Verhältnis zu dem angestrebten Schutzzweck stehen muss. Neben den Bezugsgrößen Schutzzweck und Aufwand der Sicherheitsmaßnahme ist gemäß der Anlage zu § 9 BDSG zudem die Art der zu schützenden Daten für die Höhe des zu gewährleistenden Sicherheitsniveaus relevant. Damit verpflichtet § 9 BDSG grundsätzlich nicht zur Gewährleistung eines optimalen Sicherheitsniveaus, sondern wie sein europarechtliches Vorbild lediglich zur Implementierung angemessener Sicherheitsmaßnahmen.[243] Die Abwägung zwischen Schutzzweck und Aufwand haben die einzelnen Unternehmen selbst vorzunehmen. Um die zur Abwägung notwendigen Faktoren bestimmen zu können verpflichtet § 9 BDSG zwar nicht ausdrücklich zur Durchführung einer Risikoanalyse, fordert diese jedoch inzident.[244] Das Konzept der Verhältnismäßigkeit macht das erzielte Sicherheitsniveau im Ergebnis wieder von wirtschaftlichen Erwägungen abhängig. Angesichts des verstärkten Wettbewerbs in den Telekommunikationsmärkten könnte dies vor allem bei kleineren TK-Unternehmen mit kleinen Gewinnmargen zu Einbußen der IT-Sicherheit führen. Dementsprechend wird vertreten, der Grundsatz der Verhältnismäßigkeit beziehe sich nur auf flankierende Maßnahmen und die Frage der Verhältnismäßigkeit stelle sich erst dann, wenn der Schutzzweck nur mit sehr kostenintensiven Maßnahmen erreicht werden kann.[245] Diese Überlegungen können jedoch nicht verhindern, dass in der Praxis Wirtschaftlichkeitserwägungen aufgrund des starken Wettbewerbs im Telekommunikationssektor stets einen großen Einfluss auf die Auswahl konkreter Sicherheitsmaßnahmen haben.

[243] Vgl. Reinhard/Pohl/Capellaro: IT-Sicherheit und Recht, S. 79.
[244] Vgl. Reinhard/Pohl/Capellaro: IT-Sicherheit und Recht, S. 81.
[245] Vgl. Reinhard/Pohl/Capellaro: IT-Sicherheit und Recht, S. 79.

	§ 113a TKG	§ 109 I TKG	§ 109 III TKG	§ 5 BDSG	§ 9 BDSG (mit Anhang)
Normadressat	Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer *(Abs. 1)*	TK-Diensteanbieter i.S.d. § 3 Nr. 6 TKG	Betreiber von TK-Anlagen, die dem Erbringen von Telekommunikationsdiens-ten für die Öffentlichkeit dienen *(S. 1)*		Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen *(S. 1)*
Vertraulichkeit	Zugang zu den gespeicherten Daten ausschließlich für hierzu besonders ermächtigte Personen *(Abs. 10 S. 2)* Löschpflicht innerhalb eines Monats nach Ablauf der 6 Mona-te *(Abs. 11)*	Schutz des Fernmeldege-heimnisses und personen-bezogener Daten *(Nr. 1)* Schutz der Telekommunika-tions- und Datenverarbei-tungssysteme gegen uner-laubte Zugriffe *(Nr. 2)*	Sicherheitskonzept (Anlagen und Dienste, Gefährdungen, Vorkehrungen und Schutzmaß-nahmen)	Datengeheimnis (mit der Datenverarbeitung beschäftig-te Personen sind zur Geheim-haltung verpflichtet)	Zutrittskontrolle *(Nr. 1)* Zugangskontrolle *(Nr. 2)* Zugriffskontrolle *(Nr. 3)* Weitergabekontrolle *(Nr. 4)* Auftragskontrolle *(Nr. 6)* Datentrennung *(Nr. 8)*
Verfügbarkeit	Unverzügliche Weiterleitung an die zuständigen Behörden muss möglich sein *(Abs.9)*				Verfügbarkeitskontrolle *(Nr. 7)* Auftragskontrolle *(Nr. 6)*
inhaltliche Kor-rektheit	Qualität und Schutz der gespei-cherten Verkehrsdaten *(Abs. 10 S. 1)*				Eingabekontrolle *(Nr. 5)* Auftragskontrolle *(Nr. 6)* Datentrennung *(Nr. 8)*
Integrität					Zutrittskontrolle *(Nr. 1)* Zugangskontrolle *(Nr. 2)* Zugriffskontrolle *(Nr. 3)* Eingabekontrolle *(Nr. 5)* Auftragskontrolle *(Nr. 6)* Datentrennung *(Nr. 8)*
Authentizität					Weitergabekontrolle *(Nr. 4)* Auftragskontrolle *(Nr. 6)*
Maßnahmen	Technische und organisatorische Maßnahmen *(Abs. 10 S. 1)*	Angemessene technische Vorkehrungen und sonstige Maßnahmen	Benennung eines Sicher-heitsbeauftragen und Erstel-lung eines Sicherheitskon-zepts *(S. 1)*		Erforderliche technische und organisatori-sche Maßnahmen
Berücksichti-gung	Im Bereich der Telekommunikati-on erforderliche Sorgfalt *(Abs. 10)*				Aufwand in angemessenem Verhältnis zum angestrebten Schutzzweck Art der verarbeitenden Daten *(S. 2)*

Tab. 10: Einfachgesetzliche Vorgaben mit datensicherheitstechnischem und -organisatorischem Bezug in Deutschland

2. Sicherheitstechnische Vorgaben auf Verwaltungsebene

Konkrete verwaltungsrechtliche Vorgaben zur technischen Ausgestaltung von Telekommunikations-Überwachungsmaßnahmen sind in der Telekommunikationsüberwachungsverordnung (TKÜV)[246] und in der Technischen Richtlinie zur TKÜV (TR TKÜV)[247] geregelt. Anforderungen an die sicherheitstechnische Absicherung der gespeicherten Vorratsdaten ergeben sich aus diesen Regelwerken jedoch nicht. Die TKÜV wurde nie an die Erfordernisse der Vorratsdatenspeicherung angepasst. Einer Anpassung derselben kam das Urteil des Bundesverfassungsgerichts (vgl. Kapitel F. II.) zuvor. Die von der Bundesnetzagentur verabschiedete TR TKÜV erfuhr eine Änderung seit der Einführung der Vorratsdatenspeicherung. Sie enthält explizite sicherheitstechnische Vorgaben in Bezug auf die Übermittlung der Vorratsdaten. Diese Vorgaben gehen jedoch nicht über die Vorgaben hinaus, die auch schon vor Einführung der Vorratsdatenspeicherung für die Übermittlung von Verkehrsdaten an berechtigte Stellen galten.

Zulässig sind insbesondere die Übermittlung per Telefax, der Postversand von Datenträgern und die Verwendung elektronischer Schnittstellen. Die technischen Anforderungen zur Verwendung elektronischer Schnittstellen orientieren sich vorrangig am technischen Standard TS 102 657 des *ETSI* (vgl. oben Kapitel D. II. 2. b).[248] Um die Vertraulichkeit, Integrität und Authentizität sind bei der Verwendung *IP*-basierter Übergabepunkte abzusichern, müssen Verschlüsselungssysteme auf Basis der *IPSec*-Protokollfamilie eingesetzt werden. Die Kommunikation zwischen der anfragenden Ermittlungsbehörde und dem Telekommunikationsunternehmen erfolgt dann innerhalb eines Virtual Private Network (VPN).[249] Dies gewährleistet z.B. die *SINA Box* von *Secunet*.[250] Die zur Authentifizierung erforderlichen Schlüssel werden von der BNetzA verwaltet und zur Verfügung gestellt. Die BNetzA verwaltet zudem eine sog. *Access Control List*, in der die möglichen Sicherheitsbeziehungen der beteiligten Entitäten hinterlegt sind. Dies verhindert die Abfrage von Daten durch unbefugte Stellen. Jedes an der Schnittstelle teilnehmende Telekommunikationsunternehmen sowie die berechtigten Stellen müssen sich bei der Bundesnetzagentur registrieren und erhalten daraufhin eine *SmartCard*, auf der die Zertifikatsschlüssel zur Authentifizierung gespeichert sind. Die Schlüssel zur Verschlüsselung der Vorratsdaten werden durch die Verschlüsselungssysteme selbst erzeugt und aktualisiert, so dass keiner der Beteiligten Kenntnis von den Schlüsseln erlangt.

Die folgende Abbildung zeigt schematisch die Struktur zur Übermittlung der Vorratsdaten über *IP*-basierte Schnittstellen:

---

[246] Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung) vom 3.11.2005 (BGBl. I, S. 3136), zuletzt geändert durch Artikel 4 des Gesetzes vom 25. Dezember 2008 (BGBl. I, S. 3083), im Internet abrufbar unter der URL http://www.gesetze-im-internet.de/bundesrecht/tk_v_2005/gesamt.pdf.

[247] Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten (TR TKÜV), Ausgabe 6.0 vom 2.12.2009, im Internet abrufbar unter der URL http://www.bundesnetzagentur.de/cae/servlet/contentblob/153314/publicationFile/6601/2009-12-00_TRTKUEVAausgb60pdf.pdf.

[248] Vgl. Teil B, Anlage 2.1 und 2.2 der TR TKÜV.

[249] Vgl. hierzu und im Folgenden Teil B, Anlage 2.3 der TR TKÜV.

[250] http://www.secunet.com/de/produkte-dienstleistungen/hochsicherheit/sina/sina-box/ .

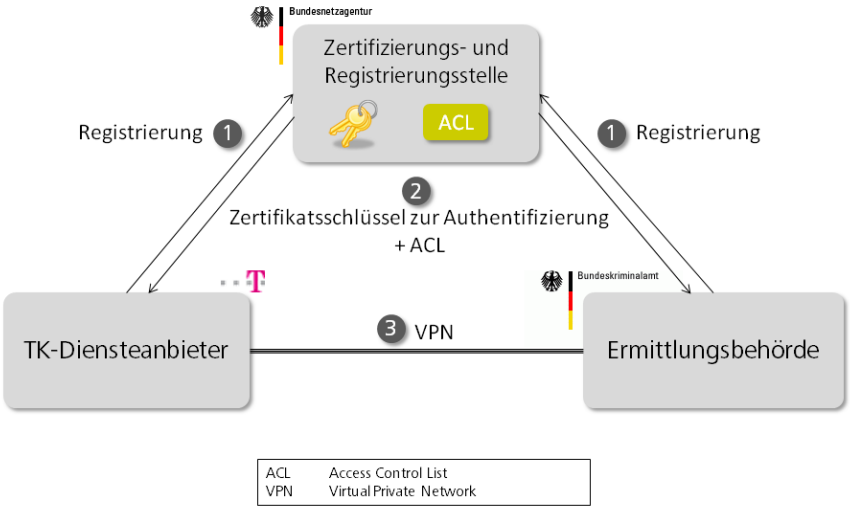


Abb. 31: Public Key Infrastruktur zur Übermittlung der Vorratsdaten

Diese Ausgestaltung schützt die Vertraulichkeit, Integrität und Authentizität der übermittelten Anfragen und Antworten. Gegen *Denial of Service*-Angriffe auf die Übermittlungsschnittstellen müssen TK-Diensteanbieter und Ermittlungsbehörden zusätzlich gesonderte Maßnahmen ergreifen.

II. Sicherheitsspezifische Aspekte des Urteils des Bundesverfassungsgerichts

Am 2. März 2010 wurde die konkrete gesetzliche Ausgestaltung der Vorratsdatenspeicherung in Deutschland vom Bundesverfassungsgericht für nichtig erklärt.[251] Dem vorausgegangen war die Einreichung mehrerer Verfassungsbeschwerden, unter anderem die Sammel-Verfassungsbeschwerde[252] des Arbeitskreis-Vorratsdatenspeicherung.[253]

Das Bundesverfassungsgericht wies in seinem Urteil auf das besondere Gewicht des mit der Speicherung der Vorratsdaten verbundenen Grundrechtseingriffs hin. Die Speicherung von Verkehrsdaten in einem so großen Umfang bedürfe der gesetzlichen Gewährleistung eines besonders hohen Standards der Datensicherheit.[254] Dieser müsse „in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgegeben“[255] werden. Diese Standards, die sich sowohl auf die Aufbewahrung als auch auf die Löschung und Übermittlung der Vorratsdaten zu beziehen haben, sah das Bundesverfassungsgericht durch die in Abschnitt F. I. beschriebene gesetzliche Ausgestaltung nicht gewährleistet.[256] § 113a X TKG sei zu unbestimmt, § 109 TKG enthalte vielfältige Relativierungen, die zudem von ihrer Systematik her unklar sind, und § 9 BDSG sei zu allgemein. Vor allem die Relativierung der Sicherheitsanforderungen aufgrund allgemeiner Wirtschaftlichkeitserwägungen (vgl. § 113 X TKG, § 109 II 4 TKG und § 9 S. 2 BDSG) gefährde vor dem Hintergrund des hohen Konkurrenz- und Kos-

[251] Urteil des BVerfG vom 2. März 2010, Az.: 1 BvR 256/08, im Internet abrufbar unter der URL http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html.
[252] Die Beschwerdeschrift ist im Internet abrufbar unter der URL http://www2.malte-spitz.de/uploads/verfassungsbeschwerde_vorratsdatenspeicherung.pdf.
[253] Daneben wurden Verfassungsbeschwerden von der FDP, Bündnis 90/Die Grünen und ver.di eingereicht.
[254] Vgl. Urteil des BVerfG vom 2. März 2010, Az.: 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 221 ff.
[255] Urteil des BVerfG vom 2. März 2010, Az.: 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 225.
[256] Vgl. hierzu und im Folgenden Urteil des BVerfG vom 2. März 2010, Az.: 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 271 ff.

tendrucks im Telekommunikationssektor eine ausreichende Absicherung der Vorratsdaten. Die konkretisierenden verwaltungsrechtlichen Vorschriften wurden zudem nur marginal an die Vorratsdatenspeicherung angepasst (vgl. Kapitel F. I. 2.) und können den erforderlichen Schutzstandard nach Ansicht des BVerfG dementsprechend auch nicht erfüllen.

Unter Hinweis auf Äußerungen von sachverständiger Seite weist das BVerfG in dem Urteil auf ein weites Spektrum verfügbarer Instrumente zur Erhöhung der Datensicherheit hin. Hierunter fallen

- die getrennte Speicherung der Daten (auf physisch getrennten und vom Internet entkoppelten Rechnern),
- die asymmetrische Verschlüsselung der Daten unter getrennter Verwahrung des Schlüssels,
- die Einhaltung des 4-Augen-Prinzips beim Zugriff auf die Daten,
- fortschrittliche Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln,
- die revisionssichere Protokollierung des Zugriffs auf die Daten und deren Löschung und
- der Einsatz von automatisierten Fehlerkorrektur- und Plausabilitätsverfahren.[257]

Vier dieser Instrumente hält das BVerfG für unabdingbar. Dies sind

- eine getrennte Speicherung der Daten,
- eine anspruchsvolle Verschlüsselung,
- ein gesichertes Zugriffsregime unter Nutzung etwa des Vier-Augen-Prinzips sowie
- eine revisionssichere Protokollierung.[258]

Um einen ausreichenden Schutzstandard zu gewährleisten, sei zudem die periodische Fortschreibung eines Sicherheitskonzepts erforderlich.[259] Dies sei durch § 109 III TKG nicht gewährleistet, der sich zudem nur auf die Netzbetreiber und damit nicht auf den gesamten Adressatenkreis des § 113a TKG bezieht.

Sollte die Vorratsdatenspeicherung in Deutschland wieder eingeführt werden, muss sich der Gesetzgeber an diese Grundsätze halten, um nicht Gefahr zu laufen, dass die gesetzliche Regelung erneut vom BVerfG für nichtig erklärt wird.

[257] Vgl. Urteil des BVerfG vom 2. März 2010, Az.: 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 223.
[258] Vgl. Urteil des BVerfG vom 2. März 2010, Az.: 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 224.
[259] Vgl. Urteil des BVerfG vom 2. März 2010, Az.: 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 273.

III. Die Praktische Umsetzung in der Bundesrepublik Deutschland

Um einen Einblick in die sicherheitstechnische Praxis der Vorratsdatenspeicherung in Deutschland (bevor diese durch das Urteil des BVerfG ausgesetzt wurde) zu gewinnen, wurden im Rahmen dieser Arbeit bei drei unterschiedlichen Unternehmen in Deutschland und insbesondere in Bayern Befragungen durchgeführt.[260] Dankbarerweise zur Verfügung gestellt haben sich hierfür der größte deutsche TK-Diensteanbieter, die *Deutsche Telekom AG* und die in Regensburg ansässige und regional in Niederbayern und der Oberpfalz tätige *R-Kom GmbH & Co. KG*. Zudem hat die *JonDos GmbH*, ein Hersteller von quelloffener Software zur Nutzung von Anonymisierungsdiensten, Informationen über die prototypische Umsetzung der Vorratsdatenspeicherung im Rahmen von *Mix*-Netzwerken bereitgestellt.[261]

Der ausgehändigte Fragenkatalog[262] unterteilt sich in zwei Teile. Der erste Abschnitt enthält Fragen zur sicherheitstechnischen Ausgestaltung der Aufbewahrung der Vorratsdaten. Der zweite Abschnitt bezieht sich auf die sicherheitstechnische Absicherung des Übermittlungsverfahrens.

1. Speicherung und Aufbewahrung der Daten

Im Hinblick auf die logische Absicherung der gespeicherten Daten lassen sich keine gravierende Unterschiede zwischen den Sicherheitsmaßnahmen der Deutschen Telekom und R-Kom feststellen. Beide Unternehmen haben die gespeicherten Vorratsdaten von den übrigen Daten logisch getrennt (die *Deutsche Telekom* zusätzlich physisch), und beschränkten den Zugriff auf einen kleinen Kreis speziell ermächtigter Mitarbeiter, die zuvor eingewiesen wurden und sich zur Geheimhaltung verpflichtet haben. Der Zugriff auf die Vorratsdaten wurde bei beiden Unternehmen protokolliert und eine automatisierte Löschung am Ende der Speicherfrist vorgesehen. Eine Verschlüsselung der Vorratsdaten hatte keines der beiden Unternehmen vorgesehen, die Deutsche Telekom hatte jedoch die Einführung eines Verschlüsselungsverfahrens geplant.[263]

2. Übermittlung der Daten an die Ermittlungsbehörde

Die praktizierten Übermittlungsmethoden der *Deutschen Telekom* variieren zwischen dem Postversand von Papierausdrucken oder Datenträger, der Versendung per Fax oder der Versendung per verschlüsselter E-Mail. Eine automatisierte Beantwortung von Anfragen war nicht vorgesehen.

Eine interessante und das Schutzziel der Vertraulichkeit schonende Methode zur Übermittlung der Daten an die Ermittlungsbehörden beinhaltet der Prototyp von *JonDos*. Um die Identität des Nutzers des Anonymisierungsdienstes aufzudecken, werden die Verkehrsdaten aller beteiligten Zwischenstationen (sog. *Mixe*) benötigt. Diese senden bei einer Abfrage durch eine Ermittlungsbehörde die Daten separat (jeder *Mix* sendet seine Daten) an die Ermittlungsbehörde. Nur wenn diese über die Daten aller

---

[260] Die entsprechenden Fragenkataloge sind inkl. Antworten im Anhang in Abschnitt 5) abgedruckt.
[261] Vgl. zur Sammlung der Daten Hermann/Wendolsky: Effectivity of Various Data Retention Schemes for Single-Hop Proxy Servers, in: Extended Abstracts of the Fourth Privacy Enhancing Technologies Convention (PET-CON 2009.1), Technical Report TUD-FI09-04, Technische Universität Dresden, im Internet abrufbar unter der URL http://www-sec.uni-regensburg.de/publ/2009/HeWe2009PETCON2009.1DataRetentionSchemes.pdf.
[262] Vgl. Anhang Abschnitt 5).
[263] Eine Zusammenstellung und systematische Gegenüberstellung der Antworten auf den Fragebogen finden sich im in Anhang in Abschnitt 5).

Mix-Stationen verfügt, kann sie die Identität des jeweiligen Nutzers aufdecken. Durch diese Konstruktion wird die Anonymität der übrigen Nutzer des Anonymisierungsdienstes gewahrt und die Wahrscheinlichkeit von Verletzungen der Vertraulichkeit reduziert.[264]

G. FAZIT

Die Vorratsdatenspeicherung gestaltet sich aus Sicht der IT-Sicherheit sehr facettenreich und wirft eine Vielzahl von Fragestellungen auf. Ähnlich wie bei der Beurteilung der verfassungsrechtlichen Zulässigkeit der Vorratsdatenspeicherung sind im Rahmen der Frage nach der konkreten sicherheitstechnischen Ausgestaltung die Interessen aller Beteiligten zu berücksichtigen. Vorrangig stehen sich hierbei die Interessen der Telekommunikationsnutzer und der staatlichen Ermittlungsbehörden gegenüber.

Die Telekommunikationsnutzer haben ein gewichtiges Interesse am Schutz der Vertraulichkeit der gespeicherten Vorratsdaten. Wie die vorangehende Betrachtung zeigt, sind die gesetzlichen Vorgaben jedoch nicht in der Lage, ein ausreichendes Maß an Vertraulichkeit der Verkehrsdaten zu gewährleisten. So hat es der europäische Gesetzgeber verpasst, konkrete technische Mindeststandards für die Aufbewahrung und Übermittlung der Vorratsdaten zu formulieren. Auch die nationalen Gesetzgeber weichen mit Ausnahme von Österreich vor der Normierung gesetzlicher Mindeststandards zurück und reichen die Verantwortung zur Gewährleistung eines ausreichenden Schutzniveaus an die Telekommunikationsunternehmer weiter. Zudem lassen die auf die Vorratsdatenspeicherung anzuwendenden sicherheitstechnischen Regelungen eine innere Systematik vermissen. Die Schutzzieldogmatik aus dem Bereich der IT-Sicherheit (vgl. Abb. 2) wurde inzwischen so weit an das allgemeine Datenschutzrecht angepasst dass diese die langen Aufzählungen von Bedrohungsszenarien ersetzen könnte. Ohne ausreichende Vollzugsmechanismen kann dies jedoch auch nicht zu einem erhöhten Sicherheitsstandard führen. So beschränkt sich die staatliche Überprüfung der von den Unternehmen implementierten Sicherheitsmaßnahmen zumeist auf die Verpflichtung zur Vorlage eines Sicherheitskonzepts. Dass die Vertraulichkeit der Vorratsdaten auch dem deutschen Gesetzgeber anscheinend weniger wichtig ist als die Sicherstellung der Verfügbarkeit der Vorratsdaten zu Ermittlungszwecken, zeigt ein Vergleich der jeweiligen Bußgeldrahmen. So ist die Nichtbeachtung der Speicherpflicht mit einem höheren Bußgeld bedroht als eine Verletzung der Datensicherheit.[265] Anstelle auf repressive Maßnahmen wie die Androhung von Bußgeldern zu setzen sollte eher versucht werden, durch proaktive Mechanismen von vornherein dafür zu sorgen, dass es erst gar nicht zu Sicherheitsverletzungen kommt. So hätte zum Beispiel der europäische Gesetzgeber die Erstattung der Kosten, die die Telekommunikationsunternehmen für die Implementierung der Vorratsdatenspeicherung aufwenden mussten, an die Durchführung einer Sicherheitszertifizierung knüpfen können. Dies hätte zu einer europaweiten Anhebung des Sicherheitsniveaus geführt.

Am wahrscheinlichsten sind negative Implikationen auf das Schutzziel der Vertraulichkeit vor allem in den Mitgliedstaaten zu erwarten, in denen eine Abfrage von Vorratsdaten auch zur Verfolgung von Ordnungswidrigkeiten erlaubt ist. Dies widerspricht den europarechtlichen Vorgaben und bedingt mit

[264] Vgl. Federrath /Köpsell/Wendolsky: Revocable Anonymity, in: Müller (Hrsg.): Proc. Emerging Trends in Information and Communication Security: International Conference, ETRICS 2006, S. 206 ff.
[265] Vgl. BVerfG, Urteil vom 2. März 2010, Az.: 1 BvR 256/08, Rn. 275.

der Vergrößerung der abrufberechtigten Stellen auch eine Vergrößerung des Kreises der Personen, die von bestimmten Vorratsdaten Kenntnis erlangen. Dementsprechend kritisch ist diese Entwicklung zu sehen, die eine Kontrolle der Verbreitung der Vorratsdaten erschwert. Der Blick in die Praxis bestätigt die erheblichen Gefahren für die Vertraulichkeit der Vorratsdaten. Vor allem in den Unternehmen, in denen keine Trennung der Vorratsdaten von den übrigen zu operativen Zwecken benötigten Daten erfolgt, scheint eine hinreichende Sensibilität im Hinblick auf die Vertraulichkeit der Daten nicht ausgeprägt zu sein. Es gibt jedoch auch Unternehmen, die einen hohen Sicherheitsstandard an die Absicherung der Vertraulichkeit der Vorratsdaten legen. Auch in diesen Unternehmen spielt jedoch der unkalkulierbare Faktor Mensch eine Rolle.

Der zweite an der Vorratsdatenspeicherung beteiligte Akteur sind die staatlichen Ermittlungsbehörden. Deren Interesse ist darauf gerichtet, im Rahmen von Ermittlungen zur Verhinderung oder Verfolgung von Straftaten möglichst schnell auf möglichst viele Vorratsdaten zugreifen zu können. Es bestehen jedoch gewichtige Zweifel, ob die Speicherung der Vorratsdaten in der konkreten Ausgestaltung überhaupt eine zusätzliche Aufklärung von Straftaten bewirkt. Statistisch nachgewiesen wurde dies bisher nicht.[266] Zudem bestehen mannigfaltige Möglichkeiten, die Vorratsdatenspeicherung zu umgehen. Hierzu ist nicht erforderlich, dass man technisch versiert ist. Zudem bestehen z.B. im *VoIP*-Bereich technische Schranken, so dass eine Speicherung von Verkehrsdaten in diesem Bereich teilweise garnicht möglich ist.

Vor dem Hintergrund, dass sicherheitstechnisch die beiden zentralen Schutzziele Vertraulichkeit und Verfügbarkeit nicht ausreichend gewährleistet werden können, stellt sich die Frage nach der Notwendigkeit der Vorratsdatenspeicherung. Am sinnvollsten erscheint es nach meiner Ansicht, das durch den immensen Umfang der Datensammlungen generierte Sicherheitsrisiko im Sinne eines proaktiven Datenschutzes erst gar nicht aufkommen zu lassen und auf die Vorratsdatenspeicherung zu verzichten.

[266] Vgl. oben Fn.108.

LITERATURVERZEICHNIS

Alperovitch, Dimitri: **An investigation of targeted intrusions into 70+ global companies, governments and non-profit organizations during the last 5 years**, August 2011, VP Threat Research McAfee, August 2011, im Internet abrufbar unter der URL http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

Arbeitskreis-Vorratsdatenspeicherung: **Es gibt keine sicheren Daten**, im Internet abrufbar unter der URL http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten.pdf

Artikel-29-Datenschutzgruppe: **Bericht 01/2010 über die zweite gemeinsame Durchsetzungsmaßnahme: Erfüllung der nach den innerstaatlichen Rechtsvorschriften über die Vorratsspeicherung von Verkehrsdaten aufgrund der Artikel 6 und 9 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und der Richtlinie 2006/24/EG (über die Vorratsspeicherung von Daten und zur Änderung der Datenschutzrichtlinie für elektronische Kommunikation) bestehenden Pflichten durch die Telekommunikations-Diensteanbieter und die Internet-Diensteanbieter auf nationaler Ebene**, WP 172, 13. Juli 2010, im Internet abrufbar unter der URL http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_de.pdf (der Anhang zur Stellungnahme ist abrufbar unter der URL http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_annex_en.pdf)

Artikel-29-Datenschutzgruppe, **Stellungnahme 4/2007 zum Begriff „personenbezogene Daten"**, WP 136, 20. Juni 2007, im Internet abrufbar unter der URL http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf

Artikel-29-Datenschutzgruppe: **Stellungnahme 3/2006 zur Richtlinie 2006 des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG**, WP 119, 25. März 2006, im Internet abrufbar unter der URL http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp119_de.pdf

Artikel-29-Datenschutzgruppe: **Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen**, 4. April 2008, im Internet abrufbar unter der URL http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_de.pdf

Bauer, Lukas/Reimer, Sebastian: **Handbuch Datenschutzrecht**, facultas.wuv, Wien 2009

Bundesnetzagentur, **Jahresbericht 2010**, im Internet abrufbar unter der URL http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/Jahresbericht2010pdf.pdf?__blob=publicationFile

Bundesnetzagentur: **Leitfaden zur Erstellung eines Sicherheitskonzeptes gemäß § 109 III TKG**, Januar 2006, im Internet abrufbar unter der URL http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Bundesnetzagentur/AmtsblattPublikationen/DruckschriftenAllgemein/SicherheitTelekommunikation/LeitfadenSicherheitskonzeptId4552pdf.pdf?__blob=publicationFile

Bundesnetzagentur: **Konsultationsentwurf der Bundesnetzagentur zu Anrufzustellung in einzelnen Mobilfunknetzen**, im Internet abrufbar unter der URL http://www.bundesnetzagentur.de/DE/DieBundesnetzagentur/Beschlusskammern/1BK-Geschaeftszeichen-Datenbank/BK1-GZ/2010/BK1-10-001/BK1-10-001_Marktdefinition.pdf?__blob=publicationFile

Büllingen, Franz/Gillet, Aurélia/Gries, Chrstin-Isabel/Hillebrand, Annette/Stamm, Peter: **Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich**, wik-Consult, Oktober 2004, im Internet abrufbar unter der URL http://www.humanistische-union.de/fileadmin/hu_upload/doku/vorratsdaten/info/Studie_VDS_final_lang.pdf

Coester, Ursula/Hein, Matthias: **IT-Sicherheit für den Mittelstand**, 1. Auflage, Datakontext-Fachverlag, Solingen 2005

Damker, Herbert/Federrath, Hannes/Schneider, Michael: **Maskerade-Angriffe im Internet, eine Demonstration von Unsicherheit**, in: DuD 20/5 (1996), S. 286-294

Dorotheee, Szuba: **Vorratsdatenspeicherung, Der europäische und deutsche Gesetzgeber im Spannungsfeld zwischen Freiheit und Sicherheit**, Frankfurter Studien zum Datenschutz, Band 37, Nomos Verlag, 1. Auflage, Baden-Baden 2011

Eckert, Claudia: **IT-Sicherheit, Konzepte – Verfahren – Protokolle, Studienausgabe**, Oldenburg Wissenschaftsverlag GmbH, München 2005

Ehmann, Eugen/Helfrich, Marcus (Hrsg.): **EG Datenschutzrichtlinie**, Kurzkommentar, Verlag Dr. Otto Schmidt, Köln 1999

Ernst, Stefan (Hrsg.): **Hacker, Cracker & Computerviren, Recht und Praxis der Informationssicherheit**, Verlag Dr. Otto Schmidt, Köln 2004

Europäische Kommission: **Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG), Bericht der Kommission an den Rat und das Europäische Parlament**, 18.4.2011, KOM(2011) 255, im Internet abrufbar unter der URL http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_de.pdf

Federrath, Hannes: **Die bedrohte Sicherheit von Informationsnetzen**, 30. November 2001, im Internet abrufbar unter der URL http://www-sec.uni-regensburg.de/publ/2002/informationsnetze.html

Federrath, Hannes: **Sicherheit im Netz**, in: Moritz, Hans-Werner Moritz/ Dreier, Thomas (Hrsg): **Rechts-Handbuch zum E-Commerce**, Verlag Dr. Otto Schmidt KG, S. 805-817, 2002

Federrath, Hannes: **Technische Aspekte des neuen Computergrundrechts**, in: Uerpmann-Wittzack, Robert (Hrsg.): Das neue Computergrundrecht, LIT Verlag, Berlin 2009, S. 53-60

Federrath, Hannes/Fuchs, Karl-Peter/Herrmann, Dominik/Maier, Daniel/Scheuer, Florian/Wagner, Kai: **Grenzen des „digitalen Radiergummis"**, DuD 6/2011, S. 403-407

Federrath, Hannes/Köpsell, Stefan/Wendolsky, Rolf: **Revocable Anonymity**, in: Müller, Günter(Hrsg.): Proc. Emerging Trends in Information and Communication Security: International Conference, ETRICS 2006, Springer-Verlag, Heidelberg 2006, S. 206-220

Forgó, Nikolaus/Jlussi, Dennis/Klügel, Christian/Krügel, Tina: **Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung**, in: DuD 10/2008. S. 680-682

Freiling, Felix C.: Zur **Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung**, Stellungnahme im Rahmen der Verfassungsbeschwerden 1 BvR 256/08, 263/08, 586/08 für das Bundesverfassungsgericht vom 22. Juni 2009, im Internet abrufbar unter der URL http://pi1.informatik.uni-mannheim.de/filepool/publications/TR-2009-005.pdf

Gausling, Tina: **Verdanchtsunabhängige Speicherung von Verkehrsdaten auf Vorrat**, Information und Recht, Band 76, Verlag C.H. Beck, München 2010

Gola, Peter/Schomerus, Rudolf (Hrsg.): **Bundesdatenschutzgesetz**, 10. Auflage, Verlag C.H.Beck, München 2010

Graf, Peter (Hrsg.): **Beck'scher Online-Kommentar StPO**, Edition 11, Stand: 15.7.2011

Gusy, Christoph: **Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**, in: DuD 1/2009, S. 33-38

Hensel, Dirk: **Die Vorratsdatenspeicherung aus datenschutzrechtlicher Sicht, Die Bildung von Persönlichkeitsprofilen und andere Probleme der Vorratsdatenspeicherung**, in: DuD 9/2009, S. 527-530

Hermann, Dominik/Wendolsky, Rolf: **Effectivity of Various Data Retention Schemes for Single-Hop Proxy Servers**, in: Extended Abstracts of the Fourth Privacy Enhancing Technologies Convention (PET-CON 2009.1), Technical Report TUD-FI09-04, Technische Universität Dresden, im Internet abrufbar unter der URL http://www-sec.uni-regensburg.de/publ/2009/HeWe2009PETCON2009.1DataRetentionSchemes.pdf

Kurz, Constanze/Rieger, Frank: **Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung** (1 BvR 256/08, 263/08, 586/08) vom 9. Juni 2009, im Internet abrufbar unter der URL http://www.ccc.de/de/vds/VDSfinal18.pdf

Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: **Datenschutzrecht**, 2. Auflage, Verlag C.F. Müller, Heidelberg 2011

Kühling, Jürgen/Sivridis, Anastasios/Schwuchow, Matthias/Burghardt, Thorben: **Das datenschutzrechtliche Vollzugsdefizit im Bereich der Telemedien – ein Schreckensbericht**, in: DuD 6/2009, S. 335-342

Lanier, Jaron: **You are not a gadget**, Alfred A. Knopf, New York 2010

Milford, Peter J.: **The Data Retention Directive - too fast, too fourious a response? Implementing and Transposing European Directive 2006/24/EC**, LLM Dissertation, Southampton Business School, im Internet abrufbar unter der URL http://www.petermilford.com/downloads/Data_Retention_PMilford.pdf

Müller, Klaus-Rainer: **IT-Sicherheit mit System**, 2. Auflage, Vieweg Verlag, Wiesbaden 2005

Pfitzmann, Andreas/Rost, Martin: **Datenschutz-Schutzziele – revisited**, in: DuD 6/2009, S. 353-358, im Internet abrufbar unter der URL http://www.maroki.de/pub/privacy/DuD0906_Schutzziele.pdf

Rannenberg, Kai/Pfitzmann, Andreas/Müller, Günter: **IT Security and Multilateral Security**, in: Müller, Günter/Rannenberg, Kai (Hrsg.): **Multilateral Security in Communications**, 3. Auflage, Addison-Wesley-Longman 1999

Raunhofer, Judith: **The Retention of Communications Data in Europe and the UK**, in: Edwards, Lilian/Waelde, Charlotte (Hrsg.): **Law and the Internet**, Hart Publishing, 3. Auflage, Portland, 2009, S. 575-599

Reinhard, Tim/Pohl, Lorenz/Capellaro, Hans-Christoph (Hrsg): **IT-Sicherheit und Recht**, Erich Schmidt Verlag, München 2006

Rost, Martin/Bock, Kirsten: **Privacy By Design und die Neuen Schutzziele**, in: DuD 1/2011, S. 30-35

Roßnagel, Alexander (Hrsg.): **Handbuch Datenschutzrecht**, Verlag C.H.Beck, München 2003

Stampfel, Gerald/Gansterer, Wilfried/Ilger, Michael: **Data Retention, The EU Directive 2006/24/EC from a Technological Perspective**, Medien und Recht Verlags GmbH, Wien 2008

Tannenbaum, Andrew Stuart: **Computernetzwerke**, 4. Auflage, Pearson Studium, München 2003

Walke, Bernhard: **Mobilfunknetze und ihre Protokolle 1**, 3. Auflage, Teubner, Stuttgart 2001

Wettern, Michael: **Umsetzung der Vorratsdatenspeicherung an den Hochschulen**, in: DuD 2009, S. 343-346

Wildhaber, Bruno: **Informationssicherheit, Rechtliche Grundlagen und Anforderungen an die Praxis**, Dissertation der Rechtswissenschaftlichen Fakultät der Universität Zürich, Schulthess Polygraphischer Verlag AG, Zürich 1993

Wimmer Andersson, Lisa/Buchinger, Kerstin u.a.: **Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung**, Studie des Ludwig Boltzmann Instituts für Menschenrechte und des Instituts für Rechtsinformatik (IRI) an der Leibniz Universität Hannover, 10. März 2008, im Internet abrufbar unter der URL http://www.univie.ac.at/bim/php/bim/get.php?id=1010

ANHANG

Seite

1) Überblick über die einzelstaatlichen rechtlichen Umsetzungen der VDSRL (Umsetzung, Speicherdauer, Zugriffsschwelle) XII

2) Überblick über die einzelstaatlichen rechtlichen Umsetzungen der sicherheitstechnischen und organisatorischen Vorgaben aus Art. 7 VDSRL XXV

3) Einzelstaatliche Normen zur Umsetzung der sicherheitstechnischen und organisatorischen Vorgaben aus Art. 7 VDSRL XXXIV

4) Überblick über die praktische Umsetzung der sicherheitstechnischen und organisatorischen einzelstaatlichen Vorgaben LXVV

5) Eigene Erhebungen zur praktischen Umsetzung der sicherheitstechnischen und organisatorischen Vorgaben in Deutschland (Deutsche Telekom AG) und Bayern (R-Kom GmbH & Co. KG, JonDos GmbH) LXXXI

Überblick über die einzelstaatlichen rechtlichen Umsetzungen der VDSRL (Umsetzung, Speicherdauer, Zugriffsschwelle)

Ohne Anspruch auf Vollständigkeit!

	Rechtliche Umsetzung[1]	Speicherdauer[2] (rechtlich)	Zweckbindung / Zugriffsschwelle[3] (rechtlich)
Vorgaben der EU-Richtlinie 2006/24/EG		6-24 Monate (Art. 6 VDSRL)	"Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden" (Art. 1 VDSRL)
Belgien	Teilweise	12-36 Monate für öffentlich zugängliche Telefondienste, keine zeitl. Vorgaben bzgl. Internet-Verkehrsdaten [> 24 Monate]	Ermittlung und Verfolgung von Straftaten, Verfolgung des Missbrauchs von Notdienstrufnummern, Untersuchungen des vorsätzlichen Missbrauchs von elektronischen Kommunikationsnetzen oder –diensten sowie für Informationsbeschaffungseinsätze ovn Geheim- und Sicherheitsdiensten [Alle Straftaten und Öffentliche Sicherheit]
Bulgarien	Vom obersten bulgarischen Verwaltungsgericht gestoppt[4], am 10.5.2010 erneut in Kraft getreten[5]	12 Monate (Daten, auf die zugegriffen wurde, können weitere 6 Monate gespeichert werden) [≤ 12 Monate]	Zur Feststellung und Ermittlung von schweren Straftaten und Straftaten nach den Artikeln 319a bis 319f des Strafgesetzbuchs sowie zur Fahndung nach Personen [Eingrenzung über Mindeststrafe oder Katalog]
Zypern	Derzeit ausgesetzt[6]		
Dänemark	Ja	12 Monate [≤ 12 Monate]	Zur Ermittlung und Verfolgung von Straftaten [Alle Straftaten und Öffentliche Sicherheit]
Deutschland	Derzeit ausgesetzt[7]		
England	Ja	12 Monate [≤ 12 Monate]	Zur Ermittlung, Feststellung und Verfolgung von schweren Straftaten [Eingrenzung auf schwere Straftaten, ohne diese zu definieren]
Estland	Ja	12 Monate [≤ 12 Monate]	Verwendung zulässig, wenn eine Sammlung von Beweismitteln durch andere Verfahrenshandlungen ausgeschlossen oder besonders schwierig ist und Gegenstand des Strafverfahrens eine Straftat ersten Grades oder eine vorsätzlich begangene und mit mindestens drei Jahren Freiheitsentzug bedrohte Straftat zweiten Grades ist [Eingrenzung über Mindeststrafe oder Katalog]
Finnland	Ja	12 Monate [≤ 12 Monate]	Zur Ermittlung, Feststellung und Verfolgung schwerer Straftaten gemäß Kapitel 5a Artikel 3 Absatz 1 des Gesetzes über Zwangsmaßnahmen [Eingrenzung über Mindeststrafe oder Katalog]
Frankreich	Ja	12 Monate [≤ 12 Monate]	Zur Feststellung, Ermittlung und Verfolgung von Straftaten und ausschließlich mit dem Ziel, den Justizbehördne benötigte Informationen zur Verfügung zu stellen, sowie zur Verhinderung von Terroranschlägen und zum Schutz von geistigem Eigentum [Alle Straftaten und Öffentliche Sicherheit]
Griechenland	Ja	12 Monate [≤ 12 Monate]	Zur Aufdeckung von besonders schweren Straftaten [Eingrenzung über Mindeststrafe oder Katalog]
Irland	Ja	24 Monate für Daten aus dem Telefonfestnetz und dem Mobilfunk, 12 Monate für Internetverkehrsdaten, E-Mail und Internet-Telefonie [≤ 24 Monate]	Zur Verhütung schwerer Straftaten (d.h. mit mindestens fünf Jahren freiheitsentzug bedrohte Straftaten oder eine der im Anhang zum Umsetzungsgesetz aufgeführten Straftaten), zum Schutz der staatlichen Sicherheit oder zur Rettung von Menschenleben [Eingrenzung über Mindeststrafe oder Katalog]
Italien	Ja	24 Monate Festnetz- und Mobilfunktelefonie,	Zur Ermittlung und Bekämpfung von Straftaten

[1] Datenquellen: EU-Kommission: Übersicht über die einzelstaatlichen Durchführungsmaßnahmen, im Internet abrufbar unter derURL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72006L0024:DE:NOT. EU-Kommission: Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung, S. 6 f.
[2] EU-Kommission: Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung, S. 16 ff.
[3] EU-Kommission: Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung, S. 11 ff.
[4] Urteil des Obersten Bulgarischen Verwaltungsgerichts vom 11. Dezember 2008, vgl. Meldung auf heise.de, im Internet abrufbar unter der URL http://www.heise.de/newsticker/meldung/Vorratsdatenspeicherung-in-Bulgarien-vorerst-gestoppt-192081.html.
[5] Vgl. bulgarisches Telekommunikationsgesetz, Art. 250a ff., im Internet abrufbar unter der URL http://www.crc.bg/files/_en/LAW_ON_ELECTRONIC_COMMUNICATIONS.pdf.
[6] Urteil des Zypriotischen Verfassungsgerichts vom 1. Februar 2011, im Internet abrufbar unter der URL http://www.supremecourt.gov.cy/Judicial/SC.nsf/All/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf.
[7] Urteil des Deutschen Bundesverfassungsgerichts vom 15. Dezember 2009, BVerfGE 125, 260, im Internet abrufbar unter der URL http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintVersion&Name=bv125260.

	Rechtliche Umsetzung[1]	Speicherdauer[2] (rechtlich)	Zweckbindung / Zugriffsschwelle[3] (rechtlich)
		12 Monate für Internet-verkehrsdaten, E-Mail und Internet-Telefonie [≤ 24 Monate]	[Alle Straftaten und Öffentliche Sicherheit]
Lettland	Ja	18 Monate [≤ 24 Monate]	Zum Schutz der staatlichen und öffentlichen Sicherheit oder zur Ermittlung von Straftaten, zur Strafverfolgung und zur Durchführung gerichtlicher Strafverfahren [Alle Straftaten und Öffentliche Sicherheit]
Litauen	Ja	6 Monate [6 Monate]	Für die Ermittlung, Feststellung und Verfolgung von schweren und sehr schweren Straftaten im Sinne des litauischen Strafgesetzbuchs [Eingrenzung über Mindeststrafe oder Katalog]
Luxemburg	Ja	6 Monate [6 Monate]	Zur Feststellung, Ermittlung und Verfolgung von mit mindestens einem Jahr Freiheitsentzug bedrohten Straftaten [Eingrenzung über Mindeststrafe oder Katalog]
Malta	Ja	12 Monate für Telefonfestnetz-, Mobilfunk- und Internet-Telefonie-Daten, 6 Monate für Daten zu Internetzugang und Internet E-Mail [≤ 12 Monate]	Zur Ermittlung, Feststellung oder Verfolgung von schweren Straftaten [Eingrenzung auf schwere Straftaten, ohne diese zu definieren]
Niederlande	Ja	12 Monate [≤ 12 Monate]	Zur Ermittlung und Verfolgung von mit Freiheitsentzug bedrohten schweren Straftaten [Eingrenzung über Mindeststrafe oder Katalog]
Österreich[8]	Ja	6 Monate (§ 102a I 1 TKG) [6 Monate]	Zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt [Eingrenzung über Mindeststrafe oder Katalog]
Polen	Ja	24 Monate [≤ 24 Monate]	Zur Verhütung oder Feststellung von Straftaten, zur Verhütung und Feststellung von Zoll- und Steuervergehen, zur Verwendung durch Staatsanwaltschaften und Gerichte, soweit dies für anhängige Gerichtsverfahren von Bedeutung ist, damit der Inlandsgeheimdienst, der Auslandsgeheimdienst, das Zentrale Antikorruptionsbüro, der Militärische Inlandsgeheimdienst und der Militärische Auslandsgeheimdienst ihre Aufgaben wahrnehmen können [Alle Straftaten und Öffentliche Sicherheit]
Portugal	Ja	12 Monate [≤ 12 Monate]	Zur Ermittlung, Feststellung und Verfolgung von schweren Straftaten [Eingrenzung auf schwere Straftaten, ohne diese zu definieren]
Rumänien	Derzeit ausgesetzt[9]		
Schweden	Nein		
Slowakei	Ja	12 Monate für Daten aus dem Telefonfestnetz und dem Mobilfunk, 6 Monate für Daten zu Internetzugang, E-Mail und Internet-Telefonie [≤ 12 Monate]	Zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten [Alle Straftaten und Öffentliche Sicherheit]
Slowenien	Ja	14 Monate für Telefoniedaten und 8 Monate für internetbezogene Daten [≤ 24 Monate]	Zur Gewährleistung der nationalen Sicherheit, der verfassungsmäßigen Ordnung sowie der Sicherheitsinteressen, politischen und wirtschaftlichen Interessen des Staates und zum Zwecke der Landesverteidigung [Alle Straftaten und Öffentliche Sicherheit]
Spanien	Ja	12 Monate	Zur Feststellung, Ermittlung und Verfolgung der im Strafgesetz-

[8] Österreichisches Umsetzungsgesetz vom 18. Mai 2011 , im Internet abrufbar unter der URL ftp://ftp.freenet.at/privacy/gesetze/vorratsdatenspeicherung.pdf.
[9] Urteil des Rumänischen Verfassungsgerichtshofs vom 7. Oktober 2009, im Internet abrufbar unter der URL http://www.ccr.ro/decisions/pdf/ro/2009/D1258_09.pdf.

	Rechtliche Umsetzung[1]	Speicherdauer[2] (rechtlich)	Zweckbindung / Zugriffsschwelle[3] (rechtlich)
		[≤ 12 Monate]	buch oder den besonderen Strafgesetzen aufgeführten schweren Straftaten [Eingrenzung über Mindeststrafe oder Katalog]
Tschechien	Derzeit ausgesetzt[10]		
Ungarn	Ja	6 Monate für erfolglose Anrufversuche, 12 Monate für restliche Verkehrsdaten [≤ 12 Monate]	Um den Ermittlungsbehörden, der Staatsanwaltschaft, den Gerichten und nationalen Sicherheitsbehörden die Wahrnehmung ihrer Aufgaben zu ermöglichen und die Polizei sowie das Nationale Steuer- und Zollamt in die Lage zu setzen, bei Straftaten zu ermitteln, die mit mindestens zwei Jahren Freiheitsentzug bedroht sind [Eingrenzung über Mindeststrafe oder Katalog]

[10] Urteil des tschechischen Verfassungsgerichts vom 31. März 2011, im Internet abrufbar unter der URL http://www.concourt.cz/clanek/GetFile?id=5075.

Überblick über die einzelstaatlichen rechtlichen Umsetzungen der sicherheitstechnischen und organisatorischen Vorgaben aus Art. 7 VDSRL

(mit Ausnahme von Griechenland, Litauen, Malta und Portugal)

Ohne Anspruch auf Vollständigkeit!

	Vertraulichkeit	Verfügbarkeit	Inhaltliche Korrektheit	Integrität	Authentizität	Technische Konkretisierung
Bulgarien	Übermittlung der Daten wenn möglich elektronisch unter Berücksichtigung der Anforderungen des nationalen Signaturgesetzes (Law of Electronic Management, Law on the Electronic Document and the Electronic Signature)[11] Tätigkeitsbezogene Beschränkung des Kreises der Zugangsberechtigten[12] Vernichtung („destroy") der Daten am Ende der Speicherfrist[13]	Abfragen müssen 24 Stunden am Tag, 7 Tage die Woche entgegengenommen werden können[14] und innerhalb von 72 Stunden beantwortet werden[15]				Konkretisierung auf Verwaltungsebene durch bulgarische Kommission[16]
	Alle 4 Grundsätze der VDSRL wortgleich umgesetzt[17] Explizit auch Schutz bei Übermittlung angesprochen[18] Berücksichtigung: technologischen Errungenschaften, Risiko und Natur der zu schützenden Daten[19]					
Dänemark	Weisungsgebundenheit des verarbeitenden Personenkreises[20]					Justizminister legt detaillierte Sicherheitsvorgaben fest[21]
	Geeignete technische und organisatorische Sicherheitsvorkehrungen zum Schutz der Daten gegen zufällige oder unberechtigte Zerstörung, Verlust oder Änderung und gegen unbefugte Kenntnisnahme, Missbrauch oder Verarbeitung unter Verletzung der Vorgaben des Datenschutzgesetzes[22]					
England	Löschung mind. monatlich in einer Weise, dass Daten nicht wiederhergestellt werden können[23]	Speicherung der Daten so, dass diese unverzüglich auf Anfragen hin übermittelt werden können[24]				
	Alle 4 Grundsätze aus Art. 7 VDSRL wortlautgetreu umgesetzt[25]					
Estland	Zugang Dritter zu Daten nur in rechtlich zulässigen Fällen[26]		Prinzip der Datenqualität: Daten sollen aktuell, vollständig und notwen-	Prinzip der Datenqualität: Daten sollen aktuell, vollständig und notwendig für		

[11] Art. 250e des bulgarischen Kommunikationsgesetzes (zuletzt geändert am 9.4.2010).
[12] Art. 252 des bulgarischen Kommunikationsgesetzes (zuletzt geändert am 9.4.2010).
[13] Art. 250a IV, Art. 261a II Nr. 4 des bulgarischen Kommunikationsgesetzes (zuletzt geändert am 9.4.2010) und Art. 25 I Nr. 1 des bulgarischen Datenschutzgesetzes (zuletzt geändert am 5.6.2009).
[14] Art. 250d I des bulgarischen Kommunikationsgesetzes (zuletzt geändert am 9.4.2010).
[15] Art. 250e II des bulgarischen Kommunikationsgesetzes (zuletzt geändert am 9.4.2010).
[16] Art. 23 V des bulgarischen Datenschutzgesetzes (zuletzt geändert am 5.6.2009).
[17] Art. 261a II des bulgarischen Kommunikationsgesetzes (zuletzt geändert am 9.4.2010).
[18] Art. 23 II des bulgarischen Datenschutzgesetzes (zuletzt geändert am 5.6.2009).
[19] Art. 23 III des bulgarischen Datenschutzgesetzes (zuletzt geändert am 5.6.2009).
[20] Nr. 41 I des dänischen Datenschutzgesetzes (zuletzt geändert am12.6.2009).
[21] Nr. 41 V des dänischen Datenschutzgesetzes (zuletzt geändert am 12.6.2009).
[22] Nr. 41 III des dänischen Datenschutzgesetzes (zuletzt geändert am 12.6.2009).
[23] Nr. 6 III der englischen Verordnung über die Vorratsdatenspeicherung (in der Fassung vom 6.4.2009).
[24] Nr. 8 der englischen Verordnung über die Vorratsdatenspeicherung (in der Fassung vom 6.4.2009).
[25] Nr. 6 I der englischen Verordnung über die Vorratsdatenspeicherung (in der Fassung vom 6.4.2009).
[26] § 101 I des estländischen Telekommunikationsgesetzes (zuletzt geändert am 24.1.2007).

	Vertraulichkeit	Verfügbarkeit	Inhaltliche Korrektheit	Integrität	Authentizität	Technische Konkretisierung
	Insb. Vertraulichkeit von Inhalts- und Verkehrsdaten[27] Explizit Löschung („destroy") von Daten, die abgefragt wurden und zu Beweis- oder Ermittlungszwecken nicht mehr benötigt werden[28] (zudem Antragsrecht des Betroffenen zur Löschung[29] und Berichtspflicht in der Kriminalakte[30])		dig für den gegebenen Zweck sein[31]	den gegebenen Zweck sein[32]		
	Gewährleistung der Sicherheit des Kommunikationsnetzes[33], Prinzip der Sicherheit: Sicherheitsmaßnahmen zum Schutz gegen unfreiwillige und unberechtigte Änderung, Zugänglichmachung oder Zerstörung personenbezogener Daten[34];					
Finnland a.A. Evaluation Kom	Löschpflicht nur für Ortsdaten[35]	Speicherung der Daten so, dass diese unverzüglich auf Anfragen hin übermittelt werden können[36]		Protokollierung des Zugriffs auf die Daten (inkl. Zeit und Dauer des Zugriffs und zugreifende Person über einen Zeitraum von 2 Jahren[37]		Übertragung der Regelung technischer Details in allen Fragen an finnische TK-Regulierungsbehörde FICORA[38]
	Alle 4 Prinzipien aus Art. 7 VDSRL umgesetzt: Betriebssicherheit, Kommunikationssicherheit, Hardware- und Softwaresicherheit und Datensicherheit, Berücksichtigung von Risiko, Stand der Technik und Kosten[39]					
Frankreich	Geeignete Maßnahmen zum Schutz der Vertraulichkeit[40] Lösch- oder Anonymisierungspflicht für Verkehrsdaten (mit Ausnahmen)[41]			Geeignete Maßnahmen zum Schutz der Integrität[42]		Regelung technischer Details zur Gewährleistung der Systemsicherheit durch französische TK-Regulierungsbehörde[43]

[27] § 102 I des estländischen Telekommunikationsgesetzes (zuletzt geändert am 24.1.2007).
[28] Artikel 122 III der estländischen Strafprozessordnung (zuletzt geändert am 15.6.2005)
[29] Artikel 122 II Absatz 2 der estländischen Strafprozessordnung (zuletzt geändert am 15.6.2005)
[30] Artikel 122 IV Absatz 2 der estländischen Strafprozessordnung (zuletzt geändert am 15.6.2005)
[31] § 6 Nr. 5) des estländischen Datenschutzgesetzes (in der Fassung vom 1.5.2004).
[32] § 6 Nr. 5) des estländischen Datenschutzgesetzes (in der Fassung vom 1.5.2004).
[33] § 101 I des estländischen Telekommunikationsgesetzes (zuletzt geändert am 24.1.2007).
[34] § 6 Nr. 6) des estländischen Datenschutzgesetzes (in der Fassung vom 1.5.2004).
[35] Abschnitt 16 III des finnischen Kommunikationsgesetzes (zuletzt geändert am 28. April 2011).
[36] Abschnitt 14b I S. 4 des finnischen Kommunikationsgesetzes (zuletzt geändert am 28. April 2011).
[37] Abschnitt 15 I des finnischen Kommunikationsgesetzes (zuletzt geändert am 28. April 2011).
[38] Abschnitt 14a VI, Abschnitt 14b IV, Abschnitt 15 II, Abschnitt 19 IV, Abschnitt 20 V des finnischen Kommunikationsgesetzes (zuletzt geändert am 28.4.2011); siehe hierzu den Internetauftritt von FICORA unter http://www.ficora.fi/en/index/saadokset/lait/svt.html.
[39] Abschnitt 19 des finnischen Kommunikationsgesetzes (zuletzt geändert am 28.4.2011).
[40] Article D98-5 I, II Code des postes et des communications électroniques (zuletzt geändert am 29.7.2005).
[41] Article L34-1 I Code des postes et des communications électroniques (zuletzt geändert am 29.7.2005).
[42] Article D98-5 II Code des postes et des communications électroniques (zuletzt geändert am 29.7.2005).
[43] Artikel 11 2° b) des Gesetzes Nr. 78-17 vom 6. Januar 1978 (zuletzt geändert am 29.3.2011), Article D98-5 III Code des postes et des communications électroniques (zuletzt geändert am 29.7.2005).

	Vertraulichkeit	Verfügbarkeit	Inhaltliche Korrektheit	Integrität	Authentizität	Technische Konkretisierung
	Gewährleistung der Datensicherheit (v.a. Schutz vor Änderung, Beschädigung oder unbefugtem Zugang Dritter)[44] Berücksichtigung der Art der Daten und dem Risiko[44] Geeignete Maßnahmen zum Schutz der Kommunikationssicherheit[45]					
Griechenland	Keine Informationen					
Irland	Vertraulichkeit der Verkehrsdaten[46] Zugang nur für speziell autorisierte Personen[47]					Empfehlungen des Datenschutzbeauftragten über Best Practices[48]
	Alle 4 Grundsätze aus Art. 7 VDSRL wortlautgetreu umgesetzt[49] Geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Dienste, u.a. Schutz der Daten vor zufälliger oder unberechtigter Zerstörung, zufälligem Verlust oder Veränderung und unberechtigter oder unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung[50] Berücksichtigung: Risiko, Stand der Technik, Kosten[50] Implementierung einer Sicherheitspolitik[51]					
Italien a.A. Kom	Authentifizierungs- und Autorisierungsmechanismen (wissensbasiert, hardwarebasiert oder biometrisch) mit Vorgaben zu sicheren Passwörtern (Länge mind 8 Zeichen, Änderung alle 3 Monate bei sensiblen Daten) + Vielzahl an detaillierten Regelungen[52] Lösch- und Anonymisierungspflicht für Verkehrsdaten[53]	Wöchentliche Backups[54]	Daten sollen inhaltlich korrekt, wenn notwendig aktuell, und vollständig sein[55]	Authentifizierungs- und Autorisierungsmechanismen (wissensbasiert, hardwarebasiert oder biometrisch) mit Vorgaben zu sicheren Passwörtern (Länge mind 8 Zeichen, Änderung alle 3 Monate bei sensiblen Daten) + Vielzahl an detaillierten Regelungen[52]		Sicherheitsvorkehrungen in Bezug auf den Daten bei den Ermittlungsbehörden werden durch Dekret des Premierministers geregelt[56] Technische Vorgaben im Anhang werden durch Dekret des Justizministers in Übereinkunft mit dem Minister für Innovation und Technologie geregelt[57]
	Mindestmaß an Sicherheitsvorkehrungen erforderlich[58] Geeignete vorbeugende Maßnahmen zur Minimierung des Risikos der beabsichtigten und unbeabsichtigten Zerstörung, des Verlusts, des unberechtigten Zugriffs und der unrechtmäßigen Verarbeitung der Daten[59]					

[44] Artikel 11 2° b) des Gesetzes Nr. 78-17 vom 6. Januar 1978 (zuletzt geändert am 29.3.2011).
[45] Article D98-5 III Code des postes et des communications électroniques (zuletzt geändert am 29.7.2005).
[46] Abschnitt 5 des irischen Datenschutzgesetzes (in der durch die Richtlinie 2006/24/EC and 2009/136/EC geänderten Fassung).
[47] Abschnitt 4 des irischen Datenschutzgesetzes (in der durch die Richtlinie 2006/24/EC and 2009/136/EC geänderten Fassung).
[48] Abschnitt 4 III des irischen Datenschutzgesetzes (in der durch die Richtlinie 2006/24/EC and 2009/136/EC geänderten Fassung).
[49] Abschnitt 4 II lit. a) des irischen Communications (Retention of Data) Act 2011 (vom 26.1.2011).
[50] Abschnitt 4 I, II lit. b) des irischen Datenschutzgesetzes (in der durch die Richtlinie 2006/24/EC and 2009/136/EC geänderten Fassung).
[51] Abschnitt 4 II lit. c) des irischen Datenschutzgesetzes (in der durch die Richtlinie 2006/24/EC and 2009/136/EC geänderten Fassung).
[52] Abschnitt 34 Nr. 1 des italienischen Datenschutzgesetzes (vom 30.6.2003).
[53] Abschnitt 123 Nr. 1 des italienischen Datenschutzgesetzes (vom 30.6.2003).
[54] Annex B Nr. 18 Abschnitt 123 Nr. 1 des italienischen Datenschutzgesetzes (in der Fassung vom 30.6.2003).
[55] Abschnitt 11 Nr. 1 lit. c) und d) des italienischen Datenschutzgesetzes (in der Fassung vom 30.6.2003).
[56] Abschnitt 58 Nr. 3 des italienischen Datenschutzgesetzes (in der Fassung vom 30.6.2003).
[57] Abschnitt 36 des italienischen Datenschutzgesetzes (vom 30.6.2003).
[58] Abschnitt 33 Nr. 1 des italienischen Datenschutzgesetzes (vom 30.6.2003).
[59] Abschnitt 31 Nr. 1 des italienischen Datenschutzgesetzes (vom 30.6.2003).

	Vertraulichkeit	Verfügbarkeit	Inhaltliche Korrektheit	Integrität	Authentizität	Technische Konkretisierung
	Geeignete Maßnahmen zur Gewährleistung der Sicherheit der Dienste und der Integrität von Verkehrsdaten, Standortdaten und der elektronischen Kommunikation gegen jede Form von unerlaubter Nutzung oder unberechtigtem Zugang[60] Berücksichtigung des technologischen Fortschritts, des Risikos und der Art und den jeweiligen Besonderheiten der Verarbeitung[61] Zulässigkeit der Datenverarbeitung abhängig von technischen Spezifikationen in Anhang B zum Gesetz (Vorgaben zu computergestützter Authentifizierung und Autorisierung, Benutzer- und Rechteverwaltung, regelmäßiger Anpassung an geänderte Abläufe, Schutz vor Schadsoftware, Backup-Systemen und jährliche Beschreibung der Sicherheitspolitik)[62] regelmäßige Aktualisierung der Sicherheitsanforderungen[63]					
Lettland	Verarbeitung der Daten nur durch spezielle autorisiertes Personal des TK-Diensteanbieters[64] Löschpflicht[65]					Technische Vorgaben zur Datensicherheit durch das Parlament[66] Technische Vorgaben zur Übermittlung der Daten an die anfragende Behörde durch das Parlament[67]
	Schutz gegen unbeabsichtigte oder unrechtmäßige Zerstörung, Verlust oder Veränderung, oder unrechtmäßige Verarbeitung oder Zugänglichmachung[68] Beschreibung der Sicherheitspolitik[69]					
Litauen	Keine Informationen					
Luxemburg	Zugriff nur für speziell autorisierte Personen[70] Physische Zutrittskontrolle[71] Schutz der Datenträger vor unberechtigten Personen[72] Schutz vor unbefugter Kenntnisnahme gespeicherter Daten[73] Schutz vor unbefugtem Gebrauch des IT-Systems[74]	Schutz der Datenträger vor unberechtigten Personen[77] Schutz vor unbefugter Löschung gespeicherter Daten[78] Backup[79]	Schutz vor unbefugter Eingabe von Daten in das Informationssystem oder Löschung gespeicherter Daten[80]	Schutz der Datenträger vor unberechtigten Personen[81] Schutz vor unbefugter Eingabe von Daten in das Informationssystem oder Veränderung oder Löschung gespeicherter Daten[82] Protokollierung der Datenzugriffe (inkl. der zugreifenden Personen)[83] Schutz vor Veränderung bei	Gewährleistung von Identifikations- und Authentifikationsmechanismen bei der Datenübermittlung an Dritte[85]	Empfehlungen über Best Practices durch die nationale Datenschutzbehörde[86]

[60] Abschnitt 32 Nr. 1 des italienischen Datenschutzgesetzes (vom 30.6.2003).
[61] Abschnitte 31 Nr. 1, 32 Nr. 1 des italienischen Datenschutzgesetzes (vom 30.6.2003).
[62] Annex B des italienischen Datenschutzgesetzes (vom 30.6.2003).
[63] Annex B Nr. 15 ff. Abschnitt 123 Nr. 1 des italienischen Datenschutzgesetzes (vom 30.6.2003).
[64] Abschnitt 71.1 VII des lettischen Telekommunikationsgesetzes (zuletzt geändert am 3.5.2007).
[65] Abschnitt 71.1 VIII des lettischen Telekommunikationsgesetzes (zuletzt geändert am 3.5.2007).
[66] Abschnitt 25 IV des lettischen Telekommunikationsgesetzes (zuletzt geändert am 3.5.2007).
[67] Abschnitt 71.1 IV des lettischen Telekommunikationsgesetzes (zuletzt geändert am 3.5.2007).
[68] Abschnitt 25 IV des lettischen Telekommunikationsgesetzes (zuletzt geändert am 3.5.2007).
[69] Art. 3 I S. 2 Sstr. 3 des luxemburgischen Gesetzes zum Schutz der Privatsphäre in der elektronischen Kommunikation (in der Fassung vom 10.8.2011).
[70] Art. 3 I S. 2 Sstr. 1 des luxemburgischen Gesetzes zum Schutz der Privatsphäre in der elektronischen Kommunikation (in der Fassung vom 10.8.2011).
[71] Art. 23 lit. a) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[72] Art. 23 lit. b) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[73] Art. 23 lit. c) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[74] Art. 23 lit. d) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).

	Vertraulichkeit	Verfügbarkeit	Inhaltliche Korrektheit	Integrität	Authentizität	Technische Konkretisierung
	Zugangskontrolle[75] Schutz vor Kenntnisnahme bei Übermittlung[76]			Übermittlung[84]		
	Geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Dienste[87] Schutz gegen unbeabsichtigte oder unrechtmäßige Zerstörung, Verlust oder zufällige Veränderung und Speicherung, Verarbeitung, Zugriff und unberechtigte oder unrechtmäßige Zugänglichmachung oder Verbreitung[88] Geeignete technische und organisatorische Maßnahmen zum Schutz der Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust, Veränderung, unberechtigte Verbreitung oder Zugänglichmachung, insbesondere wenn die Daten über ein Netzwerk übermittelt werden, und jede andere Form der unrechtmäßigen Verarbeitung[89] Berücksichtigung des Risikos für die Privatsphäre, des Standes der Technik und der Kosten der Durchführung der Maßnahme [90]					
Malta	Keine Informationen					
Niederlande	Schutz der Daten vor unbefugter Kenntnisnahme[91] Beschränkung des Zugangs auf speziell berechtigten Personenkreis[92] Löschpflicht („vernietigen“) unmittelbar am Ende der Speicherfrist[93]	Unverzügliche Beantwortung der Anfragen[94]				Technische Konkretisierung durch Ratsbeschluss[95]
	Geeignete technische und organisatorische Maßnahmen zum Schutz der Daten gegen Zerstörung, Verlust oder Veränderung, unbefugte Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung[96] Geeignete technische und organisatorische Maßnahmen zum Schutz der Daten gegen Verlust oder jede Form der unrechtmäßigen Verarbeitung[97]					

[77] Art. 23 lit. b) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[78] Art. 23 lit. c) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[79] Art. 23 lit. i) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[80] Art. 23 lit. c) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[81] Art. 23 lit. b) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[82] Art. 23 lit. c) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[83] Art. 23 lit. g) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[85] Art. 23 lit. f) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[86] Art. 3 I S. 2 a.E. des luxemburgischen Gesetzes zum Schutz der Privatsphäre in der elektronischen Kommunikation (in der Fassung vom 10.8.2011).
[75] Art. 23 lit. e) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[76] Art. 23 lit. h) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[84] Art. 23 lit. h) des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[87] Art. 3 I S. 1 des luxemburgischen Gesetzes zum Schutz der Privatsphäre in der elektronischen Kommunikation (in der Fassung vom 10.8.2011).
[88] Art. 3 I S. 2 Sstr. 2 des luxemburgischen Gesetzes zum Schutz der Privatsphäre in der elektronischen Kommunikation (in der Fassung vom 10.8.2011).
[89] Art. 22 I des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[90] Art. 23 des luxemburgischen Gesetzes zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (in der Fassung vom 13.8.2002).
[91] Art. 13.5 Nr. 1 des niederländischen Telekommunikationsgesetzes (in der Fassung vom 3.11.2011).
[92] Art. 13.5 Nr. 2 lit. b) des niederländischen Telekommunikationsgesetzes (in der Fassung vom 3.11.2011).
[93] Art. 13.5 Nr. 2 lit. c), Nr. 3 lit. b) des niederländischen Telekommunikationsgesetzes (in der Fassung vom 3.11.2011).
[94] Art. 13.4 Nr. 1 des niederländischen Telekommunikationsgesetzes (in der Fassung vom 3.11.2011).
[95] Art. 13.5 Nr. 4 des niederländischen Telekommunikationsgesetzes (in der Fassung vom 3.11.2011).
[96] Art. 13.5 Nr. 2 lit. a) des niederländischen Telekommunikationsgesetzes (in der Fassung vom 3.11.2011).

	Vertraulichkeit	Verfügbarkeit	Inhaltliche Korrektheit	Integrität	Authentizität	Technische Konkretisierung
	Berücksichtigung: Stand der Technik, Risiken, Kosten, Natur der Daten[98]					
Österreich	Pflicht der Auftraggeber, Dienstleister und ihrer Mitarbeiter zur Geheimhaltung, Übermittlung der Daten nur auf ausdrückliche Anordnung des Arbeitgebers hin[99] Klare Aufgabenverteilung und Regelung von Zutritts- und Zugriffsberechtigungen[100] Zugang zu den Vorratsdaten ausschließlich dazu ermächtigten Personen unter Einhaltung des 4-Augen-Prinzips[101] Übermittlung der Daten in angemessen geschützter Form(technisch anspruchsvolle Verschlüsselung)[102] Pflicht zur Löschung der Vorratsdaten spätestens 1 Monat nach Ablauf der Speicherfrist[103]	Pflicht zur Bereitstellung von Einrichtungen, die zur Auskunft über Vorratsdaten erforderlich sind[104] Speicherung der Daten so, dass sie auf Anfrage hin unverzüglich übermittelt werden können[105] Übertragung in CSV-Format[106]	Protokollierung der Änderungen, Abfragen und Übermittlungen (3 Jahre lange Aufbewahrung der Protokolldaten)[107]	Klare Aufgabenverteilung und Regelung von Zutritts- und Zugriffsberechtigungen[100] Verwendung einer entspr. Übertragungstechnologie zur Sicherstellung der Datenintegrität[108] Protokollierung der Änderungen, Abfragen und Übermittlungen (3 Jahre lange Aufbewahrung der Protokolldaten)[107]	Verwendung einer entspr. Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sicherstellt[108]	Konkretisierung des Sorgfaltsmaßstabs durch Verordnung durch den Bundesminister für Verkehr, Innovation und Technologie[109]
	Unterscheidung der Vorratsdaten von anderen Daten muss möglich sein[110] Geeignete technische und Organisatorische Maßnahmen zum Schutz gegen unrechtmäßige Zerstörung, zufälligen Verlust oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung und Verbreitung[111] Datensicherheitsmaßnahmen zum Schutz gegen zufällige oder unrechtmäßige Zerstörung und vor Verlust, vor unrechtmäßiger Verwendung und unberechtigtem Zugang (inkl. Konkretisierung)[112] Berücksichtigung: Art der verwendeten Daten, Umfang und Zweck der Verwendung, Stand der technischen Möglichkeiten, wirtschaftliche Vertretbarkeit[113]					

[97] Art. 13 des niederländischen Datenschutzgesetzes (in der Fassung 23.11.1999).
[98] Art. 13 des niederländischen Datenschutzgesetzes (in der Fassung 23.11.1999).
[99] § 15 I, II des österreichischen Datenschutzgesetzes 2000 (in der Fassung vom 27.8.2011).
[100] § 14 II Nr. 1, 2, 4, 5, 6 des österreichischen Datenschutzgesetzes 2000 (in der Fassung vom 27.8.2011).
[101] § 102c I S. 3 Telekommunikationsgesetzes (in der Fassung vom 18.5.2011).
[102] §§ 94 IV, 102b III des österreichischen Telekommunikationsgesetzes (in der Fassung vom 18.5.2011).
[103] § 102a VIII des österreichischen Telekommunikationsgesetzes (in der Fassung vom 18.5.2011).
[104] § 94 I des österreichischen Telekommunikationsgesetzes (in der Fassung vom 18.5.2011).
[105] § 102b II des österreichischen Telekommunikationsgesetzes (in der Fassung vom 18.5.2011).
[106] § 94 IV des österreichischen Telekommunikationsgesetzes (in der Fassung vom 18.5.2011).
[107] § 14 II Nr. 7, V des österreichischen Datenschutzgesetzes 2000 (in der Fassung vom 27.8.2011) und § 102c I S. 4, II-VI des österreichischen Telekommunikationsgesetzes (in der Fassung vom 18.5.2011).
[108] § 94 IV des österreichischenTelekommunikationsgesetzes (in der Fassung vom 18.5.2011).
[109] § 94 IV des österreichischen Telekommunikationsgesetzes (in der Fassung vom 18.5.2011).
[110] § 102c I S. 1 des österreichischen Telekommunikationsgesetzes (in der Fassung vom 18.5.2011).
[111] § 102c I S. 2 des österreichischen Telekommunikationsgesetzes (in der Fassung vom 18.5.2011).
[112] §§ 95 I des österreichischen Telekommunikationsgesetzes (in der Fassung vom 18.5.2011) i.V.m. § 14 des österreichischen Datenschutzgesetzes 2000 (in der Fassung vom 27.8.2011).

	Vertraulichkeit	Verfügbarkeit	Inhaltliche Korrektheit	Integrität	Authentizität	Technische Konkretisierung
Polen	Verpflichtung zur Gewährleistung der Vertraulichkeit von Verkehrsdaten[114] mit der unter Berücksichtigung von technischen und wirtschaftlichen Gegebenheiten erforderlichen Sorgfalt[115] Geeignete technische und organisatorische Maßnahmen, um Zugang auf spezielle autorisierte Mitarbeiter zu beschränken[116]	Bereitstellung der Daten über ein elektronisches Kommunikationsnetz, sofern nichts anders in besonderen Vorschriften geregelt[117]				
	Schutz der Daten gegen zufällige oder unrechtmäßige Zerstörung, Verlust oder Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung[118] Technische und organisatorische Maßnahmen, um die Sicherheit der Nachrichtenübertragung in Bezug auf die von ihn erbrachten Dienste zu gewährleisten[119]					
Portugal	Keine Informationen					
Slowakei	Umfassende Geheimhaltungspflicht in Bezug auf personenbezogene Daten[120]	Pflicht zur unverzüglichen Bereitstellung der Daten auf Anfrage[121]				
	4 Grundsätze aus Art. 7 VDSRL wortlautgetreu umgesetzt[122] Geeignete technische und organisatorische Maßnahmen um die Sicherheit ihrer Netze und Dienste zu gewährleisten (Berücksichtigung: Stand der Technik, Implementierungskosten, Risiko)[123] Geeignete technische und organisatorische Maßnahmen zum Schutz gegen zufällige oder unrechtmäßige Beschädigung oder Zerstörung, zufälligen Verlust oder Änderung, unautorisierter Zugang und Verbreitung (Berücksichtigung: Stand der Technik, Risiko, Schutzwürdigkeit und Bedeutung der verarbeiteten Daten)[124] Detaillierte Organisationsvorgaben zur Ermittlung des Umfangs und der Art der technischen und organisatorischen Maßnahmen im Rahmen („**Security Project**")[125]					
Slowenien	Explizite Löschpflicht ("destroy")[126] Verschwiegenheitspflicht der die Daten verarbeitenden Mitarbeiter[127] Schutz der Räumlichkeiten, Geräte			Schutz der Räumlichkeiten, Geräte und Systeme[134] Schutz der Software-Anwendungen[135]		

[113] § 14 I, II a.E. des österreichischen Datenschutzgesetzes 2000 (in der Fassung vom 27.8.2011).
[114] Art. 160 I des polnischen Kommunikationsgesetzes (in der Fassung vom 1.1.2010).
[115] Art. 180a I Nr. 3 des polnischen Telekommunikationsgesetzes (in der Fassung vom 1.1. 2010).
[116] Art. 180e des polnischen Telekommunikationsgesetzes (in der Fassung vom 1.1.2010).
[117] Art. 180a VII des polnischen Telekommunikationsgesetzes (in der Fassung vom 1.1.2010).
[118] Art. 180a I Nr. 3 des polnischen Telekommunikationsgesetzes (in der Fassung vom 1.1. 2010).
[119] Art. 175 I des polnischen Telekommunikationsgesetzes (in der Fassung vom 1.1.2010).
[120] Abschnitt 18 des slowakischen Datenschutzgesetzes (zuletzt geändert durch Act No. 90/2005 Coll.).
[121] § 59a VIII des slowakischen Telekommunikationsgesetzes (in der Fassung vom 18.3.2010).
[122] § 59a XI des slowakischen Telekommunikationsgesetzes (in der Fassung vom 18.3.2010).
[123] § 57 I des slowakischen Telekommunikationsgesetzes (in der Fassung vom 18.3.2010).
[124] Abschnitt 15 I des slowakischen Datenschutzgesetzes (zuletzt geändert durch Act No. 90/2005 Coll.).
[125] Abschnitte 15 II und 16 des slowakischen Datenschutzgesetzes (zuletzt geändert durch Act No. 90/2005 Coll.).
[126] Art. 107a VI des slowenischen Telekommunikationsgesetzes (in der Fassung vom 1.2.2007).
[127] Art. 24 IV des slowenischen Datenschutzgesetzes (in der Fassung vom 15.7.2004)

	Vertraulichkeit	Verfügbarkeit	Inhaltliche Korrektheit	Integrität	Authentizität	Technische Konkretisierung
	und Systeme[128] Schutz der Software-Anwendungen[129] Schutz vor unbefugtem Zugriff während Übertragung[130] Gewährleistung einer effektiven Methode der Blockierung, Zerstörung, Löschung oder Anonymisierung[131] Protokollierung (inkl. der zugreifenden Person)[132] Beschränkung des zugriffsberechtigten Personenkreises[133]			Protokollierung (inkl. der zugreifenden Person)[136]		
	Geeignete technische und organisatorische Maßnahmen zum Schutz der gespeicherten Daten gegen Zerstörung, Verlust oder Änderung, unbefugte oder unrechtmäßige Speicherung, Verarbeitung, Zugang oder Verbreitung[137] Technische, organisatorische und logische Maßnahmen zum Schutz personenbezogener Daten gegen zufällige und vorsätzlich unbefugte Zerstörung, Veränderung, Verlust und unbefugte Verarbeitung[138] Berücksichtigung: Risiko und Natur der Daten[139]					
Spanien	Beschränkung des zugriffsberechtigten Personenkreises[140] Pflicht zur Löschung der von den Ermittlungsbehörden abgefragten Daten, sobald diese nicht mehr für die Ermittlungen benötigt werden[141]		Daten müssen genau, aktuell und inhaltlich korrekt sein[144]	Integrität der Daten[145]		

[134] Art. 24 I Nr. 1 des slowenischen Datenschutzgesetzes (in der Fassung vom 15.7.2004).
[135] Art. 24 I Nr. 2 des slowenischen Datenschutzgesetzes (in der Fassung vom 15.7.2004).
[128] Art. 24 I Nr. 1 des slowenischen Datenschutzgesetzes (in der Fassung vom 15.7.2004).
[129] Art. 24 I Nr. 2 des slowenischen Datenschutzgesetzes (in der Fassung vom 15.7.2004).
[130] Art. 24 I Nr. 3des slowenischen Datenschutzgesetzes (in der Fassung vom 15.7.2004).
[131] Art. 24 I Nr. 4 des slowenischen Datenschutzgesetzes (in der Fassung vom 15.7.2004).
[132] Art. 24 INr. 5 des slowenischen Datenschutzgesetzes (in der Fassung vom 15.7. 2004).
[133] Art. 25 II des slowenischen Datenschutzgesetzes (in der Fassung vom 15.7.2004).
[136] Art. 24 INr. 5 des slowenischen Datenschutzgesetzes (in der Fassung vom 15.7.2004).
[137] Art. 107c I des slowenischen Telekommunikationsgesetzes (in der Fassung vom 1.2.2007).
[138] Art. 24 I des slowenischen Datenschutzgesetzes (in der Fassung vom 15.7.2004).
[139] Art. 24 III des slowenischen Datenschutzgesetzes (in der Fassung vom 15.7.2004).
[140] Art. 8 Nr. 1 des spanischen Gesetzes zur Aufbewahrung von Daten im Bereich elektronischer Kommunikationsnetze (in der Fassung vom 19.10.2007).
[141] Art. 8 Nr. 2 des spanischen Gesetzes zur Aufbewahrung von Daten im Bereich elektronischer Kommunikationsnetze (in der Fassung vom 19.10.2007) und Art. 22 Nr. 4 des spanischen Datenschutzgesetzes (in der Fassung vom 14.12.1999).

	Vertraulichkeit	Verfügbarkeit	Inhaltliche Korrektheit	Integrität	Authentizität	Technische Konkretisierung
	Verschwiegenheitspflicht der die Daten verarbeitenden Mitarbeiter[142] Löschpflicht[143]					
	Technische und organisatorische Maßnahmen zum Schutz der Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung[146] Geeignete technische und organisatorische Maßnahmen zum Schutz der Daten gegen Veränderung, Verlust oder unberechtigten Zugriff[147] Berücksichtigung: Stand der Technik, Risiko, Natur der Daten[148] Gewährleistung der Sicherheit der Rechenzentren, Gebäude, Systeme und Anwendungen[149]					
Ungarn	Daten müssen gegen unbefugten Zugriff geschützt werden[150] Technische und organisatorische Maßnahmen zur Gewährleistung der Vertraulichkeit[151] Anonymisierung, sofern Daten nicht mehr für Zweck gebraucht werden[152]	Daten müssen berechtigten Personen zur Verfügung stehen[153]	Authentizität der verwalteten Daten ist zu gewährleisten[154] Richtigkeit, Vollständigkeit und Aktualität der Daten[155]	Konsistenz der Daten ist zu gewährleisten[156]		
	Gewährleistung der Datensicherheit Technische und organisatorische Maßnahmen um gesetzliche Anforderungen im Hinblick auf Datenschutz zu erfüllen[157] Berücksichtigung: Risiko[158] Schutz der Daten gegen unbefugten Zugang, Veränderung, Übermittlung, Zugänglichmachung, Löschung oder Zerstörung und gegen zufällige Zerstörung oder Beschädigung (explizit auch bei deren Übermittlung)[159] Erfroderlichkeit eines Benutzer- und Rechtemanagements[160]					

[144] Art. 4 Nr. 3, 4 des spanischen Datenschutzgesetzes (in der Fassung vom 14.12.1999).
[145] Art. 9 Nr. 2 des spanischen Datenschutzgesetzes (in der Fassung vom 14.12.1999).
[142] Art. 10 des spanischen Datenschutzgesetzes (in der Fassung vom 14.12.1999).
[143] Art. 4 Nr. 5 des spanischen Datenschutzgesetzes (in der Fassung vom 14.12.1999).
[146] Art. 8 Nr. 1 des spanischen Gesetzes zur Aufbewahrung von Daten im Bereich elektronischer Kommunikationsnetze (in der Fassung vom 19.10.2007).
[147] Art. 9 Nr. 1 des spanischen Datenschutzgesetzes (in der Fassung vom 14.12.1999).
[148] Art. 9 Nr. 1 des spanischen Datenschutzgesetzes (in der Fassung vom 14.12.1999).
[149] Art. 9 Nr. 2 des spanischen Datenschutzgesetzes (in der Fassung vom 14.12.1999).
[150] Art. 2 I lit. d) des Dekrets 226/2003 der ungarischen Regierung (in der Fassung vom 13.12.2003).
[151] Art. 10 I des ungarischen Datenschutzgesetzes (in der Fassung vom 17.11.1992).
[152] Art. 10 I lit. c) des ungarischen Datenschutzgesetzes (in der Fassung vom 17.11.1992).
[153] Art. 2 I lit. a) des Dekrets 226/2003 der ungarischen Regierung (in der Fassung vom 13.12.2003).
[154] Art. 2 I lit. b) des Dekrets 226/2003 der ungarischen Regierung (in der Fassung vom 13.12.2003).
[155] Art. 7 I lit. b) des ungarischen Datenschutzgesetzes (in der Fassung vom 17.11.1992).
[156] Art. 2 I lit. c) des Dekrets 226/2003 der ungarischen Regierung (in der Fassung vom 13.12.2003).
[157] Art. 10 I des ungarischen Datenschutzgesetzes (in der Fassung vom 17.11.1992).
[158] Art. 2 II des Dekrets 226/2003 der ungarischen Regierung (in der Fassung vom 13.12.2003).
[159] Art. 10 II des ungarischen Datenschutzgesetzes (in der Fassung vom 17.11.1992).
[160] Art. 7 II des ungarischen Datenschutzgesetzes (in der Fassung vom 17.11.1992).

Einzelstaatliche Normen zur Umsetzung der sicherheitstechnischen und organisatorischen Vorgaben aus Art. 7 VDSRL

(mit Ausnahme von Griechenland, Litauen, Malta und Portugal)

Ohne Anspruch auf Vollständigkeit!

Übersicht

BULGARIEN ..... **XXXVIII**

Artikel 243 I, 250a, 250d, 250e, 252, 261a, 261b des Gesetzes über die elektronische Kommunikation (zuletzt geändert am 9.4.2010) XXXVIII

Artikel 23, 25 des Gesetzes zum Schutz personenbezogener Daten (zuletzt geändert am 5.6.2009) XL

DÄNEMARK ..... **XLI**

Abschnitte 41 und 42 des Gesetzes über die Verarbeitung personenbezogener Daten (zuletzt geändert am 12.6.2009) XLI

Abschnitt 31 der Durchführungsverordnung Nr. 714 über die Bereitstellung elektronischer Kommunikationsnetze und -dienste vom 26.6.2008 XLI

ENGLAND ..... **XLII**

Artikel 6 der Verordnung über die Vorratsdatenspeicherung (in der Fassung vom 6.4.2009) XLII

ESTLAND ..... **XLII**

§§ 101, 102 des Gesetzes über die elektronische Kommunikation (zuletzt geändert am 24.1.2007) XLII

§ 6 des Gesetzes über die Verarbeitung personenbezogener Daten (in der Fassung vom 1.5.2004) XLIII

Artikel 122 Absatz 2 der Strafprozessordnung (zuletzt geändert am 15.6.2005) XLIII

FINNLAND ..... **XLIV**

Abschnitte 2, 14a, 14b, 15, 16, 19, 20 Absatz 3 des Gesetzes über die elektronische Kommunikation (zuletzt geändert am 28.4.2011) XLIV

FRANKREICH ..... **XLVI**

Artikel 11 des Gesetzes Nr. 78-17 vom 6. Januar 1978 (zuletzt geändert am 29.3.2011) XLVI

Artikel D98-5, L34-1 Code des postes et des communications électroniques XLVIII

IRLAND ..... **L**

Abschnitte 4 und 12 des Communications (Retention of Data) Act 2011 (in der Fassung vom 26.1.2011) L

Abschnitte 4 und 5 des Datenschutzgesetzes (in der durch die Richtlinie 2006/24/EC and 2009/136/EC geänderten Fassung) L

ITALIEN ..... **LII**

Abschnitte 31, 32, 33, 34, 35, 36, 58, 123 und Annex B des Datenschutzgesetzes vom 30.6.2003 LII

LETTLAND ..... **LVII**

Abschnitte 19, 25 und 71.1 des Gesetzes über die elektronische Kommunikation (zuletzt geändert am 3.5.2007) LVII

LUXEMBURG LVIII

Art. 2, 3 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques (in der Fassung vom 10.8.2011) LVIII

Art. 22 et 23 de loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (in der Fassung vom 13.8.2002) LIX

Art. 67-1 Code d'instruction criminelle (in der Fassung vom 25.11.2011) LX

NIEDERLANDE LX

Artikel 13.2, 13.4, Telecommunicatiewet (in der Fassung vom 3.11.2011) LX

Artikel 13 Personal Data Protection Act (in der Fassung vom 23.11.1999) LXII

ÖSTERREICH LXII

§§ 94, 95, 99, 102c des Telekommunikationsgesetzes (zuletzt geändert am 18.5.2011) LXII

§ 14, 15 des Datenschutzgesetzes 2000 (in der Fassung vom 27.8.2011) LXIV

POLEN LXVI

Artikel 180a und 180e des Telekommunikationsgesetzes (in der Fassung vom 1.1.2010) LXVI

SLOWAKEI LXVII

§§ 57 I, 59a Gesetz über die elektronische Kommunikation (in der Fassung vom 18.3.2010) LXVII

Abschnitte 15 und 16 des Datenschutzgesetzes (zuletzt geändert durch Act No. 90/2005 Coll.) LXVII

SLOWENIEN LXIX

Artikel 107a Absatz 6 und Artikel 107c des Gesetzes über die elektronische Kommunikation (in der Fassung vom 1.2.2007) LXIX

Artikel 24, 25 des Datenschutzgesetzes (in der Fassung vom 15.7.2004) LXX

SPANIEN LXXI

Articulo 8 Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (in der Fassung vom 19.10.2007) LXXI

Articulos 4, 9, 22 und 23 Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (in der Fassung vom 14.12.1999) LXXI

UNGARN LXXIII

Article 157 of Act C/2003 on electronic communications (in der Fassung vom 24.11.2003) LXXIII

Article 2 Government Decree 226/2003 (in der Fassung vom 13.12.2003) LXXIII

Article 7, 10 Act LXIII/1992 on Data Protection (in der Fassung vom 17.11.1992) LXXIII

Bulgarien

Artikel 243 I, 250a, 250d, 250e, 252, 261a, 261b des Gesetzes über die elektronische Kommunikation (zuletzt geändert am 9.4.2010)

(Quelle: http://www.crc.bg/files/_en/LAW_ON_ELECTRONIC_COMMUNICATIONS.pdf)

Art. 243
(1) Undertakings, providing public electronic communications services shall be obligated to take the necessary technical and organizational measures, and if necessary in cooperation with the undertakings, providing public electronic communications networks, to safeguard security of the electronic communications networks and/or services.
…

Art. 250a
(1) The undertakings providing public electronic communication networks and/or services, shall store for a period of 12 months data, generated or processed in the process of their activity, required for:
1. tracing and identification of the source of the connection;
2. identification of the direction of the connection;
3. identification of the date, time and duration of the connection;
4. identification of the type of the connection;
5. identification of the user's end electronic communication facility or of the one, presented as his/her end facility;
6. setting of used cells identifier.
(2) The information under Para 1 shall be stored for the purpose of discovering and investigating severe crimes and crimes under Art. 319a - 319f of the Penal Code, as well as for searching persons.
(3) Other data, including data, disclosing the content of communications, may not be stored pursuant to this procedure.
(4) Undertakings, providing public electronic communication networks and/or services shall be obliged to destroy the data after expiration of the term of par. 1.
(5) The preservation for a period of up to 6 months from the date of providing information that has been accessed and stored may be required by the head of the requesting authority from the providing undertaking.
(6) The information under Para 1 shall be processed and stored in compliance with the requirements of the Law on Protection of the Personal Data.

Art. 250d
(1) The undertakings providing public electronic communication networks and/or services shall be obliged to ensure that the order under Art. 250c, Para 1 and Art. 251, Para 2 can be received 24 hours per day, 7 days per week.
(2) The heads of the undertakings providing public electronic communication networks and/or services shall submit to the Communications Regulatory Commission a list indicating:
1. a current address on which to receive the order under Art. 250c, Para 1 and Art. 251, Para 2;
2. a name, second name, surname and position of the authorised officials who shall receive the orders under Art. 250c, Para 1 and Art. 251, Para 2, as well as a telephone number to contact them; where the data is changed, the Communications Regulatory Commission shall be notified in writing within 24 hours and its Chairman shall immediately make the lists available to the heads of the authorities under Art/ 250b, Para 1.

Art. 250e
(1) The undertakings providing public electronic communication networks and/or services shall perform an inquiry about the information under Art. 250a, Para 1 after submission of an access order. The submitted access order shall be entered into a special non-public register.
(2) Within shortest terms, but no more than 72 hours from submission of the access order under Art. 250c, Para 1 and Art. 251, Para 2 to the undertaking, the undertakings providing public electronic communication networks and/or services shall send the information to the official under Art. 250c, Para 2, Item 3. The Minister of Interior or official authorised by him in writing may specify a concrete term for sending the information.

(3) Inquiries about the information under Art. 250a, Para 1 in the undertakings providing public electronic communication networks and/or services may be carried out only by officials authorised in writing by the head of the undertaking.
(4) After being drawn up the inquiry shall be signed by the head of the undertaking, providing public electronic communication networks and/or services, or by an official authorised in writing by him. The inquiry shall be entered into a special register and shall be sent to an official specified in the order to be provided the information.
(5) Where possible the order of the judge and the inquiry under Para 4 shall be sent electronically in compliance with the requirements of the Law on the Electronic Management and the Law on the Electronic Document and the Electronic Signature.

Art. 252
(1) Processing of traffic data shall be carried out by officials authorised by the undertakings providing electronic communications services, who are in charge of:
1. the administration of traffic data and data under Art. 248, Para 2, Item 2;
2. end-users inquiries,
3. identification of misuse;
4. marketing of electronic communications services;
5. provision of value added services, requiring further processing of traffic data or location data, different from the traffic data, required for the transfer of communication or for its charging
(2) Officials shall have access only to the information, required for the respective activity.

Art. 261a
(1) The Commission for Protection of Personal Data shall be a supervisory authority for security of the information retained under Art. 250a, Para 1.
(2) As a supervisory authority the Commission for Protection of Personal Data shall supervise the activity of the undertakings providing public electronic communication networks and/or services for compliance with the following rules for retention of the information under Art. 250a, Para 1 in order to guarantee their protection and security:
1. the retained information shall be of the same quality and shall be subject to the same security and protection as the corresponding information in the network;
2. provision of appropriate technical and organizational measures to protect the information of accidental or illegal destruction, accidental loss or change, or unauthorized or illegal retention, processing, access or disclosure;
3. provision of appropriate technical and organizational measures to guarantee access to the data only to specially authorised staff;
4. the information, except that provided to the competent authorities and retained by them, shall be destroyed at the end of the retention period, except in the cases explicitly specified in the law.
(3) For carrying out the activity under Para 2 the Commission for Protection of Personal Data shall be entitled to:
1. request within its competence information from the undertakings providing public electronic communication networks and/or services;
2. give mandatory instructions subject to immediate performance.
(4) Annually, by 31 March, the undertakings providing public electronic communication networks and/or services shall provide to the Commission for Protection of Personal Data as a supervisory authority statistical information about:
1. the cases of provided information to the competent authorities under Art. 250b, Para 1 and Art. 250c, Para 4;
2. the time that has expired since the initial date of retention to the date of the request of the information by the competent authorities;
3. the cases, where the information request could not be answered.
(5) The Commission for Protection of Personal Data shall provide annually to the National Assembly and to the European Commission summarised information under Para 4 within two months from receiving it.
(6) The summarised statistical information under Para 4 and 5 shall not contain personal data.

Art. 261b
(1) The National Assembly, through a commission specified in its structural and activity regulations, shall carry out parliamentary control and supervision of the procedures of permission and access to the information under Art. 250a, Para 1, as well as for protection of the rights and freedoms of the citizens against illegal access to such information.

(2) For performing its functions the commission under Para 1 shall have the right:
1. to request within its competence information from the authorities under Art. 250b, Para 1, from the undertakings providing public electronic communication networks and/or services and from the Commission for Protection of Personal Data;
2. to check the procedures and methods of retention of information under Art. 250a, Para 1, of the requests and orders, as well as the procedures for destruction of the information under Art. 250a, Para 1 and Art. 250f;
3. to access the premises of the authorities under Art. 250b, Para 1 and of the undertakings providing public electronic communication networks and/or services;
4. to draw up annual reports of the conducted checks and to extend proposals for improvement of the procedures for retention and processing of the information under Art. 250a, Para 1.
(3) The Ministry of Interior, the Ministry of Defense, the State Agency „National Security", the National Intelligence Service and the Chief Prosecutor shall draw up by 31 March every year summarised statistical information of the submitted requests, the issued judicial orders, the received and the destroyed inquiries regarding information under Art. 250a, Para 1, which shall be submitted to the commission under Para 1.
(4) In cases of finding unlawful use, retention or destruction of information under Art. 250a, Para 1 the commission shall notify of the violations the competent prosecution authorities and the heads of the authorities under Art. 250b, Para 1 and of the undertakings providing public electronic communication networks and/or services. The heads of the authorities and the undertakings shall be obliged to notify in due time the commission of the measures that have been undertaken to terminate the violations.
(5) The commission under Para 1 shall notify ex officio the citizens of any requested or granted illegal access to information under Art. 250a, Para 1 regarding them.
(6) The citizens shall not be notified if thus the achievement of the purposes under Art. 250a, Para 2 or Art. 250c, Para 4 can be endangered.
Art. 262. For all matters not covered by this chapter concerning natural persons the provisions of the Law for Protection of the Personal Data shall apply.

Artikel 23, 25 des Gesetzes zum Schutz personenbezogener Daten (zuletzt geändert am 5.6.2009)

(Quelle: http://www.aip-bg.org/pdf/pdpa.pdf)

Art. 23
(1) The personal data controller shall take appropriate technical and organisational measures to protect data against accidental or unlawful destruction, or against accidental loss, unauthorised access, alteration or dissemination, and against other unlawful forms of processing.
(2) The data controller shall take special protection measures when processing involves the transmission of data by electronic means.
(3) The measures referred to in para. (1) and para. (2) shall take into account the modern technological achievements and ensure a level of security adequate to the risks related to processing, and the nature of the data to be protected.
(4) The measures referred to in para. (1) and para. (2) shall be determined in an instruction issued by the personal data controller.
(5) The Commission shall specify in an ordinance the minimum level of technical and organizational measures, as well as the admissible type of protection. Such ordinance shall be published in the State Gazette.

Art. 25
(1) After the achievement of the purpose of personal data processing, the data controller shall be required:
1. either to destroy the data, or
2. transfer them to another data controller by preliminary notification to the Commission, if such transfer is specified in a law and the purposes of processing are identical.

Dänemark

Abschnitte 41 und 42 des Gesetzes über die Verarbeitung personenbezogener Daten (zuletzt geändert am 12.6.2009)

(Quelle: http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/)

41.
(1) Individuals, companies etc. performing work for the controller or the processor and who have access to data may process these only on instructions from the controller unless otherwise provided by law or regulations.
(2) The instruction mentioned in subsection (1) may not restrict journalistic freedom or impede the production of an artistic or literary product.
(3) The controller shall implement appropriate technical and organizational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in this Act. The same shall apply to processors.
(4) As regards data which are processed for the public administration and which are of special interest to foreign powers, measures shall be taken to ensure that they can be disposed of or destroyed in the event of war or similar conditions.
(5) The Minister of Justice may lay down more detailed rules concerning the security measures mentioned in subsection (3).

42.
(1) Where a controller leaves the processing of data to a processor, the controller shall make sure that the processor is in a position to implement the technical and organizational security measures mentioned in section 41 (3) to (5), and shall ensure compliance with those measures.
(2) The carrying out of processing by way of a processor must be governed by a written contract between the parties. This contract must stipulate that the processor shall act only on instructions from the controller and that the rules laid down in section 41 (3) to (5) shall also apply to processing by way of a processor. If the processor is established in a different Member State, the contract must stipulate that the provisions on security measures laid down by the law in the Member State in which the processor is established shall also be incumbent on the processor.

Abschnitt 31 der Durchführungsverordnung Nr. 714 über die Bereitstellung elektronischer Kommunikationsnetze und -dienste vom 26.6.2008

(Quelle: http://en.itst.dk/telecom-internet-regulation/filarkiv-obligations-for-suppliers/executive-order-on-the-provision-of-electronic-communications-networks-and-services)

31.
(1) To ensure network security, providers of public electronic communications networks or services shall take appropriate technical and organisational measures to safeguard the security of their services. If necessary, this shall be undertaken in conjunction with the owner or provider of the public electronic communications network in question.
(2) Providers of public electronic communications networks or services shall inform subscribers of any special risks of a breach of the security of the network. The providers shall also give information about the possibility of preventing such breach and the costs involved.

England

Artikel 6 der Verordnung über die Vorratsdatenspeicherung (in der Fassung vom 6.4.2009)

(Quelle: http://www.legislation.gov.uk/uksi/2009/859/pdfs/uksi_20090859_en.pdf)

6. Data protection and data security
(1) Public communications providers must observe the following principles with respect to data retained in accordance with these Regulations—
(a) the retained data must be of the same quality and subject to the same security and protection as those data on the public electronic communications network;
(b) the data must be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
(c) the data must be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;
(d) except in the case of data lawfully accessed and preserved, the data retained solely in accordance with these Regulations must be destroyed at the end of the retention period.
(2) It is the duty of the Information Commissioner, as the Supervisory Authority designated for the purposes of Article 9 of the Data Retention Directive, to monitor the application of the provisions of these Regulations with respect to the security of stored data.
(3) As regards the destruction of data at the end of the retention period—
(a) the duty of a public communications provider is to delete the data in such a way as to make access to the data impossible; and
(b) it is sufficient for a public communications provider to make arrangements for the operation of so deleting data to take place at such monthly or shorter intervals as appear to the provider to be convenient.

8. Storage requirements for retained data
The data retained in pursuance of these Regulations must be retained in such a way that it can be transmitted without undue delay in response to requests.

Estland

§§ 101, 102 des Gesetzes über die elektronische Kommunikation (zuletzt geändert am 24.1.2007)

(Quelle: http://www.legaltext.ee/text/en/X90001K2.htm)

§ 101 - Security requirement
(1) A communications undertaking must guarantee the security of a communications network and prevent third persons from accessing the data specified in subsection 102 (1) of this section without legal grounds.
(2) If clear and present danger exists to the security of the communications network, the communications undertaking shall immediately inform the subscriber of such danger in a reasonable manner and, if elimination of the danger by the efforts of the undertaking is impossible, also of possible means to combat the threat and of any costs related thereto.

§ 102 - General principles of data protection

(1) A communications undertaking is required to maintain the confidentiality of all information which becomes known thereto in the process of provision of communications services and which concerns subscribers as well as other persons who have not entered into a contract for the provision of communications services but who use communications services with the consent of a subscriber; above all, the following data must be protected:
1) specific data of using communications services;
2) the content and format of messages transmitted through the communications network;
3) information concerning the time and manner of transmission of messages.
(2) The information specified in subsection (1) of this section may be disclosed only to the relevant subscriber and, with the consent of the subscriber, to third persons, except in the cases specified in §§ 112, 113 and 1141 of this Act. A subscriber has the right to withdraw his or her consent at any time.
(3) A communications undertaking may process the information provided for in subsection (1) of this section if the undertaking notifies the subscriber, in a clear and unambiguous manner, of the purposes of processing the information, and gives the subscriber an opportunity to refuse the processing.
(4) The obligation of a communications undertaking specified in subsection (3) of this section does not restrict the right of the undertaking to collect and process, without the consent of a subscriber, information which must be processed for the purposes of recording the transactions carried out in the conduct of business activities and for other business-related exchange of information. In addition to the above, the restriction provided in subsection (3) of this section does not limit the right of a communications undertaking to store or process data without the consent of a subscriber if the sole purpose of such activity is the provision of services through the communications network, or if such activity is necessary for the provision of the Information Society services defined by the Information Society Services Act which are directly requested for by the subscriber.

§ 6 des Gesetzes über die Verarbeitung personenbezogener Daten (in der Fassung vom 1.5.2004)

(Quelle: http://www.legaltext.ee/text/en/X70030.htm)

§ 6. Principles of processing of personal data
In the processing of personal data, chief processors and authorised processors of personal data are required to take guidance from the following principles:
1) the principle of legality – personal data may be collected in an honest and legal manner;
2) the principle of purposefulness – personal data may be collected only for specified and legitimate purposes and personal data shall not be processed in a manner which fails to comply with the purposes of data processing;
3) the principle of minimality – personal data may be collected only to the extent which is necessary for the purposes for which they are collected;
4) the principle of restriction on use – personal data may be used for other purposes only with the consent of the data subject or with the permission of a competent body;
5) the principle of data quality – personal data shall be kept up to date, be complete and necessary for the given purpose of data processing;
6) the principle of security – security measures to prevent the involuntary or unauthorised alteration, disclosure or destruction of personal data shall be applied in order to protect the data;
7) the principle of individual participation – a data subject shall be notified of data collected thereon, access to data pertaining to the data subject shall be ensured to him or her and the data subject has the right to demand the rectification of inaccurate or misleading data.

Artikel 122 Absatz 2 der Strafprozessordnung (zuletzt geändert am 15.6.2005)

(Quelle: http://www.legaltext.ee/text/en/X60027K5.htm)

§ 122. Storage and destruction of data recordings collected by surveillance activities
(1) The photographs, films, audio and video recordings and other data recordings necessary for the adjudication of a criminal matter and made in the course of surveillance activities shall be stored in the criminal file or together with the criminal matter. The rest of the materials on surveillance activities shall be stored in a surveillance file.

(2) If preservation of a data recording made in the course of surveillance activities and added to a criminal file is not necessary, the person subject to the surveillance activities or any other person whose private or family life was violated by such activities may request destruction of the data recording after the entry into force of the court judgment.
(3) A body which conducted surveillance activities destroys a data recording at the request of a Prosecutor's Office and on the basis of an order of a preliminary investigation judge of a court which granted permission for the surveillance activities and in the presence of the prosecutor and the preliminary investigation judge.
(4) A report shall be prepared on the destruction of a data recording and included in the criminal file.

Finnland

Abschnitte 2, 14a, 14b, 15, 16, 19, 20 Absatz 3 des Gesetzes über die elektronische Kommunikation (zuletzt geändert am 28.4.2011)

(Quelle: http://www.finlex.fi/fi/laki/kaannokset/2004/en20040516.pdf)

Section 2 - Definitions
13) ***information security*** means the **administrative and technical measures** taken to ensure that data is **only accessible by those who are entitled to use** it, that data can **only be modified by those who are entitled to do so**, and that **data systems can be used by those who are entitled to use them**;

Section 14a - Obligation to store data for the purposes of the authorities
(1) Notwithstanding the provisions of this Chapter concerning the processing of identification data, a service operator obliged to submit a telecommunications notification shall ensure, under the conditions prescribed below, that data referred to in Article 5 of the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC are retained for a period of 12 months from the date of the communication. Such data may be used only for the purposes of investigating, solving and considering charges for criminal acts referred to in Chapter 5 a(3)(1) of the Coercive Measures Act (450/1987).
(2) The retention obligation applies to data related to:
1) a service operator's telephone service or additional service through a fixed network, telephone service, additional service, SMS service, EMS service or multimedia service through a mobile network;
2) Internet connection service provided by a service operator;
3) e-mail service provided by a service operator;
4) Internet telephony service provided by a service operator;
5) a call for which a connection has been established but the call remains unanswered or is prevented from being connected due to network management measures.
(3) The retention obligation does not apply to the contents of a message or identification data generated through the browsing of websites.
(4) A requirement for the retention obligation is that the data is available and generated or processed in connection with publicly available communications services provided on the basis of this Chapter or the provisions of the Personal Data Act.
(5) Further provisions on a more specific definition of data under the retention obligation may be issued by Government decree.
(6) Technical details of data under the retention obligation are defined in a Finnish Communications Regulatory Authority regulation.

Section 14b - Obligations and procedures for processing data retained for the purposes of the authorities
(1) A service operator under the retention obligation shall discuss the implementation and application of data retention with the Ministry of the Interior in order to ensure that all data considered necessary by the authorities will be retained**. If no consensus is reached on the implementation of data retention, the**

service operator decides on the technical implementation of the retention. The implementation shall follow the principles of cost-efficiency and consider the business needs of the service operator, the technical features of the systems, and the needs of the authority paying for the costs for the retention. Data should be retained in such a way as to avoid the same data being retained by several service operators. **It must be ensured that the data retained can be transmitted to the authorities entitled to it without undue delay.** A service operator under the retention obligation shall, together with a network operator if necessary, ensure that the obligation is met in such a way that the available data referred to in section 14 a processed by the network operator in providing the service operator's service shall be retained. A service operator under the retention obligation shall ensure that information about data retention and its purposes is available to the subscriber.
(2) Provisions on compensation for costs incurred by fulfilling the retention obligation and preparing for it are laid down in section 98 of the Communications Market Act. Provisions on retaining data for the purpose of investigating a single crime are laid down in Chapter 4(4 b and c) of the Coercive Measures Act.
(3) Further provisions on meeting the retention obligation may be given by Government decree.
(4) The Finnish Communications Regulatory Authority may issue further orders on the technical implementation of the retention obligations.

Section 15 - Saving information on processing
(1) A telecommunications provider **shall save detailed event log information on any processing of identification data**. This event information must show the **time and duration of the processing** and the **person performing the processing**. The event information shall be stored for **two years** from the date on which it was saved.
(2) The Finnish Communications Regulatory Authority may issue further regulations on the technical implementation of the saving and storing referred to in subsection 1.

Section 16 - Processing and disclosure of location data
(1) Telecommunications operators, value added service providers and corporate or association subscribers and any persons acting on their behalf may process location data subject to the provisions of this Chapter for the purpose of providing and using value added services. However, the provisions of this Chapter do not, unless otherwise provided by law, apply to location data rendered such that it cannot, in itself or in combination with other data, be associated with a specific subscriber or user.
(2) Processing of location data shall be restricted to persons employed by or acting on behalf of the telecommunications operator, value added service provider or corporate or association subscriber whose job involves the processing of location data for the purpose of carrying out measures referred to in this Chapter.
(3) Such processing is allowed only to the extent required for the purpose of the processing, and it shall not limit the protection of privacy any more than is necessary. After processing, the location data shall, unless otherwise provided by law, be destroyed or rendered such that it cannot be associated with a specific subscriber or user.
(4) The prohibiting of the processing of location data and the service-specific consent referred to in this Chapter are decided in the case of minors under the age of 15 by their guardian under section 4 of the Child Custody and Right of Access Act (361/1983), and in the case of legally incompetent persons other than minors by their guardian under the Guardianship Services Act (442/1999), unless this is impossible by virtue of the technical nature of the service.

Section 19 - Obligation to maintain information security
(1) Telecommunications operators and value added service providers shall **maintain the information security of their services**. Corporate or association subscribers shall **maintain information security in processing their users' identification data and location data**. Maintaining information security in such services or processing means taking measures to ensure **operating security**, **communications security**, **hardware and software security** and **data security**. These measures shall be commensurate with the **seriousness of threats, level of technical development** and **costs**.
(2) The obligation to maintain information security of services laid down in subsection 1 above also applies to processing of data for the purpose of meeting the retention obligation referred to in section 14 a. A service operator shall also name the people entitled to process retained data.
(3) Telecommunications operators and value added service providers are responsible to subscribers and users for the information security referred to in subsections 1 and 2 also on the behalf of any third party that wholly or in part provides a network service, communications service, data retention or value added service. The responsibility specified in this subsection applies to corporate or association subscribers with regard to the processing of users' identification data and location data processed by a third party.

(4) The Finnish Communications Regulatory Authority may issue further regulations to a telecommunications operator regarding information security of services or of data retention referred to in subsections 1–3.

Section 20 - Measures taken to implement information security
(1) A telecommunications operator, value added service provider or corporate or association subscriber, or any party acting on their behalf has the right to undertake necessary **measures** referred to in section 2 **for ensuring information security:**
1) in order to detect, prevent, investigate and commit to pre-trial investigation any disruptions in information security of communications networks or related services;
2) in order to safeguard the communications ability of the sender or the recipient of the message; or
3) in order to prevent preparations of means of payment fraud referred to in Chapter 37(11) of the Penal Code planned to be implemented on a wide scale via communication services.
(2) Measures referred to in subsection 1 above may include:
1) automatic analysis of message content;
2) automatic prevention or limitation of message conveyance or reception;
3) automatic removal from messages of malicious software that pose a threat to information security;
4) any other comparable technical measures.
(3) If it is evident due to the message type, form or some other similar reason that the message contains a malicious software or command, and automatic content analysis of the message cannot ensure the attainment of the goals referred to in subsection 1, the contents of a single message may be processed manually. The sender and recipient of a message whose contents have been manually processed shall be informed of the processing, unless the information would apparently endanger the attainment of the goals referred to in subsection 1.
(4) Any measures referred to in this section shall be implemented with care, and they shall be commensurate with the seriousness of the disruption being combated. Such measures shall not limit freedom of speech, the confidentiality of a message or the protection of privacy any more than is necessary for the purpose of safeguarding the goals referred to in subsection 1. Such measures shall be discontinued if the conditions for them specified in this section no longer exist.
(5) The Finnish Communications Regulatory Authority may issue further regulations to telecommunications operators and value added service providers on the technical implementation of the measures referred to in this section.

Frankreich

Artikel 11 des Gesetzes Nr. 78-17 vom 6. Januar 1978 (zuletzt geändert am 29.3.2011)

(Quelle: http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=BA88C5A0F7F1A163FF35EA0F847947BE.tpdjo11v_1?cidTexte=JORFTEXT000000886460&idArticle=&dateTexte=20110517)

Article 11
La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle exerce les missions suivantes :
1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ;
2° Elle veille à ce que les traitements de données à caractère personnel soient mis en oeuvre conformément aux dispositions de la présente loi.
A ce titre :
a) Elle autorise les traitements mentionnés à l'article 25, donne un avis sur les traitements mentionnés aux articles 26 et 27 et reçoit les déclarations relatives aux autres traitements ;
b) Elle établit et publie les normes mentionnées au I de l'article 24 et édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes ;
c) Elle reçoit les réclamations, pétitions et plaintes relatives à la mise en oeuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci ;

d) Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en oeuvre ou envisagent de mettre en oeuvre des traitements automatisés de données à caractère personnel ;
e) Elle informe sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance, et peut présenter des observations dans les procédures pénales, dans les conditions prévues à l'article 52 ;
f) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou le secrétaire général, dans les conditions prévues à l'article 44, de procéder ou de faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions ;
g) (Abrogé)
h) Elle répond aux demandes d'accès concernant les traitements mentionnés aux articles 41 et 42 ;
3° A la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements :
a) Elle donne un avis sur la conformité aux dispositions de la présente loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, ou à l'anonymisation de ces données, qui lui sont soumis ;
b) Elle porte une appréciation sur les garanties offertes par des règles professionnelles qu'elle a précédemment reconnues conformes aux dispositions de la présente loi, au regard du respect des droits fondamentaux des personnes ;
c) Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elles les a reconnus conformes aux dispositions de la présente loi dans le cadre de l'instruction préalable à la délivrance du label par la commission. Le président peut, lorsque la complexité du produit ou de la procédure le justifie, recourir à toute personne indépendante qualifiée pour procéder à leur évaluation. Le coût de cette évaluation est pris en charge par l'entreprise qui demande le label ;
4° Elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés mentionnés à l'article 1er ;
A ce titre :
a) Elle est consultée sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés.A la demande du président de l'une des commissions permanentes prévue à l'article 43 de la Constitution, l'avis de la commission sur tout projet de loi est rendu public ;
b) Elle propose au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques ;
c) A la demande d'autres autorités administratives indépendantes, elle peut apporter son concours en matière de protection des données ;
d) Elle peut être associée, à la demande du Premier ministre, à la préparation et à la définition de la position française dans les négociations internationales dans le domaine de la protection des données à caractère personnel. Elle peut participer, à la demande du Premier ministre, à la représentation française dans les organisations internationales et communautaires compétentes en ce domaine.
Pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi.
La commission présente chaque année au Président de la République, au Premier ministre et au Parlement un rapport public rendant compte de l'exécution de sa mission.

Article 34
Le responsable du traitement est tenu de prendre toutes précautions utiles, **au regard de la nature des données et des risques présentés** par le traitement, pour **préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.**
Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8.

Artikel D98-5, L34-1 Code des postes et des communications électroniques

(Quellen: http://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000006181878&cidTexte=LEGITEXT000006070987&dateTexte=20110517#, http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000020740388)

Article D98-5

Règles portant sur les conditions de **confidentialité et de neutralité au regard des messages transmis et des informations liées aux communications**.

I. - Respect du secret des correspondances et neutralité.

L'opérateur prend les mesures nécessaires pour garantir la neutralité de ses services vis-à-vis du contenu des messages transmis sur son réseau et le secret des correspondances.

A cet effet, l'opérateur assure ses services sans discrimination quelle que soit la nature des messages transmis et prend les dispositions utiles pour assurer l'intégrité des messages.

L'opérateur est tenu de porter à la connaissance de son personnel les obligations et peines qu'il encourt au titre des dispositions du code pénal, et notamment au titre des articles 226-13, 226-15 et 432-9 relatifs au secret des correspondances.

II. - Traitement des données à caractère personnel.

L'opérateur prend les **mesures propres à assurer la protection, l'intégrité et la confidentialité des données à caractère personnel qu'il détient et qu'il traite**.

L'opérateur est tenu d'exploiter les données à caractère personnel conformément aux finalités déclarées.

1. L'opérateur garantit à tout client, outre les droits mentionnés à l'article R. 10, le droit :

- d'exercer gratuitement son droit d'accès aux données à caractère personnel le concernant ainsi que son droit de rectification de celles-ci ;
- de recevoir des factures non détaillées et, sur sa demande, des factures détaillées.

2. Lorsque les clients de l'opérateur reçoivent une facturation détaillée, les factures adressées :

- comportent un niveau de détail suffisant pour permettre la vérification des montants facturés ;
- ne mentionnent pas les appels à destination des numéros gratuits pour l'utilisateur ;
- n'indiquent pas les quatre derniers chiffres des numéros appelés, à moins que le client n'ait expressément demandé que cela soit le cas.

La facturation détaillée est disponible gratuitement pour l'abonné. Toutefois, des prestations supplémentaires peuvent être, le cas échéant, proposées à l'abonné à un tarif raisonnable.

3. L'opérateur permet à chacun de ses clients de s'opposer gratuitement et par un moyen simple, appel par appel ou de façon permanente (secret permanent), à l'identification de sa ligne par les postes appelés.

Lorsqu'un abonné dispose de plusieurs lignes, cette fonction est offerte pour chaque ligne. Cette fonction doit également être proposée pour des communications effectuées à partir de cabines téléphoniques publiques. L'opérateur met en oeuvre un dispositif particulier de suppression de cette fonction pour des raisons liées au fonctionnement des services d'urgence ou à la tranquillité de l'appelé, conformément à la réglementation en vigueur.

Lorsqu'un abonné dispose du secret permanent, l'opérateur lui permet de supprimer cette fonction, appel par appel, gratuitement et par un moyen simple.

4. L'opérateur informe les abonnés lorsqu'il propose un service d'identification de la ligne appelante ou de la ligne connectée. Il les informe également des possibilités prévues aux trois alinéas suivants :

Dans le cas où l'identification de la ligne appelante est offerte, l'opérateur permet à tout abonné d'empêcher par un moyen simple et gratuit que l'identification de la ligne appelante soit transmise vers son poste.

Dans le cas où l'identification de la ligne appelante est offerte et est indiquée avant l'établissement de l'appel, l'opérateur permet à tout abonné de refuser, par un moyen simple, les appels entrants émanant d'une ligne non identifiée. L'opérateur peut, pour des raisons techniques justifiées, demander à l'Autorité de régulation des communications électroniques et des postes de disposer d'un délai pour la mise en oeuvre de cette fonction.

Dans le cas où l'identification de la ligne obtenue est offerte, l'opérateur permet à tout abonné d'empêcher par un moyen simple et gratuit l'identification de la ligne obtenue auprès de la personne qui appelle.

5. L'opérateur permet à l'abonné vers lequel des appels sont transférés d'interrompre ou de faire interrompre le transfert d'appel gratuitement et par un moyen simple.

L'opérateur informe tout abonné, préalablement à la souscription du contrat, des droits mentionnés au 1 du II du présent article.

Lorsque l'opérateur fait appel à des sociétés de commercialisation de services, il veille, dans les relations contractuelles avec celles-ci, au respect de ses obligations relatives aux conditions de confidentialité et de neutralité au regard des messages transmis et des informations liées aux communications.

III. - Sécurité des communications.
L'opérateur prend toutes les dispositions nécessaires pour assurer la sécurité des communications empruntant son réseau. Il se conforme aux prescriptions techniques en matière de sécurité éventuellement édictées par l'Autorité de régulation des communications électroniques et des postes dans les conditions de l'article L. 36-6. Dans ce cadre et à titre confidentiel, l'Autorité de régulation des communications électroniques et des postes peut se faire communiquer les dispositions prises pour la sécurisation du réseau.
L'opérateur informe ses clients des services existants permettant, le cas échéant, de renforcer la sécurité des communications.
Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, l'opérateur informe les abonnés de ce risque ainsi que de tout moyen éventuel d'y remédier et du coût que cela implique.

Article L34-1
I.-Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des II, III, IV et V.
Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.
II.-Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le V, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs.
III.-Pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le V, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.
Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.
IV.-Sans préjudice des dispositions du II et du III et sous réserve des nécessités des enquêtes judiciaires, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers.L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement.L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.
V.-Les données conservées et traitées dans les conditions définies aux II, III et IV portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux.
Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.
La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article.

Irland

Abschnitte 4 und 12 des Communications (Retention of Data) Act 2011 (in der Fassung vom 26.1.2011)

(Quelle: http://www.oireachtas.ie/documents/bills28/acts/2011/a311.pdf)

4.
(1) A service provider who retains data under *section 3(1)* shall take the **following security measures** in relation to the retained data:
(*a*) the data shall be of the same quality and subject to the same security and protection as those data relating to the publicly available electronic communications service or to the public communications network, as the case may be;
(*b*) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
(*c*) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by authorised personnel only;
(*d*) the data, except those that have been accessed and preserved, shall be destroyed by the service provider after—
(i) in the case of the data in the categories specified in *Part 1* of *Schedule 2*, a period of 2 years and one month, or
(ii) in the case of the data in the categories specified in *Part 2* of *Schedule 2*, a period of one year and one month.
(2) The Data Protection Commissioner is hereby designated as the national supervisory authority for the purposes of this Act and Directive No. 2006/24/EC of the European Parliament and of the Council.

Abschnitte 4 und 5 des Datenschutzgesetzes (in der durch die Richtlinie 2006/24/EC and 2009/136/EC geänderten Fassung)

(Quelle: http://www.dataprotection.ie/documents/legal/SI336of2011.pdf)

4. Security of processing
(1) With respect to network security and, in particular, the requirements of paragraph (2), an undertaking providing a publicly available electronic communications network or service shall take **appropriate technical and organizational measures to safeguard the security of its services**, if necessary, in conjunction with undertakings upon whose networks such services are transmitted. These measures shall ensure **the level of security appropriate to the risk** presented having **regard to the state of the art** and the **cost** of their implementation.
(2) Without prejudice to the Data Protection Acts, the measures referred to in paragraph (1) shall at least—
(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,
(b) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorized or unlawful storage, processing, access or disclosure, and
(c) ensure the implementation of a security policy with respect to the processing of personal data.

(3) The **Commissioner** may audit the measures taken by an undertaking providing publicly available electronic communications services and issue **recommendations about best practices concerning the level of security which those measures should achieve**.
(4) In the case of a particular risk of a breach of the security of the public communications network, the undertaking providing the publicly available electronic communications service shall inform its subscribers concerning such risk without delay and, where the risk lies outside the scope of the measures to be taken by the relevant service provider, any possible remedies including an indication of the likely costs involved.
(5) An undertaking whose public communications network is used by another undertaking for the supply of a publicly available electronic communications service shall comply with any reasonable request made by the undertaking using the public communications network for the purpose of complying with this Regulation.
(6) Where there has been a personal data breach, the undertaking shall, without undue delay—
(a) notify the Commissioner of the said breach, and
(b) where the said breach is likely to adversely affect the personal data or privacy of a subscriber or individual, notify the subscriber or individual of the breach.
(7) A notification under paragraph (6)(b) shall not be required if the undertaking has demonstrated to the satisfaction of the Commissioner that it has implemented appropriate technological protection measures which render the data unintelligible to any person who is not authorised to access it and that those measures were applied to the data affected by the security breach.
(8) Without prejudice to paragraphs (6) and (7), where the undertaking has not notified the subscriber or individual of the personal data breach, the Commissioner may, having considered the likely adverse effects of the breach, require the undertaking to do so by serving an enforcement notice on the undertaking in accordance with Regulation 17(4).
(9) A notification under paragraph (6) shall, at least, contain—
(a) a description of the nature of the personal data breach,
(b) a description of the contact points where more information can be obtained,
(c) a recommendation on measures to mitigate the possible adverse effects of the personal data breach, and
(d) where the notification is under paragraph 6(a), a description of the consequences of, and the measures proposed to be taken by the undertaking to address, the personal data breach.
(10) Subject to any technical implementing measures adopted by the European Commission under Article 4(5) of the Directive on privacy and electronic communications, the Commissioner may adopt guidelines concerning the circumstances in which undertakings are required to notify personal data breaches, the format of such notification and the manner in which such notification is to be made. Where necessary the Commissioner may, for the purpose of this paragraph, issue such instructions as he or she considers necessary.
(11) The Commissioner may conduct an audit to determine compliance with guidelines and instructions issued under paragraph (10).
(12) Undertakings shall maintain an inventory of personal data breaches which shall comprise the following information—
(a) the facts surrounding the breach,
(b) the effects of the breach, and
(c) any remedial action taken, and shall be sufficient to enable the Commissioner to verify compliance with paragraphs (6) to (10).
(13) An undertaking that—
(a) fails to comply with the requirements of paragraph (1),
(b) fails to comply with the requirements of paragraph (4),
(c) subject to paragraph (7), fails to comply with the requirements of paragraph (6),
(d) refuses to co-operate with an audit referred to in paragraph (3) or (11), or
(e) fails to comply with the requirements of paragraph (12), commits an offence.
(14) (a) An undertaking that commits an offence under this Regulation (other than under paragraph 13(a) or (c)) is liable on summary conviction to a class A fine.
(b) An undertaking that commits an offence under paragraph 13(a) or (c) is liable, on summary conviction, to a class A fine or, on indictment—
(i) in the case of a body corporate, to a fine not exceeding €250,000, or
(ii) in the case of a natural person, to a fine not exceeding €50,000.

5. Confidentiality of communications
(1) Without prejudice to section 98 of the Act of 1983 and section 2 of the Act of 1993 and except where legally authorised under a provision adopted in accordance with Article 15(1) of the Directive on privacy and electronic communications, the listening, tapping, storage or other kinds

of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, is prohibited.
(2) Paragraph (1) does not—
(a) prevent the technical storage of communications and the related traffic data which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality, and
(b) affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction
or of any other business communication.
(3) A person shall not use an electronic communications network to store information, or to gain access to information already stored in the terminal equipment of a subscriber or user, unless
(a) the subscriber or user has given his or her consent to that use, and
(b) the subscriber or user has been provided with clear and comprehensive information in accordance with the Data Protection Acts which—
(i) is both prominently displayed and easily accessible, and
(ii) includes, without limitation, the purposes of the processing of the information.
(4) For the purpose of paragraph (3), the methods of providing information and giving consent should be as user-friendly as possible. Where it is technically possible and effective, having regard to the relevant provisions of the Data Protection Acts, the user's consent to the storing of information or to gaining access to information already stored may be given by the use of appropriate browser settings or other technological application by means of which the user can be considered to have given his or her consent.
(5) Paragraph (3) does not prevent any technical storage of, or access to, information for the sole purpose of carrying out the transmission of a communication over an electronic communications network or which is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Italien

Abschnitte 11, 31, 32, 33, 34, 35, 36, 58, 123 und Annex B des Datenschutzgesetzes vom 30.6.2003

(Quelle: http://www.privacy.it/privacycode-en.html)

Section 11 - Processing Arrangements and Data Quality
1. Personal data undergoing processing shall be:
a) processed lawfully and fairly;
b) collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes;
c) accurate and, when necessary, kept up to date;
d) relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed;
e) kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed.
2. Any personal data that is processed in breach of the relevant provisions concerning the processing of personal data may not be used.

Section 31 - Security Requirements
1. Personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimise, by means of suitable preventative security measures, the risk of their destruction or loss, whether by accident or not, of unauthorized access to the data or of processing

operations that are either unlawful or inconsistent with the purposes for which the data have been collected.

Section 32 - Specific Categories of Data Controller
1. The provider of a publicly available electronic communications service shall take **suitable technical and organisational measures** under Section 31 that are **adequate in the light of the existing risk, in order to safeguard security of its services and integrity of traffic data, location data and electronic communications against any form of unauthorised utilisation or access.**
2. Whenever security of service or personal data makes it necessary to also take measures applying to the network, the provider of a publicly available electronic communications service shall take those measures jointly with the provider of the public communications network. Failing an agreement between said providers, the dispute shall be settled, at the instance of either provider, by the Authority for Communications Safeguards in pursuance of the arrangements set out in the legislation in force.
3. In case of a particular risk of a breach of network security, the provider of a publicly available electronic communications service shall inform subscribers and, if possible, users concerning said risk and, when the risk lies outside the scope of the measures to be taken by said provider pursuant to paragraphs 1 and 2, of all the possible remedies including an indication of the likely costs involved. This information shall be also provided to the Garante and the Authority for Communications Safeguards.

Section 33 - Minimum Security Measures
1. Within the framework of the more general security requirements referred to in Section 31, or else provided for by specific regulations, data controllers shall be required in any case to adopt the minimum security measures pursuant either to this Chapter or to Section 58(3) in order to ensure a minimum level of personal data protection.

Section 34 - Processing by Electronic Means
1. Processing personal data by electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B:
a) computerised authentication,
b) implementation of authentication credentials management procedures,
c) use of an authorisation system,
d) regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintenancing electronic means,
e) protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software,
f) implementation of procedures for safekeeping backup copies and restoring data and system availability,
g) keeping an up-to-date security policy document,
h) implementation of encryption techniques or identification codes for specific processing operations performed by health care bodies in respect of data disclosing health and sex life.

Section 35 – Processing without Electronic Means
1. Processing personal data without electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B:
a) regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of the processing and/or by the individual organisational departments,
b) implementing procedures such as to ensure safekeeping of records and documents committed to the entities in charge of the processing for the latter to discharge the relevant tasks,
c) implementing procedures to keep certain records in restricted-access filing systems and regulating access mechanisms with a view to enabling identification of the entities in charge of the processing.

Section 36 - Upgrading
1. The **technical specifications as per Annex B** concerning the minimum measures referred to in this Chapter shall be regularly updated by a **decree of the Minister of Justice issued in agreement with the Minister for Innovation and Technologies** by having regard to both technical developments and the experience gathered in this sector.

Section 58 - Applicable Provisions
1. As regards the processing operations carried out by the entities referred to in Sections 3, 4 and 6 of Act no. 801 of 24 October 1977, as well as the data to which State secret applies under Section 12 of said Act, the provisions of this Code shall apply insofar as they are set out in Sections 1 to 6, 11, 14, 15, 31, 33, 58, 154, 160 and 169.
2. As regards the processing operations carried out by public bodies for purposes of defence or relating to State security, as expressly required by laws that specifically provide for such processing operations, the provisions of this Code shall apply insofar as they are set out in paragraph 1 as well as in Sections 37, 38 and 163.
3. The security measures relating to the data processed by the agencies as per paragraph 1 shall be laid down and regularly updated in a decree by the Prime Minister's Office in compliance with the provisions applying to this subject matter.
4. The arrangements to implement the applicable provisions of this Code with regard to categories of data, data subject, permitted processing operation and entities in charge of the processing, also with a view to updating and retaining the data, shall be laid down in a decree by the Prime Minister's Office.

Section 123 - Traffic Data
1. Traffic data relating to subscribers and users that are processed by the provider of a public communications network or publicly available electronic communications service shall be **erased or made anonymous** when they are no longer necessary for the purpose of transmitting the electronic communication, subject to paragraphs 2, 3 and 5.
2. Providers shall be allowed to process traffic data that are strictly necessary for subscriber billing and interconnection payments for a period not in excess of six months in order to provide evidence in case the bill is challenged or payment is to be pursued, subject to such additional retention as may be specifically necessary on account of a claim also lodged with judicial authorities.
3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 2 to the extent and for the duration necessary for such services or marketing, on condition that the subscriber or user to whom the data relate has given his/her consent. Such consent may be withdrawn at any time.
4. In providing the information referred to in Section 13, the service provider shall inform a subscriber or user on the nature of the traffic data processed as well as on duration of the processing for the purposes referred to in paragraphs 2 and 3.
5. Processing of traffic data shall be restricted to persons in charge of the processing who act – pursuant to Section 30 – directly under the authority of the provider of a publicly available electronic communications service or, where applicable, the provider of a public communications network and deal with billing or traffic management, customer enquiries, fraud detection, marketing of electronic communications or the provision of value-added services. Processing shall be
restricted to what is absolutely necessary for the purposes of such activities and must allow identification of the person in charge of the processing who accesses the data, also by means of automated interrogation procedures.
6. The Authority for Communications Safeguards may obtain traffic and billing data that are necessary for settling disputes, particularly with regard to interconnection or billing matters.

TECHNICAL SPECIFICATIONS CONCERNING MINIMUM SECURITY MEASURES (ANNEX B)
(see Sections 33 to 36 of the Code)

PROCESSING BY ELECTRONIC MEANS
The following technical arrangements to be implemented by the data controller, data processor — if nominated — and person(s) in charge of the processing whenever data are processed by electronic means:

Computerised Authentication System
1. Persons in charge of the processing shall be allowed to process personal data by electronic means if they are provided with **authentication credentials** such as to successfully complete an **authentication procedure** relating either to a specific processing operation or to a set of processing operations.
2. Authentication credentials shall consist in an **ID code** for the person in charge of the processing as associated with a **secret password** that shall only be known to the latter person; alternatively, they shall consist in an **authentication device** that shall be used and held exclusively by the person in charge of the processing and may be associated with either an ID code or a password, or else in a **biometric feature** that

relates to the person in charge of the processing and may be associated with either an ID code or a password.
3. **One or more** authentication credentials shall be assigned to or associated with each person in charge of the processing.
4. The instructions provided to the persons in charge of the processing shall lay down the obligation to take such precautions as may be necessary to ensure that the **confidential component(s) in the credentials are kept secret and that the devices used and held exclusively by persons in charge of the processing are kept with due care**.
5. Where provided for by the relevant authentication system, a **password** shall consist of **at least eight characters**; if this is not allowed by the electronic equipment, a password shall consist of the **maximum permitted number of characters**. It shall not contain any item that can be easily related to the person in charge of the processing and shall be **modified by the latter when it is first used** as well as **at least every six months thereafter**. If **sensitive or judicial data** are processed, the password shall be modified at least every **three months**.
6. An ID code, if used, may not be assigned to another person in charge of the processing even at a different time.
7. **Authentication credentials shall be de-activated** if they have **not been used for at least six months**, except for those that have been authorised exclusively for technical management purposes.
8. **Authentication credentials shall be also de-activated** if the person in charge of the processing is **disqualified from accessing personal data**.
9. The persons in charge of the processing shall be instructed to the effect that **electronic equipment should not be left unattended and made accessible during processing sessions**.
10. Where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the data controller can ensure that data or electronic equipment are available in case the person in charge of the processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operationality and security. In this case, copies of the credentials shall be kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Said entities shall have to inform the person in charge of the processing, without delay, as to the activities carried out.
11. The provisions concerning the authentication system referred to above as well as those concerning the authorisation system shall not apply to the processing of personal data that are intended for dissemination.
Authorisation System
12. Where authorisation profiles with different scope have been set out for the persons in charge of the processing, an **authorisation system shall be used**.
13. Authorisation profiles for each person or homogeneous set of persons in charge of the processing shall be set out and configured prior to start of the processing in such a way as to **only enable access to the data that are necessary to perform processing operations**.
14. It shall be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorisation profiles still apply.

Other Security Measures
15. Within the framework of the **regular update — to be performed at least at yearly intervals — of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the processing as well as to the technicians responsible for management and/or maintenance of electronic equipment**, the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile.
16. **Personal data shall be protected against the risk of intrusion and the effects of programmes** as per Section 615-quinquies of the Criminal Code by implementing **suitable electronic means to be updated at least every six months.**
17. The regular update of computer programmes as aimed at preventing vulnerability and removing flaws of electronic means shall be carried out at least **annually**. If **sensitive or judicial data** are processed, such update shall be carried out at least **every six months**.
18. **Organisational and technical instructions** shall be issued such as to require at least **weekly data back-ups.**

Security Policy Document

19. By 31 March of each year, the controller of processing operations concerning sensitive and/or judicial data shall draw up, also by the agency of the data processor, if nominated, a security policy document containing appropriate information with regard to:
19.1 the list of processing operations concerning personal data,
19.2 the distribution of tasks and responsibilities among the departments/divisions in charge of processing data,
19.3 an analysis of the risks applying to the data,
19.4 the measures to be taken in order to ensure data integrity and availability as well as protection of areas and premises insofar as they are relevant for the purpose of keeping and accessing such data,
19.5 a description of the criteria and mechanisms to restore data availability following destruction and/or damage as per point 23 below,
19.6 a schedule of training activities concerning the persons in charge of the processing with a view to informing them on the risks applying to the data, the measures that are available to prevent harmful events, the most important features of personal data protection legislation in connection with the relevant activities, the resulting liability and the arrangements to get updated information on the minimum security measures adopted by the data controller. Said training activities shall be planned as of the start of the employment relationship as well as in connection with changes in the task(s) discharged and/or the implementation of new, significant means that are relevant to the processing of personal data,
19.7 a description of the criteria to be implemented in order to ensure adoption of the minimum security measures whenever processing operations concerning personal data are externalised in accordance with the Code,
19.8 as for the personal data disclosing health and sex life referred to under point 24, the specification of the criteria to be implemented in order to either encrypt such data or keep them separate from other personal data concerning the same data subject.
Additional Measures Applying to Processing of Sensitive or Judicial Data
20. Sensitive or judicial data shall be protected against unauthorised access as per Section 615-ter of the Criminal Code by implementing suitable electronic means.
21. Organisational and technical instructions shall be issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorised access and processing.
22. The removable media containing sensitive or judicial data shall be destroyed or made unusable if they are not used; alternatively, they may be re-used by other persons in charge of the processing, who are not authorised to process the same data, if the information previously contained in them is not intelligible and cannot be re-constructed by any technical means.
23. If either the data or electronic means have been damaged, suitable measures shall be adopted to ensure that data access is restored within a specific deadline, which must be compatible with data subjects' rights and not in excess of seven days.
24. Health care bodies and professionals shall process data disclosing health and sex life as contained in lists, registers or data banks in accordance with the mechanisms referred to in Section 22(6) of the Code also in order to ensure that said data are processed separately from the other personal data allowing data subjects to be identified directly. Data concerning genetic identity shall only be processed in protected premises that may only be accessed by such persons in charge of the processing and entities as have been specifically authorised to access them. Containers equipped with locks or equivalent devices shall have to be used in order to remove the data outside the premises reserved for their processing; the data shall have to be encrypted for the purpose of electronically transferring them.
Safeguards and Protections
25. Where a data controller adopts minimum security measures by committing the relevant tasks to external entities, prior to implementing such measures he or she shall require the installing technician(s) to supply a written description of the activities performed by which it is certified that they are compliant with the provisions set out in these technical specifications.
26. The circumstance that the security policy document has been drawn up and/or updated shall be referred to in the management report that the data controller may be required to submit together with the relevant balance sheet.

PROCESSING WITHOUT ELECTRONIC MEANS
The following technical arrangements to be implemented by the data controller, data processor — if nominated — and person(s) in charge of the processing whenever data are processed without electronic means:
27. The persons in charge of the processing shall be instructed in writing with regard to controlling and keeping, throughout the steps required to perform processing operations, records and documents containing personal data. Within the framework of the regular update — to be performed at least at yearly intervals — of the specifications concerning the scope of the processing operations that are entrusted to the

individual persons in charge of the processing, the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile.
28. If records and documents containing sensitive or judicial personal data are entrusted to the persons in charge of the processing for the latter to discharge the relevant tasks, said records and documents shall be kept and controlled by the persons in charge of the processing until they are returned so as to prevent unauthorised entities from accessing them; they shall be returned once the relevant tasks have been discharged.
29. Access to archives containing sensitive or judicial data shall be controlled. The persons authorised to access said archives for whatever purpose after closing time shall be identified and registered. If an archive is not equipped with electronic devices for access control or is not placed under the surveillance of security staff, the persons accessing said archive shall have to be authorised in advance.

Lettland

Abschnitte 19, 25 und 71.1 des Gesetzes über die elektronische Kommunikation (zuletzt geändert am 3.5.2007)

(Quelle: http://www.sprk.gov.lv/index.php?id=1116&sadala=193)

Section 19 - Duties of Electronic Communications Merchants
…
16) perform **according to the procedures specified by the Cabinet technical and organisational measures in relation to the security of the electronic communications network for the protection of the user data thereof**, as well as in the case of a threat to a specific electronic communications network to inform users regarding the risks of using the electronic communications network and the accessible means of legal protection for the reduction of such risks; and
17) inform users regarding the possibility of installing a content filter, which restricts access of such material in which is propagandised cruel behaviour, violence, erotica and pornography, and which creates a threat to the mental development of children, as well as ensure the installation of content filters if the subscriber and the electronic communications merchant have mutually agreed regarding them.

Section 25 - Use of Private Electronic Communications Networks
(1) A natural person or legal entity has the right to establish and use a private electronic communications network.
(2) The provision of electronic communications services utilising a private electronic communications network is prohibited.
(3) The Cabinet shall determine the procedures by which the State private electronic communications network shall be ensured and used.
(4) The Cabinet shall determine the unified data security requirements for electronic communications infrastructure or terminal equipment connected to the State private electronic communications network

Section 71.1 - Utilisation and Processing of Data to be Retained
(1) Data to be retained shall be retained and transferred to pre-trial investigation institutions, persons performing investigative field work, State security institutions, the Office of the Public Prosecutor and the courts in order to protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings.
(2) An electronic communications merchant shall ensure the retention of retained data in such volume as they are acquired or processed in providing electronic communications services, **as well as ensuring the protection thereof against accidental or unlawful destruction, loss or modification, or processing or disclosure not provided for in this Law**. The electronic communications merchant does not have a duty to perform additional measures to acquire the data to be retained if in providing electronic communications services, the technical equipment of the merchant does not generate, process and register such data.

(3) An electronic communications merchant shall ensure the transfer of data to be retained to the institutions referred to in Paragraph one of this Section on the basis of a request therefrom.
(4) The Cabinet shall determine the procedures for the requesting by and transfer of data to be retained to the institutions referred to in Paragraph one of this Section.
(5) The Data State Inspection according to the procedures and in the volume specified by the Cabinet shall once per year compile statistical information regarding the requests to receive data to be retained from the institutions referred to in Paragraph one of this Section and regarding the issuing of such data.
(6) An electronic communications merchant does not have the right to disclose information regarding the fact that data to be retained has been requested by or transferred to the institutions referred to in Paragraph one of this Section, as well as information regarding users or subscribers in relation to whom data to be retained has been requested or transferred, except in the cases specified in regulatory enactments.
(7) Processing of data to be retained may be performed only by an authorised person of the electronic communications merchant.
(8) Data to be retained shall be extinguished at the end of the time period specified in Section 19, Paragraph one, Clause 11, except for the data, which the institutions referred to in Paragraph one of this Section have requested up to the end of the time period for the retention of data, but which have not yet been issued, as well as data, which is necessary for the provision of further services, payment accounting for services provided, the examination of claims, recovery of payments or ensuring interconnections.

Luxemburg

Art. 2, 3 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques (in der Fassung vom 10.8.2011)

(Quelle: http://www.legilux.public.lu/leg/a/archives/2011/0172/a172.pdf)

Art. 2. Définitions
(m) «violation de données à caractère personnel»: une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public.

Art. 3. Sécurité du traitement
(1) Le fournisseur de services prend les mesures **techniques et d'organisation appropriées afin de garantir la sécurité de ses services**, le cas échéant conjointement avec l'opérateur en ce qui concerne la sécurité du réseau. En cas d'atteinte ou de risque d'atteinte grave à la sécurité du réseau ou des services, le fournisseur de services et le cas échéant l'opérateur prend les mesures appropriées pour y remédier, les frais étant à sa seule charge.
Sous réserve des dispositions générales de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, les mesures visées ci-dessus, pour le moins:
– **garantissent que seules des personnes autorisées peuvent avoir accès aux données à caractère personnel à des fins légalement autorisées**,
– **protègent les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites**, et
– **assurent la mise en oeuvre d'une politique de sécurité relative au traitement des données à caractère personnel**.
La Commission nationale pour la protection des données est habilitée à vérifier les mesures prises par les fournisseurs de services de communications électroniques accessibles au public, ainsi **qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient atteindre.**
(2) Sans préjudice de ce qui précède, le fournisseur de services et le cas échéant l'opérateur informe ses abonnés de tout risque imminent d'atteinte à la sécurité du réseau ou des services mettant en cause la con-

fidentialité des communications ainsi que du moyen éventuel pour y remédier, y compris en en indiquant le coût probable.
(3) En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit sans retard la Commission nationale pour la protection des données de la violation. Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également sans retard indu l'abonné ou le particulier concerné de la violation.
La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si le fournisseur a prouvé, à la satisfaction de la Commission nationale pour la protection des données, qu'il a mis en oeuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès. Sans préjudice de l'obligation du fournisseur d'informer l'abonné et le particulier concerné, si le fournisseur n'a pas déjà averti l'abonné ou le particulier de la violation de données à caractère personnel, la Commission nationale pour la protection des données peut, après avoir examiné les effets éventuellement négatifs de cette violation, exiger du fournisseur qu'il s'exécute.
La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel. La notification faite à la Commission nationale pour la protection des données décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par le fournisseur pour y remédier.
La Commission nationale pour la protection des données peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant les circonstances dans lesquelles le fournisseur est tenu de notifier la violation de données à caractère personnel, le format applicable à cette notification et sa procédure de transmission.
Lors d'un premier manquement aux obligations de notification, le fournisseur est averti par la Commission nationale pour la protection des données. En cas de manquement répété la Commission nationale peut prononcer une amende d'ordre qui ne peut excéder 50.000 euros.
Un recours en réformation est ouvert devant le tribunal administratif contre les décisions prises par la Commission nationale pour la protection des données dans le cadre du présent article.
(4) Les fournisseurs tiennent à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, les données consignées devant être suffisantes pour permettre à la Commission nationale pour la protection des données de vérifier le respect des dispositions du paragraphe (3). Cet inventaire comporte uniquement les informations nécessaires à cette fin.
(5) Quiconque contrevient aux dispositions des paragraphes (1), (2) et (4) est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 22 et 23 de loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (in der Fassung vom 13.8.2002)

(Quelle: http://www.legilux.public.lu/leg/a/archives/2002/0091/a091.pdf#page=2)

Art. 22 - Sécurité des traitements
(1) Le responsable du traitement doit mettre en œuvre **toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.** Ces mesures font l'objet d'un rapport annuel à soumettre par le responsable du traitement à la Commission nationale.
(2) Lorsque le traitement est mis en œuvre pour compte du responsable du traitement, celui-ci doit choisir un sous- traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect de ces mesures.
(3) Tout traitement effectué pour compte doit être régi par un contrat ou un acte juridique consigné par

écrit qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que:
(a) le sous-traitant n'agit que sur la seule instruction du responsable du traitement; et que (b) les obligations visées au présent article incombent également à celui-ci.1845

Art. 23 - Mesures de sécurité particulières
En fonction du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et des coûts liés à leur mise en œuvre, les mesures visées à l'article 22, paragraphe (1) doivent:
(a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données (contrôle à l'entrée des installations);
(b) empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports);
(c) empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées (contrôle de la mémoire);
(d) empêcher que des systèmes de traitements de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation);
(e) garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur compétence (contrôle de l'accès);
(f) garantir que puisse être vérifié et constaté l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission (contrôle de la transmission);
(g) garantir que puisse être vérifié et constaté a posteriori l'identité des personnes ayant eu accès au système d'information et quelles données ont été introduites dans le système, à quel moment et par quelle personne (contrôle de l'introduction);
(h) empêcher que, lors de la communication de données et du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport);
(i) sauvegarder les données par la constitution de copies de sécurité (contrôle de la disponibilité).

Art. 67-1 Code d'instruction criminelle (in der Fassung vom 25.11.2011)

(Quelle: http://www.legilux.public.lu/leg/textescoordonnes/codes/code_instruction_criminelle/CodeInstrCrim_PageAccueil.pdf)

Art. 67-1
(1) Lorsque le juge d'instruction saisi de faits qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, estime qu'il existe des circonstances qui rendent le repérage de télécommunications ou la localisation de l'origine ou de la destination de telecommunications nécessaire à la manifestation de la vérité, il peut faire procéder, en requérant au besoin le concours technique de l'opérateur de télécommunications et/ou du fournisseur d'un service de télécommunications:

Niederlande

Artikel 13.2, 13.4, Telecommunicatiewet (in der Fassung vom 3.11.2011)

(Quelle: http://wetten.overheid.nl/BWBR0009950/Hoofdstuk1319/Artikel135/geldigheidsdatum_03-08-2011)

Artikel 13.2a
1. In dit artikel wordt verstaan onder:

a. *gegevens:* de verkeers- en locatiegegevens, bedoeld in artikel 11.1, onderdeel b respectievelijk onderdeel d, alsmede de daarmee verband houdende gegevens die nodig zijn om de abonnee of gebruiker te identificeren;
b. *oproeppoging zonder resultaat:* een communicatie waarbij een telefoonoproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord.
2. Aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten bewaren de in de bij deze wet behorende bijlage aangewezen gegevens, voorzover deze in het kader van de aangeboden netwerken of diensten worden gegenereerd of verwerkt, ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven.
3. De gegevens, bedoeld in het tweede lid, worden door de aanbieders bewaard gedurende een periode van:
a. twaalf maanden voor gegevens in verband met telefonie over een vast of mobiel netwerk, bedoeld in de bij deze wet behorende bijlage, onder A, of
b. zes maanden voor gegevens in verband met internettoegang, e-mail over het internet en internettelefonie, bedoeld in de bij deze wet behorende bijlage, onder B, gerekend vanaf de datum van de communicatie.
4. De verplichting, bedoeld in het tweede lid, heeft betrekking op gegevens van oproeppogingen zonder resultaat, voorzover deze gegevens door de aanbieders bij het aanbieden van openbare telecommunicatienetwerken of openbare telecommunicatiediensten worden gegenereerd, verwerkt en opgeslagen of gelogd.

Artikel 13.4
1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten voldoen **onverwijld** aan een vordering op grond van artikel 126n of artikel 126na, dan wel artikel 126u of artikel 126ua, van het Wetboek van Strafvordering dan wel een verzoek op grond van artikel 28 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het verstrekken van gegevens over een gebruiker van een openbaar telecommunicatienetwerk dan wel een openbare telecommunicatiedienst en het telecommunicatieverkeer met betrekking tot die gebruiker.
2. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten voldoen aan een vordering op grond van artikel 126na, eerste lid, 126ua, eerste lid, of 126zi van het Wetboek van Strafvordering dan wel een verzoek op grond van artikel 29 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het verstrekken van gegevens terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een openbaar telecommunicatienetwerk dan wel een openbare telecommunicatiedienst.
3. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten voldoen aan een vordering op grond van artikel 126na, tweede lid, 126ua, tweede lid, of 126zi van het Wetboek van Strafvordering dan wel een verzoek op grond van artikel 29 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het op bij algemene maatregel van bestuur te bepalen wijze achterhalen en verstrekken van de gegevens, bedoeld in het eerste lid.Teneinde aan deze verplichtingen te kunnen voldoen bewaren de aanbieders de bij algemene maatregel van bestuur aan te wijzen gegevens voor een periode van twaalf maanden, vanaf het tijdstip waarop deze gegevens voor de eerste maal zijn verwerkt.
4. Bij algemene maatregel van bestuur, op voordracht van Onze Minister van Justitie, Onze Minister, Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister van Defensie kunnen regels worden gesteld met betrekking tot de wijze waarop de aanbieders aan een vordering of een verzoek, bedoeld in het eerste, tweede en derde lid, voldoen, de registratie van statistische gegevens en de termijnen waarbinnen die gegevens beschikbaar worden gesteld en de wijze waarop de gegevens, bedoeld in het tweede en derde lid, beschikbaar worden gehouden. De voordracht voor een krachtens de eerste volzin vast te stellen algemene maatregel van bestuur wordt niet eerder gedaan dan vier weken nadat het ontwerp aan beide kamers der Staten-Generaal is overgelegd.

Artikel 13.5
1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zijn verplicht gegevens met betrekking tot een bijzondere last dan wel toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 als bedoeld in artikel 13.2 dan wel een vordering of een verzoek als bedoeld in artikel 13.2b of artikel 13.4, eerste, tweede of derde lid, te beveiligen tegen kennisneming door onbevoegden alsmede geheimhouding te betrachten met betrekking tot deze gegevens.
2. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten nemen met betrekking tot de gegevens die ingevolge artikel 13.2a, tweede lid, worden bewaard passende technische en organisatorische maatregelen teneinde:

a. de gegevens te beveiligen tegen vernietiging, tegen verlies of wijziging en niet toegelaten opslag, verwerking, toegang of openbaarmaking;
b. te waarborgen dat toegang tot de gegevens, bedoeld in onderdeel a, slechts geschiedt door speciaal daartoe bevoegde personen;
c. de gegevens te kunnen vernietigen na afloop van de periode, bedoeld in artikel 13.2a, derde lid.
3. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten dragen er zorg voor dat de gegevens, die ingevolge artikel 13.2a, tweede lid, worden bewaard:
a. dezelfde kwaliteit hebben en worden onderworpen aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk;
b. onverwijld worden vernietigd na afloop van de periode, bedoeld in artikel 13.2a, derde lid.
4. Op voordracht van Onze Minister van Justitie, Onze Minister, Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister van Defensie kunnen bij algemene maatregel van bestuur regels worden gesteld met betrekking tot de te nemen maatregelen in verband met de beveiliging en de waarborging bedoeld in het eerste, tweede en derde lid. De voordracht voor een krachtens de eerste volzin vast te stellen algemene maatregel van bestuur wordt niet eerder gedaan dan vier weken nadat het ontwerp aan beide kamers der Staten-Generaal is overgelegd.

Artikel 13 Personal Data Protection Act (in der Fassung vom 23.11.1999)

(Quelle: http://www.dutchdpa.nl/downloads_wetten/wbp.pdf)

Article 13
The responsible party shall implement appropriate technical and organizational measures to secure personal data against loss or against any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. These measures shall also aim at preventing unnecessary collection and further processing of personal data.

Österreich

§§ 94, 95, 99, 102c des Telekommunikationsgesetzes (zuletzt geändert am 18.5.2011)

(Quelle: http://www.parlinkom.gv.at/PAKT/VHG/XXIV/I/I_01157/fname_213346.pdf)

§ 94 - Technische Einrichtungen
(1) Der Anbieter ist nach Maßgabe der gemäß Abs. 3 und 4 erlassenen Verordnungen verpflichtet, alle Einrichtungen bereitzustellen, die zur Überwachung von Nachrichten sowie zur Auskunft über Daten einer Nachrichtenübermittlung einschließlich der Auskunft über Vorratsdaten nach den Bestimmungen der StPO erforderlich sind. Für die Bereitstellung sind dem Anbieter 80% der Kosten (Personal- und Sachaufwendungen), die er aufwenden musste, um die gemäß den Abs. 3 und 4 erlassenen Verordnungen erforderlichen Funktionen in seinen Anlagen einzurichten, zu ersetzen. Der Bundesminister für Verkehr, Innovation und Technologie hat im Einvernehmen mit dem Bundesminister für Inneres, dem Bundesminister für Justiz und dem Bundesminister für Finanzen durch Verordnung die Bemessungsgrundlage für diesen Prozentsatz sowie die Modalitäten für die Geltendmachung dieses Ersatzanspruches festzusetzen. Dabei ist insbesondere auf die wirtschaftliche Zumutbarkeit des Aufwandes, auf ein allfälliges Interesse des betroffenen Unternehmers an den zu erbringenden Leistungen und auf eine allfällige durch die gebotenen technischen Möglichkeiten bewirkte Gefährdung, der durch die verlangte Mitwirkung entgegengewirkt werden soll, sowie auf die Einfachheit und Kostengünstigkeit des Verfahrens Bedacht zu nehmen.
(2) Der Anbieter ist verpflichtet, an der Überwachung von Nachrichten sowie der Auskunft über Daten einer Nachrichtenübermittlung einschließlich der Auskunft über Vorratsdaten nach den Bestimmungen der StPO im erforderlichen Ausmaß mitzuwirken. Der Bundesminister für Justiz hat im Einvernehmen mit dem Bun-

desminister für Verkehr, Innovation und Technologie und dem Bundesminister für Finanzen durch Verordnung einen angemessenen Kostenersatz vorzusehen. Dabei ist insbesondere auf die wirtschaftliche Zumutbarkeit des Aufwandes, auf ein allfälliges Interesse des betroffenen Unternehmers an den zu erbringenden Leistungen und auf eine allfällige durch die gebotenen technischen Möglichkeiten bewirkte Gefährdung, der durch die verlangte Mitwirkung entgegengewirkt werden soll, sowie der öffentlichen Aufgabe der Rechtspflege Bedacht zu nehmen.
(3) Durch Verordnung kann der Bundesminister für Verkehr, Innovation und Technologie im Einvernehmen mit den Bundesministern für Inneres und für Justiz dem jeweiligen Stand der Technik entsprechend die näheren Bestimmungen für die Gestaltung der technischen Einrichtungen zur Gewährleistung der Überwachung von Nachrichten nach den Bestimmungen der StPO und zum Schutz der zu übermittelnden Daten gegen die unbefugte Kenntnisnahme oder Verwendung durch Dritte festsetzen. Nach Erlass der Verordnung ist unmittelbar dem Hauptausschuss des Nationalrates zu berichten.
(4) Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG, hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als "Comma-Separated Value (CSV)" - Dateiformat zu übermitteln.
Ausgenommen davon ist die Übermittlung von Daten in den Fällen des § 98, von Daten in den Fällen von § 99 Abs. 5 Z 3 und 4 bei Gefahr in Verzug, von Standortdaten in den Fällen der Feststellung des aktuellen Standortes gemäß §§ 134 ff StPO sowie die Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten. Durch Verordnung kann der Bundesminister für Verkehr, Innovation und Technologie im Einvernehmen mit den Bundesministern für Inneres und für Justiz die näheren Bestimmungen zur einheitlichen Definition der Syntax, der Datenfelder und der Verschlüsselung, zur Speicherung und Übermittlung der Daten sowie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102c angefertigten Protokolle festsetzen. Nach Erlass der Verordnung ist unmittelbar dem Hauptausschuss des Nationalrates zu berichten.

§ 95 - Sicherheit des Netzbetriebs
(1) Die Pflicht zur Erlassung von **Datensicherheitsmaßnahmen im Sinne des § 14 des Datenschutzgesetzes** 2000 im Zusammenhang mit der Erbringung eines öffentlichen Kommunikationsdienstes obliegt jedem Betreiber jeweils für jeden von ihm erbrachten Dienst.
(2) Unbeschadet des Abs. 1 hat der Betreiber in jenen Fällen, in denen ein besonderes Risiko der Verletzung der Vertraulichkeit besteht, die Teilnehmer über dieses Risiko und - wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahmen liegt - über mögliche Abhilfen einschließlich deren Kosten zu unterrichten.

§ 99 - Verkehrsdaten
(1) Verkehrsdaten dürfen außer in den in diesem Gesetz geregelten Fällen nicht gespeichert oder übermittelt werden und sind vom Anbieter nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Die Zulässigkeit der weiteren Verwendung von Verkehrsdaten, die nach Abs. 5 übermittelt werden, richtet sich nach den Vorschriften der StPO sowie des SPG.
…

§ 102a - Vorratsdaten
…
(7) Der Inhalt der Kommunikation und **insbesondere Daten über im Internet aufgerufene Adressen dürfen auf Grund dieser Vorschrift nicht gespeichert werden**.
(8) Die nach Abs. 1 zu speichernden Daten sind nach Ablauf der Speicherfrist unbeschadet des § 99 Abs. 2 **unverzüglich, spätestens jedoch einen Monat nach Ablauf der Speicherfrist, zu löschen**. Die Erteilung einer Auskunft nach Ablauf der Speicherfrist ist unzulässig.
(9) Im Hinblick auf Vorratsdaten, die gemäß § 102b übermittelt werden,

§ 102b – Auskunft über Vorratsdaten
(1) Eine Auskunft über Vorratsdaten ist ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt, zulässig.
(2) Die nach § 102a zu speichernden Daten sind **so zu speichern, dass sie unverzüglich an die nach den Bestimmungen der StPO und nach dem dort vorgesehenen Verfahren für die Erteilung einer Aus-**

kunft über Daten einer Nachrichtenübermittlung zuständigen Behörden übermittelt werden können.
(3) Die **Übermittlung der Daten** hat in **angemessen geschützter Form** nach **Maßgabe des § 94 Abs. 4** zu erfolgen.

§ 102c - Datensicherheit, Protokollierung und Statistik
(1) Die Speicherung der Vorratsdaten hat so zu erfolgen, dass eine **Unterscheidung von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherten Daten möglich ist**. Die Daten sind durch **geeignete technische und organisatorische Maßnahmen vor unrechtmäßiger Zerstörung, zufälligem Verlust oder unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung und Verbreitung zu schützen**. Ebenso ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass der **Zugang zu den Vorratsdaten ausschließlich dazu ermächtigten Personen unter Einhaltung des Vier-Augen-Prinzips** vorbehalten ist. Die **Protokolldaten sind drei Jahre ab Ende der Speicherfrist für das betreffende Vorratsdatum zu speichern**. Die Kontrolle über die Einhaltung dieser Vorschriften obliegt der für die Datenschutzkontrolle gemäß § 30 DSG 2000 zuständigen Datenschutzkommission. **Eine nähere Beschreibung des Sorgfaltsmaßstabs zur Gewährleistung der Datensicherheit kann der Bundesminister für Verkehr, Innovation und Technologie per Verordnung festschreiben**.
(2) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben zu gewährleisten, dass **jeder Zugriff auf Vorratsdaten sowie jede Anfrage und jede Auskunft über Vorratsdaten** nach § 102b **revisionssicher protokolliert** wird. Diese **Protokollierung umfasst**
1. die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Referenz zur staatsanwaltschaftlichen oder gerichtlichen Anordnung gemäß den Bestimmungen der StPO, die der Übermittlung der Daten zugrunde liegt,
2. in den Fällen des § 99 Abs. 5 Z 3 und 4 die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Aktenzahl der Sicherheitsbehörde,
3. das Datum der Anfrage sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft,
4. die nach Datum und Kategorien gemäß § 102a Abs. 2 bis 4 aufgeschlüsselte Anzahl der übermittelten Datensätze,
5. die Speicherdauer der übermittelten Daten zum Zeitpunkt der Anordnung der Übermittlung,
6. den Namen und die Anschrift des von der Auskunft über Vorratsdaten betroffenen Teilnehmers, soweit der Anbieter über diese Daten verfügt sowie
7. eine eindeutige Kennung, welche eine Zuordnung der Personen ermöglicht, die im Unternehmen des Anbieters auf Vorratsdaten zugegriffen haben.
(3) Die **Speicherung der Protokolldaten** hat so zu erfolgen, dass deren **Unterscheidung von Vorratsdaten sowie von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherter Daten möglich ist**.
(4) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben
1. für Zwecke der Kontrolle des Datenschutzes und zur Gewährleistung der Datensicherheit die **Protokolldaten** gemäß Abs. 2 **an die Datenschutzkommission und den Datenschutzrat** sowie
2. zum Zweck der Berichterstattung **an die Europäische Kommission und an den Nationalrat** die Protokolldaten gemäß Abs. 2 Z 2 bis 4 **an den Bundesminister für Justiz** zu übermitteln.
(5) Die Übermittlung der Protokolldaten hat auf s**chriftliches Ersuchen der Datenschutzkommission bzw. des Bundesministers für Justiz** zu erfolgen; die Übermittlung an den Bundesminister muss darüber hinaus jährlich bis zum 31. Jänner für das vorangegangene Kalenderjahr erfolgen.
(6) Über die Protokollierungspflichten nach Abs. 2 hinaus ist eine Speicherung der übermittelten Datensätze selbst unzulässig.

§ 14, 15 des Datenschutzgesetzes 2000 (in der Fassung vom 27.8.2011)

(Quelle: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597)

§ 14 - Datensicherheitsmaßnahmen
(1) Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind **Maßnahmen zur Gewährleistung der Datensicherheit** zu treffen. Dabei ist je nach der **Art der verwendeten Daten** und nach **Umfang und Zweck der Verwendung** sowie unter Bedachtnahme auf den **Stand der technischen Möglichkeiten** und auf die **wirtschaftliche Vertretbarkeit sicherzustellen**, daß die **Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, daß ihre Verwendung ordnungsgemäß erfolgt und daß die Daten Unbefugten nicht zugänglich sind**.

(2) Insbesondere ist, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist,

1. **die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,**
2. **die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,**
3. **jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,**
4. **die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,**
5. **die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,**
6. **die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,**
7. **Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,**
8. **eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.**

Diese Maßnahmen müssen unter Berücksichtigung des **Standes der Technik** und der bei der Durchführung erwachsenden **Kosten** ein Schutzniveau gewährleisten, das den **von der Verwendung ausgehenden Risiken** und der **Art der zu schützenden Daten angemessen** ist.

(3) Nicht registrierte Übermittlungen aus Datenanwendungen, die einer Verpflichtung zur Auskunftserteilung gemäß § 26 unterliegen, sind so zu **protokollieren**, daß dem Betroffenen Auskunft gemäß § 26 gegeben werden kann. In der Standardverordnung (§ 17 Abs. 2 Z 6) oder in der Musterverordnung (§ 19 Abs. 2) vorgesehene Übermittlungen bedürfen keiner Protokollierung.

(4) Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck - das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes - unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, daß es sich um die Verwendung zum Zweck der Verhinderung oder Verfolgung eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, handelt.

(5) Sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, sind **Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren**. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird.

(6) Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, daß sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können.

§ 15 - Datengeheimnis

(1) **Auftraggeber, Dienstleister und ihre Mitarbeiter** - das sind Arbeitnehmer (Dienstnehmer) und **Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis** - **haben Daten** aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, **geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht (Datengeheimnis)**.

(2) Mitarbeiter dürfen Daten **nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers** (Dienstgebers) **übermitteln**. Auftraggeber und Dienstleister haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, daß sie Daten aus Datenanwendungen nur auf Grund von Anordnungen übermitteln und das Datengeheimnis auch nach Beendigung des Arbeits(Dienst)verhältnisses zum Auftraggeber oder Dienstleister einhalten werden.

(3) Auftraggeber und Dienstleister dürfen Anordnungen zur Übermittlung von Daten nur erteilen, wenn dies nach den Bestimmungen dieses Bundesgesetzes zulässig ist. Sie haben die von der Anordnung betroffenen

Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.
(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur Datenübermittlung wegen Verstoßes gegen die Bestimmungen dieses Bundesgesetzes kein Nachteil erwachsen.

Polen

Artikel 180a und 180e des Telekommunikationsgesetzes (in der Fassung vom 1.1.2010)

(Quelle: http://www.en.uke.gov.pl/_gAllery/10/58/1058/telecommunications_law.pdf)

Article 160
1. An entity participating in the performance of telecommunications activities within public networks and entities cooperating with it **shall keep the telecommunications confidentiality**.
2. Entities referred to in paragraph 1 shall maintain due diligence, within the scope justified by technical or economic reasons, while securing telecommunications equipment, telecommunications networks and data collections from disclosing the telecommunications confidentiality.
3. A person coming into possession of a message not meant to be read by him/her when using radio or terminal equipment shall keep the telecommunications confidentiality. The provisions of Article 159 (3) and (4) shall respectively apply.
4. The recording of a message acquired in a manner described in paragraph 3 by a body executing control of telecommunications activities in order to document a violation of a provision of the Act, shall not be a violation of the telecommunications confidentiality.

Article 175
1. A provider of publicly available telecommunications services or an operator of a public telephone network shall undertake technical and organisational means in order to ensure the security of message transfer in relation to the services provided by them.
2. A service provider shall inform users, in particular in the case of a specific threat to the violation of service security, about the fact that technical means employed by it do not guarantee the security of message transfer, as well as with regard to existing possibilities to undertake such security and related costs.

Article 180a.
1. Subject to Article 180c (2) (2), an operator of a public telecommunications network and the provider of publicly available telecommunications services shall be obliged at their cost to:
1) retain and store data referred to in Article 180c generated in a telecommunications network or processed by that operator or provider, in the territory of the Republic of Poland, for the period of 24 months counted from the day of a call or an unsuccessful call attempt, and to erase the data as of the expiry of this period, excluding data protected under separate provisions.
2) make available the data referred to in point 1 to authorised entities as well as to the court and prosecutor under the terms and procedure specified in separate provisions;
3) protect data referred to in point 1 against accidental or unlawful destruction, loss or alternation, unauthorised or unlawful storage, processing, access or disclosure, in accordance with the provisions of Article 159-175 and Article 180e.
2. Subject to paragraph 3, the obligation referred to in paragraph 1 shall be considered as completed, if an operator of a public telecommunications network or the provider of publicly available telecommunications services in case they cease telecommunications activities submit the data to another operator of a public telecommunications network or the provider of publicly available telecommunications services for further storage, making available and protection.
3. If an operator of a public telecommunications network or the provider of publicly available telecommunications services was declared bankrupt, the bankrupt operator or provider shall have the obligation to submit the data referred to in paragraph 1 to the President of UKE for further storage, making available and protection.

4. The Prime Minister shall define, by means of an ordinance, the method of submitting data to the President of UKE in the case referred to in paragraph 3 as well as the method of making this data available by the President of UKE to entities referred to in paragraph 1 (2) in order to ensure that the tasks are performed by these entities.
5. Data on calls made and unsuccessful call attempts referred to in Article 159 (1) (5) shall be subject to the obligation referred to in paragraph 1.
6. The obligation referred to in paragraph 1 should be performed in a way that does not lead to a disclosure of a telecommunications message.
7. Making available the data referred to in paragraph 1 (1) may take place by means of a telecommunications network, unless otherwise provided for in separate provisions.

Article 180e. For the purposes of data protection referred to in Article 180a (1) (3) a telecommunications undertaking shall apply **appropriate technical and organizational measures** and shall provide **access to this data only to authorized employees.**

Slowakei

§§ 57 I, 59a Gesetz über die elektronische Kommunikation (in der Fassung vom 18.3.2010)

(Quelle: http://www.vyvlastnenie.sk/predpisy/zakon-o-elektronickych-komunikaciach/)

§ 57- Bezpečnosť a ochrana osobných údajov v prevádzke siete
(1) Podnik je povinný prijať zodpovedajúce technické a organizačné opatrenia na ochranu bezpečnosti svojich sietí, služieb alebo sietí a služieb, ktoré s ohľadom na stav techniky a náklady na realizáciu musia zabezpečiť úroveň bezpečnosti, ktorá je primeraná existujúcemu riziku.

§ 59a
…
(11) Podnik pri uchovávaní údajov podľa odseku 6 okrem splnenia povinnosti podľa § 57 ods. 1 zabezpečí, aby
a) uchovávané údaje mali rovnakú kvalitu a podliehali rovnakému zabezpečeniu a ochrane ako údaje podnikom spracúvané alebo uchovávané pri poskytovaní sietí alebo služieb,
b) údaje podliehali príslušným technickým opatreniam a organizačným opatreniam na ochranu údajov proti náhodnému alebo protiprávnemu zničeniu, náhodnej strate alebo zmene, neoprávnenému alebo protiprávnemu uchovaniu, spracovaniu, prístupu alebo zverejneniu,
c) údaje podliehali príslušným technickým opatreniam a organizačným opatreniam, ktoré zabezpečia, aby údaje mohli byť sprístupnené len oprávneným osobám konajúcim na základe poverenia alebo plnomocenstva podniku a oprávneným orgánom štátu a ich povereným alebo inak oprávneným príslušníkom, alebo zamestnancom,
d) údaje na konci doby určenej na ich uchovávanie boli zlikvidované okrem údajov, ktoré boli sprístupnené a zabezpečené.

Abschnitte 15 und 16 des Datenschutzgesetzes (zuletzt geändert durch Act No. 90/2005 Coll.)

(Quelle: http://www.dataprotection.gov.sk/buxus/docs/act_428.pdf)

Section 15 - Liability for Security of Personal Data
(1) The controller and the processor shall be responsible for **security of personal data by protecting them against accidental or unlawful damage or destruction, accidental loss, alteration, unauthorized access and making available, as well as against any other unauthorized forms of processing.**

For this purpose he shall take due technical, organizational and personal measures adequate to the manner of processing, while he shall take into account above all
a) the existing technical means,
b) the extent of possible risk that could violate security or functionality of the filing system,
c) confidentiality and importance of the processed personal data.
(2) The controller and the processor shall take the measures under Paragraph 1 in the form of a **security project** of the filing system (hereinafter the "Security Project") and they shall provide its development if
a) special categories of personal data under Section 8 are processed in the filing system and the filing system is interconnected with a publicly accessible computer network or it is operated in a computer network interconnected with a publicly accessible computer network,
b) special categories of personal data under Section 8 are processed in the filing system; in such case the controller and the processor shall only **document the taken technical, organisational and personal measures in the extent stipulated by Section 16 Paragraph 3 Subparagraph c) and Paragraph 6**; or
c) the filing system is used for safeguarding the public interest under Section 2 Paragraph 1; the provision of Section 16 shall not apply to development of the Security Project only provided that an obligation to elaborate a Security Project pursuant to a special Act simultaneously applies to the respective case.
(3) Upon request of the Office the controller and the processor shall prove the extent and contents of the taken technical, organisational and personal measures under Paragraph 1 or 2.
(4) If the subject of the inspection is constituted by the filing systems under Paragraph 2, the Office shall be entitled to request the controller or the processor for submittal of an evaluation report on the outcome of an audit of the filing system's security (hereinafter the "evaluation report"), provided that there are serious doubts about its security or about practical implementation of the measures referred to in the Security Project. The controller or the processor shall submit the evaluation report, not older than two years, to the Office without undue delay, otherwise he shall provide performance of an audit of the filing system's security at his own expense and submit an evaluation report within three months from the day of the obligation's imposition.
(5) The audit of the filing system's security may only be performed by an external, professionally qualified legal or natural person, who did not participate in development of the Security Project of the respective filing system and there are no doubts about its impartiality.

Section 16
Security Project
(1) The Security Project shall define the extent and manner of the technical, organisational and personal measures necessary for elimination and minimizing of the threats and risks affecting the filing system from the viewpoint of impairing its security, reliability and functionality.
(2) The Security Project shall be developed in accordance with the basic rules of filing system's security, the issued security standards, legal regulations and international treaties binding for the Slovak Republic.
(3) The Security Project shall include above all
a) a security policy,
b) analysis of the filing system's security,
c) security directives.
(4) The security policy shall specify the basic security objectives that must be achieved for protection of the filing system against violation of its security and it shall contain above all
a) specification of the **basic security objectives** and the **minimum required security measures**,
b) specification of the **technical, organisational and personal measures for ensuring protection of personal data in the filing system** and the manner of their use,
c) definition of the **filing system's environment and its relation to the possible security violation**,
d) definition of the limits determining residual risks.
(5) Analysis of the filing system's security shall mean a detailed analysis of the state of the filing system's security containing above all
a) **qualitative risk analysis**, within of which the threats affecting individual items of the filing system capable of violating its security or functionality are identified; the result of the qualitative risk analysis shall be a list of threats that could endanger confidentiality, integrity and availability of the processed personal data, while it shall also state the extent of the possible risk, proposals of the measures eliminating or minimizing the affect of the risk and a list of the remaining risks,
b) **use of security standards** and determination of other methods and means of the protection of personal data; evaluation of conformity of the proposed security measures with the applied security standards, methods and means shall constitute a part of the analysis of the filing system's security.
(6) Security directives shall specify and apply the **conclusions resulting from the Security Project** to the concrete conditions of the operated filing system and they shall include above all

a) description of the technical, organisational and personal measures defined in the Security Project and their use in concrete conditions,
b) the scope of powers and description of the permitted activities of individual entitled persons, the manner of their identification and authentication in accessing the filing system,
c) the scope of liability of entitled persons and of the personal data protection official (Section 19),
d) the manner, form and periodicity of performance of the inspection activities focused on observation of the filing system's security,
e) procedures during breakdowns, failures and other extraordinary situations including preventive measures for restricting the occurrence of extraordinary situations and possibilities of an effective restoration of the state before the breakdown.

Section 17 - Advice
The controller or the processor shall be obliged to advise the entitled persons on the rights and obligations stipulated by this Act and on the liability for their breach. The controller or the processor shall advise on the above before giving the first instruction to the entitled person to perform any processing operation with the personal data. The entitled person shall confirm the advice by his signature; the controller or the processor shall make a written record of the advice.
Section 18 - Obligation to Maintain Secrecy
(1) The controller and the processor shall be obliged to maintain secrecy about the personal data which they process. The obligation to maintain secrecy also applies after termination of the processing. The obligation to maintain secrecy shall not apply to them if pursuant to a special Act it is necessary for fulfilment of the tasks of the law enforcement agencies; this shall not affect provisions of special Acts.
(2) The entitled person shall be obliged to maintain secrecy about the personal data which he comes across; he must not use them even for his personal needs and he must not make them public, provide them or make them available to anybody without consent of the controller.
(3) The obligation to maintain secrecy under Paragraph 2 shall also apply to other natural persons, who come across the personal data at the controller's or processor's place within the framework of their activities (e.g. maintenance and service of the technical means).
(4) The obligation to maintain secrecy under Paragraph 2 shall also apply after termination of the function of the entitled person or after termination of his employment relationship or similar labour relation, as well as the civil service employment relationship or the relation under Paragraph 3.
(5) Paragraphs 1 to 4 and the obligation to maintain secrecy imposed on controllers, processors and entitled persons pursuant to special regulations23) shall not apply in respect of the Office in the course of fulfilment of its tasks (Sections 38 to 44).

Slowenien

Artikel 107a Absatz 6 und Artikel 107c des Gesetzes über die elektronische Kommunikation (in der Fassung vom 1.2.2007)

(Quelle: http://www.apek.si/sl/datoteke/File/2007/osebna%20izkaznica/electronic_communications_act_official_consolidated_version_zekom-upb1_unofficial_translation_english.pdf)

Article 107a - general provisions on retained data
(1) Operators shall be obliged for the purposes of acquiring data on traffic in electronic communications networks as stipulated by the law governing the criminal procedure, for the purposes of ensuring national security and the constitutional order, and the security, political and economic interests of the state, as stipulated by the law governing the Slovenian Intelligence-Security Agency, and for the purposes of national defence as stipulated by the law governing defence of the state, to retain data from Article 107b of this Act if they create or process them in providing the associated public communications services.

(2) The obligation from the previous paragraph shall also include the retention of data on unsuccessful calls, where the operator creates or processes and retains or records such data in providing the associated public communications services, but shall not include the retention of data on connections that were not successfully established and the contents of communications.
(3) Operators may join together to ensure the retention of data from Article 107b. The Agency may instruct an operator by a decision to ensure retention for other operators, if appropriate and necessary with regard to the mutual business relations of operators. The decision shall also rule on reasonable costs of the operator charged with data retention.
(4) Operators shall ensure the retention of data from the first, second and third paragraphs of this Article in accordance with the provisions of this Act for a period of 24 months from the date of communication.
(5) The competent body that decides on access to data from the first paragraph of this Article may at the suggestion of the proposer of the order for access to data, extend the duration of retention for a limited period, if justified by the specific circumstances of criminal prosecution stipulated by the law governing the criminal procedure, ensuring national security and the constitutional order and the security, political and economic interests of the state as stipulated by the law governing the Slovenian Intelligence-Security Agency, and national defence as stipulated by the law governing national defence. The competent body deciding on access to data shall inform the ministry and the information commissioner thereof. The ministry shall officially inform the European Commission and other European Union member states of the extension, and state the grounds for the extension. Implementation of the measure shall cease immediately the special circumstances cease to apply or when the competent body that decided on the extension receives notification from the European Commission that the measure is impermissible.
(6) Operators shall be obliged at the end of the retention period to destroy all data retained in accordance with the provisions of this Act, except for such data for which an access order was granted and which was sent to the competent body.

Article 107c - protection of retained data
(1) Operators shall ensure the **protection of retained data in accordance with the law governing the protection of personal data**. In connection with this, each operator alone or together shall adopt **appropriate technical and organisational measures to protect the retained data against destruction, loss or alteration, and unauthorised or unlawful forms of storage, processing, access or disclosure.**
(2) Operators may process retained data only to the extent necessary to ensure retention.
(**3) Retained data must be of the same quality as data in the network. The provisions of this Act on the security and protection of data in the network shall apply to retained data.**

Artikel 24, 25 des Datenschutzgesetzes (in der Fassung vom 15.7.2004)

(Quelle: http://ec.europa.eu/justice/policies/privacy/docs/implementation/personal_data_protection_act_rs_2004.pdf)

Article 24
(1) Security of personal data comprises organisational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data:
1. by protecting premises, equipment and systems software, including input-output units;
2. by protecting software applications used to process personal data;
3. by preventing unauthorised access to personal data during transmission thereof, including transmission via telecommunications means and networks;
4. by ensuring effective methods of blocking, destruction, deletion or anonymisation of personal data;
5. by enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data.
(2) In cases of processing of personal data accessible over telecommunications means or network, the hardware, systems software and software applications must ensure that the processing of personal data in filing systems is within the limits of authorisations of the data recipient.
(3) The procedures and measures to protect personal data must be adequate in view of the risk posed by processing and the nature of the specific personal data being processed.

(4) Functionaries, employees and other individuals performing work or tasks at persons that process personal data shall be bound to protect the secrecy of personal data with which they become familiar in performing their functions, work and tasks. The duty to protect the secrecy of personal data shall also be binding on them after termination of their function, work or tasks, or the performance of contractual processing services.

Article 25
(1) Data controllers and data processors shall be bound to ensure the protection of personal data in the manner set out in Article 24 of this Act.
(2) Data controllers shall prescribe in their internal acts the procedures and measures for security of personal data and shall define the persons responsible for individual filing systems and the persons who, due to the nature of their work, shall process individual personal data.

Spanien

Articulo 8 Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (in der Fassung vom 19.10.2007)

(Quelle: http://www.boe.es/boe/dias/2007/10/19/pdfs/A42517-42523.pdf)

Artículo 8 - Protección y seguridad de los datos
1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.
2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.
3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.
4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley.

Articulos 4, 9, 22 und 23 Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (in der Fassung vom 14.12.1999)

(Quelle: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf)

Artículo 4 - Calidad de los datos
1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.
5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.
6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 9 - Seguridad de los datos
1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán **adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.**
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
3. Reglamentariamente se establecerán los requisites y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10 - Deber de secreto
El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de character personal están obligados al secreto profesional respect de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 22 - Ficheros de las Fuerzas y Cuerpos de Seguridad
1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.
2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas
están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión
de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.
3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente
en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensions formuladas en su caso por los interesados que
corresponden a los órganos jurisdiccionales.
4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusion de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23 - Excepciones a los derechos de acceso, rectificación y cancelación
1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del BOE núm. 298 Martes 14 diciembre 1999 43093 artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de
terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones
tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.
3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del
Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Ungarn

Article 157 of Act C/2003 on electronic communications (in der Fassung vom 24.11.2003)

(Quelle: http://www.ictregulationtoolkit.org/en/Document.2347.pdf)

Article 4 – Duties of the Government
(1) The Government shall
…
g) specify the fundamental principles associated with the security of electronic communications and the regime of making preparations for qualified periods, putting in place the conditions for the duties to be performed by public administration;
…

Article 2 Government Decree 226/2003 (in der Fassung vom 13.12.2003)

(Quelle: http://www.nhh.hu/dokumentum.php?cid=10781&letolt)

Article 2
(1) The service provider shall **select and operate the electronic communications devices used for the management of personal data during the provision of the service in such a way that**
***a)* the managed data are available to the authorized persons (availability),**
***b)* the authenticity and authentication of the managed data are ensured (authenticity of data management),**
***c)* the consistency of the managed data can be proven (data integrity),**
***d)* the managed data are protected against unauthorized access (confidentiality of data).**
(2) The service provider shall ensure the protection of the security of data management with technical and organizational measures that provide a level of protection corresponding to the risks arising in connection with data management.

Article 7, 10 Act LXIII/1992 on Data Protection (in der Fassung vom 17.11.1992)

(Quelle: http://abiweb.obh.hu/dpc/index.php?menu=gyoker/relevant/national/1992_LXIII)

Article 7 – Quality of Data
(1) Personal data undergoing processing shall be:
a) obtained and processed fairly and lawfully,
b) accurate, complete and, where necessary, kept up to date,
c) stored in a way that allows identification of data subjects for no longer than it is required for the purpose for which these data are stored.
(2) The application of general and uniform personal identification codes which can be used without restriction shall be prohibited.

Article 10 – Data Security
(1) The data controller and, within its scope of activities the technical data processor, shall ensure **data security** and shall **take all technical and organisational measures** and elaborate the rules of procedure necessary to enforce compliance with this Act and other rules pertaining to data protection and confidentiality.
(2) Data shall be protected in particular against unauthorised access, alteration, transfer, making public, deletion or destruction, as well as against accidental destruction or damage. If personal data are transferred via a network or other information technology equipment, the data controller, technical data processor and the operator of the telecommunications or information technology equipment shall take special protective measures to ensure the technical protection of personal data.

Überblick über die praktische Umsetzung der sicherheitstechnischen und organisatorischen einzelstaatlichen Vorgaben

(mit Ausnahme von Österreich und Portugal)

Ohne Anspruch auf Vollständigkeit!

Quelle: Anhang des Berichts 1/2010 der Artikel-29-Datenschutzgruppe (Stand: Juli 2010)

	Logische Sicherheitsmaßnahme	Physische Sicherheitsmaßnahmen	Spezifische Personalschulung	Backup und Disaster Recovery	Datentrennung	Übermittlung an die Ermittlungsbehörde	Speicherung im Ausland
Belgien	Keine Verschlüsselung von Verkehrsdaten Zugriff auf die Daten strengstens beschränkt(ID/PW) Risikobewertung (50%) Sicherheits-Zertifizierung (50%) Verantwortlicher für IT-Sicherheit (CISO) benannt Penetrationstest Zugriffs-Protokollierung (Administratoren werden nicht geloggt)	Zutrittskontrolle mit Chipkarten System gegen Einbrecher Videoüberwachung Alarmzentrale Wächter Brandmeldeanlagen, Hochwasserschutz (50%)	Ja	Backup (100%) Disaster Recovery (50%)	Ja	Fax/Brief	Nein
Bulgarien	Keine Verschlüsselung Zugangsbeschränkung Protokollierung des Zugriffs auf Verkehrsdaten	Alarmanlage, physische Zutrittskontrolle Videoüberwachung, Brandschutzmaßnahmen Wächter	Keine Details	Backup (100%) Recovery Systeme (Keine Angaben)	Ja		In Einklang mit internationalen Abkommen
Cypern	Verschlüsselung nur bei Übermittlung Zugriff auf die Daten strengstens beschränkt(ID/PW) Zugriffs-Protokollierung (50%) Risikoanalyse (50%) Audit (50%) Keine Sicherheitszertifizierung Kein Penetrationstest	Zutrittskontrolle mit Chipkarten System gegen Einbrecher Videoüberwachung Wächter	Ja	Backup (100%) Disaster Recovery (nur einer)	Ja (2/3)	Überbringung durch Angestellten	Nein
Dänemark	Risikoanalyse (2/3) Audit (2/3) Sicherheitszertifizierung (1/3) Verantwortlicher für IT-Sicherheit (CISO) benannt Schwachstellenanalyse (1/3) Zugriff auf die Daten strengstens beschränkt(ID/PW) Zugriffs-Protokollierung (2/3)	Zutrittskontrolle mit Chipkarten System gegen Einbrecher	Ja	Backup (100%)	Ja (2/3)	Brief	Nein
Deutschland	Risikoanalyse Penetrationstests Zugriff auf die Daten strengstens beschränkt(ID/PW) Zugriffs-Protokollierung	Datenzentren sind hochsicher (Alarm, Vieoüberwachung, automatische Feuerlöschsysteme)	Ja	Backup-Systeme, teilweise verschlüsselt	Ja	Fax, CD oder DVD per Post mit PGP verschlüsselte E-Mail	Nein
England	Verschlüsselung nur bei Übermittlung Keine gesonderten Sicherheitsmaßnahmen für Verkehrsdaten Risikoanalyse ISO 27001-Zertifizierung (50%) Intrusion Detection System Zugriff auf die Daten strengstens beschränkt(ID/PW) Zugriffs-Protokollierung	Umzäunung Sichere Hosting-Umgebung Alarm Videoüberwachung Zutrittskontrolle 24 Stunden Polizeischutz	Nein	Backup (100%) Recovery Systeme (Off-Site Backup)	Unterschiedlich, teilweise physische Trennung	Bevorzugt elektronisch mittels SSL, Fax und E-Mail	Nein

	Logische Sicherheitsmaßnahme	Physische Sicherheitsmaßnahmen	Spezifische Personalschulung	Backup und Disaster Recovery	Datentrennung	Übermittlung an die Ermittlungsbehörde	Speicherung im Ausland
Estland	Nur ein Teil der Daten verschlüsselt Gesondertes Risikomanagement (ein Fall) Interner Audit Keine Sicherheitszertifizierung Verantwortlicher für IT-Sicherheit (CISO) benannt (Fall) Zugriff auf die Daten strengstens beschränkt(ID/PW) Zugriffs-Protokollierung (nicht alle)	Physisch geschützte Serverräume Zutrittsbeschränkung Feuer- und Einbruchalarm	Nein	Zentrales Backup, Backup-Politik, automatischer Lebenszyklus von Backup-Kopien	Ja, physische und logische Trennung	Brief, direkter Zugriff, elektronisch über HTTPS	Ein Fall (in EU)
Finland	Verschlüsselung nur bei Übermittlung Risikoanalyse IT-Sicherheit-Audits Zugang zu Daten ist beschränkt (ID/PW) Kein konsolidiertes Log-Handling für Auditing-Zwecke	Niedergeschriebene Verfahren	Ja	Backup	Nein	PGP	Nein
Frankreich	Verschlüsselung nur bei Übermittlung Keine gesonderten Sicherheitsmaßnahmen für Verkehrsdaten Penetrationstest Schwachstellenanalyse Zugang zu Daten ist beschränkt (ID/PW) Zugriffs-Protokollierung	Einbruchalarm Zutrittskontrolle mit Chipkarten oder speziellen Schlüsseln Videoüberwachung Brandschutz für Server und Backups	Nein	Backup (100%) Recovery Systeme (keine Details)	Ja	Fax, verschlüsselte E-Mail	Nein
Griechenland	Keine Verschlüsselung Zugangskontrolle Audit-Trail Verwendung sicherer Kommunikationskanäle Risikoanalyse Interne Audits Sicherheitszertifizierung (nur einer) Verantwortlicher für IT-Sicherheit (CISO) benannt Penetrationstest/Schwachstellenanalyse (30%) Zugang zu Daten ist beschränkt (ID/PW) Zugriffs-Protokollierung (login-logout, nicht die Aktionen des Eingeloggten)	Keine gesonderten physischen Sicherheitsmaßnahmen für Verkehrsdaten	Nein	Backup (100%) Recovery Systeme (keine Details)	Nein	Gesiegelte Umschläge, E-Mail, Fax, verschlüsselte E-Mail	Ein Fall (in EU)
Irland	Zugang zu Daten ist beschränkt Zugangsprotokollierung Keine gesonderten Risiko-Studien Sicherheitszertifizierung Verantwortlicher für IT-Sicherheit (CISO) benannt	Speicherung der Daten auf zweckbestimmten Systemen Videoüberwachung	Ja	Backup (100%) Disaster Recovery (keine gesonderte für Verkehrsdaten)	Nein	Verschlüsselte E-Mail	Nein
Italien	Verschlüsselung nur bei Übermittlung Verwendung von sicheren Protokollen zur Datenübermittlung Risikoanalyse Starke (biometrische)Authentifizierung Antiviren-Software	H24 monitoring Zutrittskontrolle Einbruchsalarm Videoüberwachung Brandmeldeanlagen Zutrittsbeschränkung in bestimmten	Ja	Backup (100%) Recovery Systeme	Ja	Fax, zertifizierte E-Mail	Nein

	Logische Sicherheitsmaßnahme	Physische Sicherheitsmaßnahmen	Spezifische Personalschulung	Backup und Disaster Recovery	Datentrennung	Übermittlung an die Ermittlungsbehörde	Speicherung im Ausland
	Intrusion Detection System Zugriffs-Protokollierung	Bereichen					
Lettland	Teilweise Verschlüsselung (10%), Übermittlungsverschlüsselung (100%) IT-Sicherheitspolitik IT-Sicherheitsaudits Externe Audits nur bei großen Betreibern Keine Zertifizierung Zugang zu Daten ist beschränkt 1/3 der Anbieter speichern keine Log-Files	Zutrittskontrolle (Code, Magnetkarten etc.) Videoüberwachung Alarmanlagen Sicherheitspersonal/Wächter	Nein	Backup (81% der Anbieter, kleine Anbieter verfügen über keine Backup-Lösungen)	62 % speichern die Vorratsdaten nicht separat	Postweg oder elektronisch	Ja (in EU)
Litauen	Teilweise Verschlüsselung Antiviren-Software, Zugang zu Daten ist beschränkt Zugriffs-Protokollierung, Penetrationstests (ein Unternehmen), Audits, ISO 27001-Zertifizierung (ein Unternehmen) Verantwortlicher für IT-Sicherheit (CISO) benannt Kein Intrusion Detection System	Zutrittskontrolle (Magnetkarten) Videoüberwachung Sicherheitspersonal 24h im Einsatz Feueralarm und Brandbekämpfungssystem; Anlage zur unterbrechungsfreien Stromversorgung	Nein	Backup (100%) Recovery Systeme (außer ein Unternehmen)	Ja	Hardcopy, verschlüsselte E-Mail, mit HTTPS gesichertes Web-Interface (Übertragungskanal mit SSL verschlüsselt)	Ein Fall (in EU)
Luxemburg	Verschlüsselung Keine gesonderten Sicherheitsmaßnahmen Keine Risikoanalyse Sicherheits-Audit (ein Unternehmen) Keine Zertifizierung Zugangskontrolle Zugangsprotokollierung	Niedergeschriebene Verfahren (nur zwei Anbieter) Zutrittskontrolle mit Chipkarten Brandschutzsystem und Einbruchsalarmsystem Backups an anderem Ort (nicht alle)	Ja (nicht alle)	Backup Systeme (Backups werden durch Überschreiben gelöscht) Kein Betriebskontinuitätsmanagement (drei Anbieter speichern Backups in separaten Standorten)	Ja (nur zwei)	Hardcopy, CD, USB-Stick	Zwei Anbieter speichern Daten in Belgien
Malta	Verschlüsselung Zugang zu Daten ist beschränkt (ID/PW) Zugriffs-Protokollierung Keine gesonderten Sicherheitsmaßnahmen Audit Risikoanalyse Verantwortlicher für IT-Sicherheit (CISO) benannt (ein Unternehmen) Keine Sicherheitszertifizierung Intrusion Detection System	Zutrittskontrolle mit Magnetkarten Videoüberwachung Sicherheitspersonal System gegen Einbrecher Niedergeschriebene Verfahren	Ja	Backup (nur ein Unternehmen)	Ja (nicht alle)	Hardcopy, CD, E-Mail, Softcopy	Ja (in EU)
Niederlande	Nur teilweise Verschlüsselung Risikoanalyse Interne und externe Informationssicherheits-Audits ISO 27001-Zertifizierung (ein Unternehmen) Verantwortlicher für IT-Sicherheit (CISO) benannt Schwachstellenanalyse Zugriffs-Protokollierung	Verschiedene physische Sicherheitsmaßnahmen, z.B. speichern Betreiber Verkehrsdaten in hochsicheren Datenzentren	Ja	Unterschiedliche Strategien, z.B. redundante Speicherung an zwei Orten	Ja, Speicherung in separaten Datenbanken	PGP	Nein

	Logische Sicherheitsmaßnahme	Physische Sicherheitsmaßnahmen	Spezifische Personalschulung	Backup und Disaster Recovery	Datentrennung	Übermittlung an die Ermittlungsbehörde	Speicherung im Ausland
Polen	Verschlüsselung nur bei Übermittlung Keine gesonderte Sicherheitspolitik für Verkehrsdaten Risikoanalyse Sicherheits-Audits Interne und externe Zertifizierung Verantwortlicher für IT-Sicherheit (CISO) benannt Intrusion Detection/Prevention Systeme Zugriff auf die Daten beschränkt (ID/PW) Zugriffs-Protokollierung (in einem Fall unveränderlich)	Alarmanlage Videoüberwachung Zutrittskontrolle Redundante Stromversorgung für bestimmte Sicherheitszonen Feueralarm	Ja	Backup (100%) Disaster Recovery (nur ein Anbieter)	Nein	Verschlüsselte, authentifizierte E-Mails	Nein
Portugal	Keine Informationen						
Rumänien	Teilweise spezifische Prozesse für Verkehrsdaten Periodische Risikoanalyse Nur ein Anbieter sicherheitszertifiziert Zugriff auf die Daten beschränkt (ID/PW) Keine Verschlüsselung Keine unabhängigen Penetrationstests oder Schwachstellenanalysen Authentifizierung der Systemadministratoren mit Benutzername und Passwort Protokollierung von (Login, Logout, Änderung des Passworts)	Videoüberwachung Erdbebenschutz Feueralarm und Brandbekämpfungssystem Keine niedergeschriebene Sicherheitspolitik	Ja	Periodisches Backup, Disaster Recovery (heißer Standort in einer anderen Stadt, kontinuierliche Synchronisierung)	Ja	Briefpost, elektronisch verschlüsselt	Nein
Slowakei	Verschlüsselung der Datenbank (mit zwei Ausnahmen) Verschlüsselung bei Übertragung (alle) Regelmäßige Sicherheits-Audits und Sicherheitsanalysen Zertifizierung (ein Unternehmen) Verantwortlicher für IT-Sicherheit (CISO) benannt Regelmäßige unabhängige Penetrationstests Zugriff auf die Daten strengstens beschränkt (ID/PW/Token) Zugriffs-Protokollierung (mit einer Ausnahme)	Zutrittsbeschränkung Sicherheitspolitik als Geschäftsgeheimnis (wird nicht veröffentlicht)	Ja	Backup (100%) Recovery Systeme	Ja	Verschlüsselte E-Mail	Ja (in EU)
Slowenien	Informationssicherheits-Management Systeme, angepasst an ISO 27001 (große Unternehmen) Zweckbestimmte Speicherlösung: WORM, CAS (große Unternehmen)	Informationssicherheits-Management Systeme, angepasst an ISO 27001 (große Unternehmen) Zweckbestimmte Speicherlösung: WORM, CAS (große Unternehmen)	Ja	Ja	Ja	Postversand von Hardcopy oder tragbaren elektronischen Medien, sichere E-Mail	Nein
Spanien	Keine Verschlüsselung (nur ein Unternehmen) Zugriff auf die Daten Daten beschränkt (ID/PW) Zugriffs-Protokollierung Keine gesonderten Sicherheitsvorkehrungen für Verkehrsdaten	Zutrittskontrolle mit Magnetkarten System gegen Einbrecher Videoüberwachung Alarmzentrale Wächter	Ja	Backup (100%) Recovery Systeme (außer einer)	Ja	Persönliche Übergabe, Zertifizierte, verschlüsselte E-Mail	Nein

	Logische Sicherheitsmaßnahme	Physische Sicherheitsmaßnahmen	Spezifische Personalschulung	Backup und Disaster Recovery	Datentrennung	Übermittlung an die Ermittlungsbehörde	Speicherung im Ausland
	Interne Audits Keine Zertifizierung Verantwortlicher für IT-Sicherheit (CISO) benannt Penetrationstests Intrusion Detection System	Niedergeschriebene Verfahren					
Tschechien	IT-Sicherheitsbeauftragter Sicherheits-Audits (50%) Sicherheitszertifizierung (50%)		Ja	Notfallplan	Ja	Persönliche Übergabe (ein Unternehmen), meist digitale Übermittlung über elektronische Kanäle	Nein
Ungarn	Protokollierung Trennung der IT-Systeme	Server stehen physisch in hochsicheren Bereichen Zutrittsbeschränkung mittels Schlüssel Videoüberwachung Wächter	Datenanfragen werden von Personen bearbeitet, die bestimmte Sicherheitsausbildung absolviert haben (*„C" type national security clearance*) zudem Trainings	Nur wenige Unternehmen verfügen über einen eigenen Recovery Plan (aber: keine Veröffentlichung der Pläne)	Rechnungsdaten und Vorratsdaten werden getrennt gespeichert		Nein

Eigene Erhebungen zur praktischen Umsetzung der sicherheitstechnischen und organisatorischen Vorgaben

in Deutschland (Deutsche Telekom AG)

und

Bayern (R-Kom GmbH & Co. KG, JonDos GmbH)

	Telekom	R-Kom	JonDos
Infrastruktur	Sammlung der Daten aus dem Billingprozess und direkt aus datenerzeugenden Netzelementen, Datenbevorratung in Hochsicherheitszentren	Speicherung der Vorratsdaten auf einem Cluster aus NetApp Appliances	Erhebung der Daten und Speicherung auf dem ersten und letzten Mix einer Kaskade (nur zwei Mixe)
Datentrennung	Physisch und logisch	Logisch	Daten wurden von kostenfreien Servern gespeichert, auf denen sonst keine anderen Daten vorliegen
Entkopplung der Systeme vom Internet	Ja	Ja	nein
Verschlüsselung	Einführung einer Verschlüsselung war geplant	Nein	Asymmetrisch, privater Schlüssel getrennt verwahrt auf Chipkarte
Logische Maßnahmen zur Zugriffsbeschränkung	Nutzer- und Rechtekonzepte (personengebundene Accounts, Passwortschutz (inkl. Passwortrichtlinien und begrenzter Lebenszeit von Passwörtern), Zugriff nur für speziell autorisiertes Personal mittels personengebundener Accounts über speziell autorisierte Arbeitsplätze (Rechnerbindung mittels IP-Adresse), Verschlüsselter Zugang (https) via Intranet, Qualitätssicherungsmaßnahmen im Rahmen eines internen Kontrollsystems (IKS) analog S-OX (Festnetz/Internet)	Zugriff über dedizierten Rechner, der über Storage-VLAN Zugriff auf die Daten hatte, Zugang auf diesen Rechner via ssh und public-key Authentifizierungsverfahren	Zugriff mittels Chipkarte
Berechtigte Mitarbeiter	Speziell für die Beantwortung von Auskunftsersuchen zuständige Mitarbeiter (Ü1 oder Ü2 sicherheitsüberprüft), kein direkter Zugriff von Ermittlungsbehörden auf die Verkehrsdaten	Nur eingewiesene Mitarbeiter, die sich zuvor schriftlich zur Einhaltung des von der BNetzA vorgegebenen Geheimhaltungsgrades VS verpflichtet haben	
Zugriffsprotokollierung	Zugriffsprotokollierung mit Deanonymisierung bei Missbrauchsverdacht Erstellung, Veränderung oder Löschung der auf Vorrat gespeicherten Verkehrsdaten auf Nutzerebene ist nicht möglich Protokollierung des Lesezugriffs auf die Daten im Festnetzbereich und der Benutzerdaten der handelnden Personen, Archivierung der Protokolldaten auf speziellem Loggingserver (auffindbar, nachvollziehbar, unveränderbar, verfälschungssicher), der in unabhängigem Administratorbereich verantwortet wird Auch Protokollierung der Zugriffe durch Systemadministratoren	Zugriffsprotokollierung über Log-Files, die im Versionierungstool cvs revisionssicher abgelegt wurden	Im Prototypen war keine Protokollierung vorgesehen
Löschung	Löschung erfolgt mit Ablauf der vorgesehenen Speicherdauer durch Überschreiben mit neuen Datensätzen (Freigabe führt auf Dauer zu einer mehrfachen Überschreibung der alten Datensätze)	Automatisierte Löschung anhand eines Zeitstempels im Dateinamen	Keine automatisierte Löschung
Redundanten Speicherung	Im Mobilfunk ja, im Festnetz Testrecovery von Teildaten analog zum SOX-Verfahren	Storagesystem war ein Cluster aus FAS 2020 Appliances von NetApp mit den dort verfügbaren Techniken für eine sichere und redundante Speicherung	k.A.
Signaturverfahren und sonstige Techniken zur Integritätssicherung	Gewährleistung der Integrität durch ausschließliches Halten in eigenen Netzen und Systemen und konsequent restriktivem Zugriffsmanagement	Es wurden die Richtlinien nach § 45g des TKG (Verbindungspreisberechnung) eingehalten	k.A.

	Telekom	R-Kom	JonDos
Übermittlungstechniken	Datenübertragung grds. als Papierausdruck oder Datei auf Datenträger per Post, zunehmend als Datei per Email, PGP verschlüsselt in eiligen Fällen per Fax mit zwingender Aufforderung, den (ordnungsgemäßen) Empfang des Faxes umgehend zu bestätigen	VS, keine Angaben	Signierung und Verschlüsselung der Daten durch einzelne Mixbetreiber mit GPG und Übertragung an die Behörde, diese muss die Daten dann zusammensetzen
Gewährleistung der Zweckbindung und Rechtmäßigkeit	Anfragen der berechtigten Stellen werden einer qualifizierten Prüfung unterzogen, um missbräuchliche oder erkennbar rechtswidrige Maßnahmen auszuschließen, Bei Zweifel Rückfrage bzw. Hinweis an die erlassende Stelle In Fällen offenkundiger Rechtswidrigkeit (z.B. Überwachungsanordnung nur durch Polizeibeamten) wird Umsetzungsmaßnahme verweigert	Beantwortung schriftlicher Anfragen ausschließlich nach individueller Prüfung	Daten müssen bei Anfragen des Staatsanwalts immer herausgegeben werden, Zweckbindung und Rechtmäßigkeit kann nur im Nachhinein vor Gericht festgestellt werden
Authentifizierung	Anfragende Behörden in der Regel bekannt und durch konkrete Adressierung der Datenlieferung bestimmt Bei unbekannten Anfragern erfolgt Identitätsabklärung	VS, keine Angaben	Anruf bei der entsprechenden Behörde und dem jeweiligen Staatsanwalt
Automatisierung	Keine automatisierte Beantwortung von Verkehrsdatenabfragen	Beantwortung manueller Anfragen unter Einbeziehung der Datenschutzbeauftragten	k.A.
Streubreite der Anfragen	Anfragen betreffen meist eine (oder mehrere) konkrete Kennung(en) und einen bestimmten Zeitraum, im Mobilfunk zunehmend Anordnungen, die die zu beauskunftenden Telekommunikationsvorgänge lediglich durch räumlich und zeitliche Bezeichnung bestimmen	VS, keine Angaben	k.A.

Fragenkatalog Deutsche Telekom AG

Vorfragen

a) Hat die Telekom die Speicherung der Daten selbst übernommen oder an einen Dritten outgesourced?
Aus Sicherheits-, Effizienz-, Qualitäts- und Datenschutzgründen wurden keine konzernexternen Dienstleister mit der Speicherung und Verarbeitung der Verkehrsdaten betraut. Die Deutsche Telekom hat Verkehrsdaten ihrer Teilnehmer im Rahmen der §§ 113a, 113b TKG (alt) selbst gespeichert. Die Speicherung erfolgte in eigenen Speichersystemen in Deutschland.

b) Wie viel musste Telekom zur Umsetzung der gesetzlichen Vorgaben des § 113a TKG investieren?
Ca. 5,2 Mio. € einmaliger Invest zuzüglich erhöhter Betriebskosten in Höhe von ca. 3,7 Mio. € p.a.

1. Fragen zur Speicherung und Aufbewahrung der Daten

1.1 Fragen zur Vertraulichkeit der Daten

a) Wie lässt sich die Infrastruktur skizzieren, innerhalb derer die Daten gespeichert wurden (logisch und physisch, alle Arten von Verkehrsdaten)?
Relevante Verkehrsdaten im Sinne des § 113a TKG (alt) wurden überwiegend aus dem Billingprozess, teilweise aber auch direkt aus den datenerzeugenden Netzelementen ausgeleitet und separat abgelegt.

b) Wurden die Daten physisch / logisch getrennt von anderen Daten (z.B. nach § 96 TKG gespeicherten Verkehrsdaten) gespeichert?
Verkehrsdaten im Sinne des § 113a TKG (alt) wurden physisch und logisch getrennt von anderen Verkehrsdaten auf eigener Hardware gespeichert.

c) Sind die Systeme, auf denen die Daten gespeichert wurden, vom Internet entkoppelt?
Ja.

d) Wurden die Daten verschlüsselt gespeichert? Wenn ja, mit welchen Verschlüsselungsverfahren (symmetrisch oder asymmetrisch) und wie wurden die Schlüssel verwahrt (getrennt, nicht getrennt)?
Einführung einer Verschlüsselung war geplant.

e) Wie erfolgte der Zugriff auf die Daten (Authentifizierungsverfahren)?
Zugriff auf VDS-Daten erhielten nur die Unternehmensmitarbeiter, welche für die Beantwortung von Auskunftsersuchen berechtigter Stellen zuständig sind. Diese Mitarbeiter sind Ü1 – teilweise auch Ü2 – sicherheitsüberprüft. Durch die Einführung von Nutzer- und Rechtekonzepten für jede Vorratsdatenspeicherungsplattform ist gewährleistet, dass nur autorisiertes Personal mittels personengebundener Accounts über speziell autorisierte Arbeitsplätze Zugriff auf die Verkehrsdaten haben. Die technischen Sicherheitsmaßnahmen können grob vereinfacht wie folgt dargestellt werden:

- Datenbevorratung erfolgt in Hochsicherheitszentren
- Verschlüsselter Zugriff (https) via Intranet
- Personengebundene Accounts
- Passwortschutz (entsprechend Passwortrichtlinien, begrenzte Lifetime von Passwörtern)
- Rechnerbindung mittels IP-Adresse
- Zugriffsprotokollierung mit Deanonymisierung bei Missbrauchsverdacht
- Qualitätssicherungsmaßnahmen im Rahmen eines Internen Kontrollsystems (IKS) analog S-OX (Festnetz/Internet)

f) Wer im Unternehmen durfte / konnte auf die Daten zugreifen?
Siehe Antwort zu 1.1. e).

g) Wie ist der Zugriff durch Ermittlungsbehörden technisch realisiert?
Ermittlungsbehörden erhielten und erhalten keinen direkten Zugriff auf Verkehrsdaten. Die Deutsche Telekom führt die angeordneten Recherchen in den Datensätzen sowie die Beauskunftung nach Prüfung der Rechtmäßigkeit der Anordnung selbst durch. Zur Übermittlung der Daten an die berechtigte Stelle siehe

unten Frage 2 a). Ein Sonderfall ist der Fall der TKÜberwachung, bei der mit den Inhaltsdaten zugleich auch die Verkehrsdaten ausgeleitet werden. Für die Übermittlung dieser Daten gelten insoweit die Anforderungen der §§ 7 und 8 TKÜV. Nach bestehender Rechtslage können berechtigte Stellen ferner verlangen, dass im Mobilfunk Verkehrsdaten zur Erhebung von Standortdaten des Betroffenen in Echtzeit an sie übermittelt werden, vgl. § 100g Abs. 1 Satz 3 StPO. Mangels technischer Vorgaben wird dies derzeit noch von keinem Unternehmen praktiziert.

h) Wie wurde der Zugriff auf die Daten protokolliert? Ist das Protokoll revisionssicher?
Eine Erstellung, Veränderung oder Löschung der auf Vorrat gespeicherten Verkehrsdaten auf Nutzerebene ist nicht möglich. Der Lesezugriff auf die Daten sowie die Benutzerdaten der handelnden Person wird im Festnetzbereich protokolliert. Die Protokolldaten werden auffindbar, nachvollziehbar, unveränderbar und verfälschungssicher auf einem speziellen Loggingserver archiviert, welcher in einem von der Vorratsdatenspeicherung unabhängigen Administrationsbereich verantwortet wird. Dies gilt auch für Zugriffe durch Systemadministratoren.

i) Wie wurden die Daten gelöscht? Erfolgte die Löschung automatisiert (Zeitstempel an den Daten)?
Verkehrsdaten, welche gemäß § 113a TKG (alt) gespeichert waren, wurden mit Ablauf der vorgesehenen Speicherdauer durch Überschreiben mit neuen Datensätzen gelöscht. Maßgeblich für den Beginn der Speicherdauer war das Entstehungsdatum des Datensatzes. Infolge der großen Datenmengen, die täglich aufkamen, führte die Freigabe auf Dauer zu einer mehrfachen Überschreibung der alten Datensätze.

1.2 Fragen zur Verfügbarkeit der Daten

Wurden die Daten redundant gespeichert? Wenn ja, wo und mit welchen Techniken?
Im Mobilfunk wurde eine doppelte Datenhaltung durchgeführt. Im Festnetz gab es bezogen auf die VDSDaten ein Testrecovery von Teildaten analog zum SOX-Verfahren.

1.3 Fragen zur Integrität der Daten

a) Wurden Signaturverfahren eingesetzt, die die Integrität der Daten gewährleistet?
Wie auch im Billingprozess wurde die Integrität der auf Vorrat gespeicherten Verkehrsdaten durch ausschließliches Halten in eigenen Netzen und Systemen und konsequent restriktives Zugriffsmanagement als gewährleistet gesehen.

b) Welche sonstigen Techniken wurden zur Integritätssicherung eingesetzt?
Eine höhere Integritätssicherung der auf Vorrat zu speichernden Verkehrsdaten als die der Verkehrsdaten, die der Konzern aus ureigenem Geschäftsinteresse speichert und nutzt, war weder rechtlich vorgeschrieben, noch wurde sie vom Konzern für erforderlich gehalten.

2. Fragen zur Übermittlung der Daten

a) Wie wurden die Daten an die Strafverfolgungsbehörden übermittelt? Welche Verschlüsselungstechniken und Techniken zur Integritätssicherung wurden dabei eingesetzt?
Grundsätzlich erfolgt die Datenübertragung als Papierausdruck oder Datei auf Datenträger per Post, zunehmend aber auch als Datei per Email, PGP verschlüsselt. In eiligen Ausnahmefällen erfolgt die Übermittlung der Daten auch per Fax mit zwingender Aufforderung, den (ordnungsgemäßen) Empfang des Faxes umgehend zu bestätigen.

b) Wie wurde die Zweckbindung und Rechtmäßigkeit der Abfrage der Daten gewährleistet?
Grundsätzlich werden Anordnungen der berechtigten Stellen im Bereich der TKÜberwachung und der Beauskunftung von Bestands- und Verkehrsdaten einer qualifizierten Prüfung unterzogen, um z.B. missbräuchliche oder erkennbar rechtswidrige Maßnahmen auszuschließen. Lässt eine solche Anordnung Zweifel an ihrer Rechtmäßigkeit erkennen, findet in der Regel eine Rückfrage bzw. ein Hinweis an die erlassende Stelle statt. In Fällen offenkundiger Rechtswidrigkeit (z.B. Überwachungsanordnung gemäß §§ 100a, 100b StPO wird „nur" durch Polizeibeamten erlassen) wird die Umsetzung der Maßnahme verweigert.

c) Wie wird die Korrektheit der Anforderung von Daten geprüft (Ticketing-System)?

Die anfragenden Behörden sind in aller Regel bekannt und durch die konkrete Adressierung der Datenlieferung bestimmt. Bei unbekannten Anfragern erfolgt eine Identitätsabklärung. Die Anforderungen selbst werden im möglichen Umfang auf rechtliche Zulässigkeit und technische Umsetzbarkeit geprüft.

d) Ist eine nicht-automatisierte Mitwirkung von Telekom bei Anfragen erforderlich bzw. werden Anforderungen vollautomatisiert beantwortet?
Es findet keine automatisierte Beantwortung von Verkehrsdatenabfragen statt. Ein (freilich anders gelagerter) Sonderfall ist die TK-Überwachung, in deren Rahmen neben den Inhaltsdaten zeitgleich auch Verkehrsdaten an die berechtigte Stelle übermittelt werden. Ferner können nach bestehender Rechtslage berechtigte Stellen verlangen, dass im Mobilfunk Verkehrsdaten zur Erhebung von Standortdaten des Betroffenen in Echtzeit an sie übermittelt werden, vgl. § 100g Abs. 1 Satz 3 StPO. Mangels technischer Vorgaben wird dies derzeit noch von keinem Unternehmen praktiziert.

e) Wurden einzelne Datensätze abgefragt oder erfolgten die Abfragen bezogen auf eine größere Anzahl von Datensätzen (Streubreite)?
Die Anfragen betreffen meist eine (oder mehrere) konkrete Kennung(en) und einen bestimmten Zeitraum, innerhalb dessen die Verkehrsdaten eines Betroffenen zu beauskunften sind. Im Mobilfunk erfolgen aber zunehmend auch Anordnungen, die die zu beauskunftenden Telekommunikationsvorgänge lediglich durch räumlich und zeitliche Bezeichnung bestimmen (§ 100 g Abs. 2 StPO).

3. Einschätzung der Telekom

Welche Schwierigkeiten / Bedenken bestanden bei der Umsetzung der rechtlichen Vorgaben?
Die anlasslose verdachtsunabhängige Speicherung von Verkehrsdaten aller Teilnehmer ist im Hinblick auf den grundrechtlichen Schutz des Fernmeldegeheimnisses ein bedenkliches Instrument.

- Vorzugswürdig ist eine Sicherung von Daten bei konkretem Tatverdacht im Einzelfall (quick-freeze).
- Generell greifen Verpflichtungen zur Vorhaltung von Verkehrsdaten zu Zwecken der Strafverfolgung und Gefahrenabwehr in besonderer Weise auch in die Grundrechte der verpflichteten TKUnternehmen ein und belasten diese mit geniun staatlichen Aufgaben der Sicherheitsvorsorge. Vor diesem Hintergrund ist die Verhältnismäßigkeit der Maßnahme kritisch zu prüfen.
- Die technische Umsetzung der VDS hat hohe Investitions- und Betriebskosten verursacht, ohne dass dafür eine Entschädigung geleistet wurde. Dies halten wir ebenfalls für verfassungsrechtlich bedenklich. Bestätigt sehen wir diese Auffassung durch das VG Berlin (Beschluss vom 16.1.2009 - VG 27 A 321.08) sowie durch die Entscheidung des BVerfG vom 02.03.2010, in der ein Eingriff in Artikel 12 Abs. 1 GG grundsätzlich bejaht und eine Grundrechtswidrigkeit lediglich im Hinblick auf die vorliegende Datengrundlage verneint wurde (vgl. Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Auflage 2011, § 113a TKG, Rn. 38).

Fragenkatalog R-Kom

Vorfragen

a) Hat die R-Kom die Speicherung der Daten selbst übernommen oder an einen Dritten outgesourced?

b) Wie viel musste R-Kom zur Umsetzung der gesetzlichen Vorgaben des § 113a TKG investieren?

1. Fragen zur Speicherung und Aufbewahrung der Daten

1.1 Fragen zur Vertraulichkeit der Daten

a) Wie lässt sich die Infrastruktur skizzieren, innerhalb derer die Daten gespeichert wurden (logisch und physisch, alle Arten von Verkehrsdaten)?
Die Daten werden auf einem Cluster aus NetApp Appliances gespeichert (http://www.netapp.com/de/). Der Zugriff auf die Daten erfolgt über ein IP-Netz.

b) Wurden die Daten physisch / logisch getrennt von anderen Daten (z.B. nach § 96 TKG gespeicherten Verkehrsdaten) gespeichert?
Es fand hier eine logische Trennung statt.

c) Sind die Systeme, auf denen die Daten gespeichert wurden, vom Internet entkoppelt?
Ja, es war kein Zugriff aus dem Internet möglich.

d) Wurden die Daten verschlüsselt gespeichert? Wenn ja, mit welchen Verschlüsselungsverfahren (symmetrisch oder asymmetrisch) und wie wurden die Schlüssel verwahrt (getrennt, nicht getrennt)?
Nein, es fand keine Verschlüsselung der Daten statt.

e) Wie erfolgte der Zugriff auf die Daten (Authentifizierungsverfahren)?
Der Zugriff auf die Daten erfolgte über einen dedizierten Rechner, der über das Storage-VLAN Zugriff auf die Daten hatte. Der Zugang auf den Rechner erfolgte via ssh und public-key Authentifizierungsverfahren.

f) Wer im Unternehmen durfte / konnte auf die Daten zugreifen?
Der Zugriff war nur für eingewiesene Mitarbeiter möglich. Die Mitarbeiter hatten sich zuvor schriftlich zur Einhaltung des von der BNetzA vorgegebenen Geheimhaltungsgrades VS (Verschlußsache)-Nur für den Dienstgebraucht verpflichtet.

g) Wie ist der Zugriff durch Ermittlungsbehörden technisch realisiert?
VS, keine Angaben

h) Wie wurde der Zugriff auf die Daten protokolliert? Ist das Protokoll revisionssicher?
Der Zugriff wurde über log-Files ptotokolliert, die im Versionierungstool cvs revisionssicher abgelegt wurden.

i) Wie wurden die Daten gelöscht? Erfolgte die Löschung automatisiert (Zeitstempel an den Daten)?
Es fand eine automatisierte Löschung Anhand eines Zeitstempels im Dateinamen statt.

1.2 Fragen zur Verfügbarkeit der Daten

Wurden die Daten redundant gespeichert? Wenn ja, wo und mit welchen Techniken?
Als Storagesystem kam ein Cluster aus FAS 2020 Appliances von NetApp mit den dort verfügbaren Techniken für eine sichere und redundante Speicherung zum Einsatz.

1.3 Fragen zur Integrität der Daten

a) Wurden Signaturverfahren eingesetzt, die die Integrität der Daten gewährleistet?
Es wurden hier die Richtlinien nach §45g des TKG (Verbindungspreisberechnung) eingehalten.

b) Welche sonstigen Techniken wurden zur Integritätssicherung eingesetzt?
Es wurden hier die Richtlinien nach §45g des TKG (Verbindungspreisberechnung) eingehalten.

2. Fragen zur Übermittlung der Daten

a) Wie wurden die Daten an die Strafverfolgungsbehörden übermittelt? Welche Verschlüsselungstechniken und Techniken zur Integritätssicherung wurden dabei eingesetzt?
VS, kein Angaben

b) Wie wurde die Zweckbindung und Rechtmäßigkeit der Abfrage der Daten gewährleistet?
Es wurden ausschließlich schriftliche Anfragen nach einer individuellen Prüfung beantwortet.

c) Wie wird die Korrektheit der Anforderung von Daten geprüft (Ticketing-System)?
VS, keine Angaben

d) Ist eine nicht-automatisierte Mitwirkung von R-Kom bei Anfragen erforderlich bzw. werden Anforderungen vollautomatisiert beantwortet?
Manuelle Anfragen wurden ausschließlich unter Einbeziehung der Datenschutzbeauftragten beantwortet.

e) Wurden einzelne Datensätze abgefragt oder erfolgten die Abfragen bezogen auf eine größere Anzahl von Datensätzen (Streubreite)?
VS, keine Angaben

3. Einschätzung der R-Kom

Welche Schwierigkeiten / Bedenken bestanden bei der Umsetzung der rechtlichen Vorgaben?

Fragenkatalog JonDos

Vorfragen

a) Hat JonDos die Speicherung der Daten selbst übernommen oder an einen Dritten outgesourced?
Wir haben selbst keine Speicherung vorgenommen, da wir selbst damals keine Anonymisierungsserver betrieben haben. Die Bundesnetzagentur hat uns und den meisten unserer Partner gegenüber keinerlei Verpflichtung zur Speicherung ausgesprochen, auch nach persönlichen Gesprächen mit unseren Anwälten. Da es außerdem noch einige Widersprüche im Gesetz gab, die sich technisch nicht auflösen ließen, haben wir unseren Partnern empfohlen, keinerlei Speicherung vorzunehmen.

Eine prototypische Speicherung wurde jedoch mit unserer Unterstützung von der TU Dresden implementiert und auch von dieser, und vom Unabhängigen Landeszentrum für Datenschutz, auf deren Mixen eingesetzt. So gut wie alle Mix-Anbeiter waren also "speicherfrei".

b) Wie viel musste JonDos zur Umsetzung der gesetzlichen Vorgaben des § 113a TKG investieren?
Wir schätzen die Kosten inklusive der Rechtsberatung auf ca. 10.000 Euro. Das war für uns damals mehr als die Hälfte eines monatlichen Umsatzes. Gewinne hatten wir noch keine erwirtschaftet. Die Kosten waren durchaus existenzgefährdend.

1. Fragen zur Speicherung und Aufbewahrung der Daten

1.1 Fragen zur Vertraulichkeit der Daten

a) Wie lässt sich die Infrastruktur skizzieren, innerhalb derer die Daten gespeichert wurden (logisch und physisch, alle Arten von Verkehrsdaten)?
Die Daten wurden jeweils auf dem ersten und dem letzten Mix einer Kaskade erhoben und gespeichert (auf mittleren nicht, da auf den betroffenen Kaskaden kein mittlerer Mix vorhanden war). Nur wenn beide Datenbestände zusammengeführt wurde, war eine Aufdeckung möglich. Folgende Daten wurden erhoben:

1. Mix: IP-Adresse des Nutzers, Zeitpunkt eines Requests, Kanal-ID eines Requests
Letzter Mix: Zeitpunkt eines Requests, Kanal-ID eines Requests, Ausgangs-Port eines Requests

b) Wurden die Daten physisch / logisch getrennt von anderen Daten (z.B. nach § 96 TKG gespeicherten Verkehrsdaten) gespeichert?
Die Daten wurden nur von einigen kostenfreien Servern gespeichert, auf denen sonst keine anderen Daten vorliegen. Es gibt also nichts, vowon man die Daten "trennen" könnte.

c) Sind die Systeme, auf denen die Daten gespeichert wurden, vom Internet entkoppelt?
Nein.

d) Wurden die Daten verschlüsselt gespeichert? Wenn ja, mit welchen Verschlüsselungsverfahren (symmetrisch oder asymmetrisch) und wie wurden die Schlüssel verwahrt (getrennt, nicht getrennt)?
Asymmetrisch, privater Schlüssel getrennt verwahrt auf Chipkarte.

e) Wie erfolgte der Zugriff auf die Daten (Authentifizierungsverfahren)?
Mittels Chipkarte.

f) Wer im Unternehmen durfte / konnte auf die Daten zugreifen?

g) Wie ist der Zugriff durch Ermittlungsbehörden technisch realisiert?

h) Wie wurde der Zugriff auf die Daten protokolliert? Ist das Protokoll revisionssicher?
Es war kein Protokoll im Prototyp vorgesehen soweit ich weiß. Meines Wissens nach wurden allerdings auch keine Daten ausgelesen. Das können
Stefan Köpsell, TU Dresden
Henry Krasemann, ULD

allerdings besser beantworten als ich, da dies die Vertreter der Organisationen sind, die Daten gespeichert haben.

i) Wie wurden die Daten gelöscht? Erfolgte die Löschung automatisiert (Zeitstempel an den Daten)?
Eine automatisierte Löschung war im Prototyp nicht vorgesehen.

j) Wurden auf allen Mix-Servern einheitliche Verfahren/Techniken verwendet?
Ja, der Code wurde soweit ich weiß unverändert auf allen Server eingesetzt, auf denen gespeichert wurde.

1.2 Fragen zur Verfügbarkeit der Daten

Wurden die Daten redundant gespeichert? Wenn ja, wo und mit welchen Techniken?
Das weiß ich leider nicht.

1.3 Fragen zur Integrität der Daten

a) Wurden Signaturverfahren eingesetzt, die die Integrität der Daten gewährleistet?
Soweit ich weiß war das im Prototyp nicht vorgesehen. Das sollte Stefan Köpsell wissen.

b) Wurden auf allen Mix-Servern einheitliche Verfahren/Techniken verwendet?
Ja, auf allen, die gespeichert haben.

c) Welche sonstigen Techniken wurden zur Integritätssicherung eingesetzt?
Weiß ich leider nicht.

2. Fragen zur Übermittlung der Daten

a) Wie wurden die Daten an die Strafverfolgungsbehörden übermittelt? Wie wurden die Daten von den einzelnen Mix-Servern zusammengetragen? Welche Verschlüsselungstechniken und Techniken zur Integritätssicherung wurden dabei eingesetzt?
Soweit ich weiß wurden keine Daten übermittelt. Dafür gab es auch keinen definierten Prozess. Wenn eine Anfrage gestellt worden wäre, wären die Daten wohl von den einzelnen Betreibern mit GPG signiert und verschlüsselt und an die Behörden geschickt worden. Das ist der übliche Weg, um Daten an die Behörden zu übermitteln. Die Behörden hätten die Daten dann "zusammensetzen" müssen.

b) Wie wurde die Zweckbindung und Rechtmäßigkeit der Abfrage der Daten gewährleistet?
Zunächst müssen solche Daten leider immer herausgegeben werden. Die Verantwortung liegt beim Staatsanwalt, der den entsprechenden Beschluss ausstellt. Eine Zweckbindung und Rechtmäßigkeit kann man dann im Nachhinein vor Gericht feststellen lassen.

c) Wie wird die Korrektheit der Anforderung von Daten geprüft (Ticketing-System)?
Durch Anruf bei der entsprechenden Behörde und dem jeweiligen Staatsanwalt.

d) Ist eine nicht-automatisierte Mitwirkung von JonDos bei Anfragen erforderlich bzw. werden Anforderungen vollautomatisiert beantwortet?

e) Wurden einzelne Datensätze abgefragt oder erfolgten die Abfragen bezogen auf eine größere Anzahl von Datensätzen (Streubreite)?

3. Einschätzung der JonDos GmbH

Welche Schwierigkeiten / Bedenken bestanden bei der Umsetzung der rechtlichen Vorgaben?