Arbeitskreis Medien Stand: 24.10.02

Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten

Übersicht

1. Allgemeines

Bei der Nutzung von Internetdiensten fallen bei Diensteanbietern eine Fülle personenbezogener Daten an. Die Rechtsgrundlagen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten ergeben sich für Tele- und Mediendienste aus dem Teledienstedatenschutzgesetz (TDDSG) beziehungsweise aus dem Mediendienste-Staatsvertrag (MDStV). Darüber hinaus handelt es sich bei der Vermittlung des Zugangs zum Internet (access providing) sowie bei E-Mail-Diensten zumindest teilweise auch um die Erbringung eines Telekommunikatonsdienstes i. S. d. TKG.. Soweit sich die folgenden Ausführungen auf die Verarbeitung personenbezogener Daten bei E-Mail-Diensten oder der Zugangsvermittlung beziehen, müssen daher auch das Telekommunikationsgesetz (TKG) und die Telekommunikations-Datenschutzverordnung (TDSV) zu Grunde gelegt werden. Bei der Beurteilung der Zulässigkeit der Datenerhebung, Verarbeitung und Nutzung ist auch der Grundsatz der **Datenvermeidung** und **Datensparsamkeit** nach § 3 a BDSG zu beachten.

Bei den einzelnen Diensten können unterschiedliche Arten personenbezogener Daten (Bestands-, Verbindungs-, Nutzungs-, Abrechnungs- und Inhaltsdaten) anfallen, deren Verwendung sich nach unterschiedlichen Regelungen richtet:

- **Teledienste** (hierunter fällt die Zugangsvermittlung nur zum Teil; s. 3.1)
  - § 5 TDDSG: Bestandsdaten
  - § 6 TDDSG: Nutzungs- und Abrechnungsdaten

- **Mediendienste**
  - § 19 Abs. 1 MDStV: Bestandsdaten
  - § 19 Abs. 2 bis 9 MDStV: Nutzungs- und Abrechnungsdaten

- **E-Mail Dienste** sowie z. T. die Zugangsvermittlung (s. 3.1)
  - § 89 Abs. 2 TKG i.V.m. § 5 TDSV unter Beachtung des § 89 Abs. 6 u. 10 Satz 1 TKG: Bestandsdaten
  - § 89 Abs. 2 TKG i.V.m. § 6 Abs. 1 TDSV: Verbindungsdaten

Soweit eine staatliche Stelle die Herausgabe von personenbezogener Daten bzw. die Überwachung eines E-Mail-Anschlusses verlangt, muss sie gegenüber dem Diensteanbieter die Rechtsgrundlage ihrer Forderung darlegen und ggf. notwendige richterliche Anordnungen beibringen. Der Diensteanbieter hat sich von der Einhaltung der formalen Anforderungen an eine entsprechende Maßnahme zu vergewissern, einer Verpflichtung zur inhaltlichen Prüfung der entsprechenden Anordnungen unterliegt er jedoch grundsätzlich nicht. Gegenüber Strafverfolgungsbehörden ist er verpflichtet, entsprechende Anordnungen zur Überwachung umzusetzen; dagegen ist er gegenüber Nachrichtendiensten unter den gesetzlichen Voraussetzungen zur Auskunft berechtigt, aber nicht verpflichtet.

2. Datentypen

2.1 Bestandsdaten

Bestandsdaten sind Daten für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses über die Nutzung von Tele-, Medien- und Telekommunikationsdiensten. Dies können sein: Name, Anschrift, E-Mail-Adresse, Telefon- oder Telefaxnummer, Geburtsdatum, Bankverbindung, Kreditkartennummer, öffentlicher Schlüssel, User-ID, aber auch statische IP-Adressen und ähnliche Angaben. Welche Bestandsdaten im Einzelnen erhoben, verarbeitet oder genutzt werden dürfen, ist im wesentlichen abhängig von der technischen Ausgestaltung des Dienstes und von dem Inhalt der jeweiligen Verträge. Die Definition dieser Daten ist für die Bereiche der Teledienste, Mediendienste und Telekommunikationsdienste identisch.

In welchem Umfang Bestandsdaten erhoben werden, ist am **Grundsatz der Erforderlichkeit** auszurichten, d.h., Daten, die für die genannten Zwecke nicht zwingend erforderlich sind, dürfen nicht erhoben, verarbeitet oder genutzt werden.

So dürfen z.B. bei der kostenlosen Bereitstellung von Informationen für die Allgemeinheit grundsätzlich **keine Bestandsdaten** erhoben werden, weil kein Vertragsverhältnis vorliegt und die Daten für die Abwicklung solcher Angebote nicht erforderlich sind

Dennoch werden bei kostenlosen Diensten wie der Anforderung bzw. Bestellung von Newslettern von den Anbietern häufig neben der E-Mail-Adresse auch noch andere personenbezogene Daten erhoben. Dies ist in der Regel nicht zulässig, da diese Daten für die Erbringung der Leistung (Übersendung einer E-Mail) nicht notwendig sind. Ihre Nutzung würde ggf. zudem gegen das Koppelungsverbot (§ 3 Abs. 4 TDDSG, § 17 Abs. 4 MDStV, §89 Abs. 10 TKG) verstoßen.

Bestandsdaten werden bei Zugangs-Providern und bei solchen Telediensteanbietern erhoben, die eine Vertragsbeziehung zwischen dem Anbieter und den Nutzenden voraussetzen, also im wesentlichen bei kostenpflichtigen Diensten.
In diesem Zusammenhang muss auf die Abgrenzung zwischen Bestandsdaten, die unter das TDDSG bzw. die TDSV fallen, und Daten, die auf Grundlage des BDSG oder einer bereichsspezifischen Rechtsvorschrift erhoben werden, hingewiesen werden. Solche Daten, die z. B. bei der Bestellung einer kommunalen Dienstleistung (Müllabfuhr) oder eines materiellen Guts in einem Online-Shop angegeben werden, sind keine Bestandsdaten i.S.d. TDDSG, sondern sog. Inhaltsdaten, die zur Offline-Abwicklung (Lieferung der Ware, Zusendung der Rechnung) des Vertrags erforderlich und daher nach BDSG zu beurteilen sind.

Löschungsfristen

Die Pflicht zur frühestmöglichen Löschung von Bestandsdaten ergibt sich für Tele- und Mediendiensteanbieter aus dem Erforderlichkeitsgrundsatz. Soweit Bestandsdaten nicht mehr zur Begründung, Ausgestaltung und Änderung des Vertragesverhältnisses erforderlich sind, etwa weil das Vertragsverhältnis beendet ist und nachvertragliche Ansprüche nicht mehr bestehen, müssen sie gelöscht werden. Die Löschungspflicht ergibt sich darüber hinaus aus § 35 Abs. 2 Nr. 3 BDSG.

Bestandsdaten, die im Zusammenhang mit der Erbringung von Telekommunikationsdiensten (E-Mail-Dienste bzw. Zugangsvermittlung) erhoben wurden, sind spätestens gem. § 5 Abs. 3 Satz 1 TDSV mit Ablauf des auf die Beendigung des Vertrages folgenden Kalenderjahres zu löschen. Ausnahmen hiervon ergeben sich aus § 35 Abs. 3 BDSG hinsichtlich einer fortdauernden Speicherung von personenbezogenen Daten im Rahmen gesetzlicher Aufbewahrungsbestimmungen. In diesem Fall sind die Daten vom operativen Datenbestand zu trennen und für eine Verwendung außerhalb der Dokumentationsverpflichtung zu sperren.

2.2 Nutzungsdaten

Nutzungsdaten fallen im Regelfall bei jedem Tele- und Mediendiensteanbieter an. Nutzungsdaten sind gem. § 6 Abs. 1 TDDSG bzw. § 19 Abs. 2 MDStV Daten, die erforderlich sind, um die Inanspruchnahme von Telediensten zu ermöglichen und diese abzurechnen. Es handelt sich hierbei insbesondere um Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angaben über die von den Nutzenden in Anspruch genommenen Teledienste.

Die Regelungen sind abschließend, d.h. die Erhebung, Verarbeitung oder Nutzung der Nutzungs- und Abrechnungsdaten durch die Diensteanbieter ist nur zulässig, soweit sie durch die Vorschriften erlaubt wird. Nutzungsdaten dürfen außerhalb dieser Bestimmungen nur verarbeitet werden, wenn eine gesetzliche Spezialregelung dies ausdrücklich erlaubt oder der Betroffene eingewilligt hat.

Die Aussagekraft der Nutzungsdaten bei Tele- und Mediendiensten ist bisweilen größer als etwa bei Verbindungsdaten der Sprachtelekommunikation. Während Verbindungsdaten lediglich Auskunft darüber geben, wer wann mit wem kommuniziert hat, offenbaren Nutzungsdaten häufig darüber hinaus, welche Inhalte übertragen wurden. Dies gilt insbesondere in bezug auf aus dem Web abgerufene Ressourcen und auf Anfragen bei Suchmaschinen.

Löschungsfristen

Nach § 6 Abs. 4 TDDSG darf der Diensteanbieter Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verarbeiten und nutzen, soweit sie für Zwecke der Abrechnung erforderlich sind. Im Umkehrschluss bedeutet dies, dass alle übrigen Nutzungsdaten frühestmöglich, spätestens unmittelbar nach Ende der Nutzung zu löschen sind. Eine entsprechende Regelung liefert § 19 Abs. 5 MDStV.

- *Nutzungsdaten, die nicht zu Abrechnungszwecken erforderlich sind*
  Zur Abrechnung von Telediensten werden die entsprechenden Daten über die beim Provider "eingehende" Telefonnummer oder eine im Vorfeld zugeteilte User-ID den Nutzenden zugeordnet. Die IP-Adressen werden hierfür aber nicht benötigt, zudem wären sie als Ordnungskriterium nicht geeignet, da sie in den meisten Fällen dynamisch vergeben werden und im Laufe einer Internet-Sitzung mehrfach wechseln können. Somit ist die **Speicherung von IP-Adressen über die Nutzungsdauer hinaus unzulässig** (zum Personenbezug von IP-Adressen s. u. 3.1). Gleiches gilt auch für die Angaben über die von den Nutzenden in Anspruch genommenen Teledienste (URLs).

- *Abrechnungsdaten (Nutzungsdaten, die zur Abrechnung erforderlich sind)*
  Abrechnungsdaten sind diejenigen Nutzungsdaten, die für die Abrechnung von Tele- und Mediendiensten verwendet werden. Üblicher Weise werden für Abrechnungszwecke Nutzungsdaten mit Bestandsdaten kombiniert und zur Rechnungsstellung verwendet. Der Gestaltung der Abrechnungsmodalitäten kommen im Hinblick auf die Erforderlichkeit der Verarbeitung personenbezogener Daten und der daraus resultierenden datenschutzrechtlichen Probleme besondere Bedeutung zu. Abrechnungsverfahren sollten nach Möglichkeit so gestaltet werden, dass für Abrechnungszwecke so wenig wie möglich personenbezogene Daten erhoben, gespeichert und genutzt werden. Die Speicherung von Nutzungsdaten auf IP-Ebene ist im Regelfall für Abrechnungszwecke nicht erforderlich. Gleiches gilt für andere technische Angaben, die die Hardware-Ausstattung des Nutzers oder die von ihm eingesetzte Software betreffen. Ebenfalls nicht erforderlich und damit im Regelfall unzulässig ist die Speicherung einzelner Inhalte oder deren Adressen, die der Nutzer abgerufen oder angesteuert hat.

  Abrechnungsdaten sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind. Eine Abrechnung mit detailgenauen Angaben (etwa Bezeichnung einer aus dem WWW abgerufenen Ressource, Bezeichnungen von Newsgroups, die in Anspruch genommen wurden) ist nur

zulässig, wenn der Nutzer einen derartigen Einzelnachweisausdrücklich verlangt (§ 6 Abs. 6 letzter Halbs. TDDSG). Im Falle des Einzelnachweises dürfen Abrechnungsdaten höchstens bis zum Ablauf von sechs Monaten (§ 6 Abs. 7 TDDSG, § 19 Abs. 8 MDStV) nach Versendung der Rechnung gespeichert werden. Lediglich in den Fällen, in denen die Nutzer oder die Nutzerinnen gegen die Entgeltforderung fristgerecht Einwendungen erhoben oder diese trotz Zahlungsaufforderung nicht beglichen haben, dürfen die Abrechnungsdaten aufbewahrt werden, bis die Einwendungen abschließend geklärt sind oder die Entgeltforderung beglichen wurde.

2.3 Verbindungsdaten bei E-Mail Diensten

Bei dem Angebot zur Übermittlung von **E-Mails** handelt es sich um einen Telekommunikationsdienst. Die bei der Erbringung dieses Dienstes anfallenden Daten sind Verbindungsdaten im Sinne des Telekommunikationsrechts (§ 2 Nr. 4 TDSV). Verbindungsdaten bei E-Mail-Diensten sind insbesondere E-Mail-Adressen (die auch Bestandsdaten sein können, s.o. 2.1), Zeitpunkte der Sendung bzw. Zustellung und Routing-Informationen (Angaben über diejenigen Rechner, die eine E-Mail durchgeleitet haben). Nicht zu den Verbindungsdaten gehören z.B. Bezeichnungen von Datei-Anlagen und über den “Betreff”.

Zulässig ist die Verarbeitung zur Entgeltermittlung und Entgeltabrechnung (§ 7 TDSV), für den Einzelverbindungsnachweis (§ 8 TDSV) und zur Erkennung und Abwehr von Störungen von Telekommunikationsanlagen und des Missbrauchs von Telekommunikationsdiensten (§ 9 TDSV).

Hiervon zu unterscheiden sind die Informationen, die ein Nutzer oder eine Nutzerin beispielsweise im persönlichen Mail-Adressbuch zur dauerhaften Nutzung abspeichert. Eine Verarbeitung oder Nutzung der Verbindungsdaten darf nur erfolgen, soweit sie zum Aufbau weiterer Verbindungen oder zu Abrechnungszwecken erforderlich sind.

Löschungsfristen

Sofern die Verarbeitung oder Nutzung der Verbindungsdaten aus vorgenannten Gründen nicht erforderlich ist, sind sie vom Diensteanbieter spätestens am Tag nach Beendigung der Verbindung unverzüglich zu löschen, wenn die Nutzenden die E-Mail abgerufen haben, und keine weitere Speicherung wünschen.

Angesichts der derzeitigen Tarifmodelle für E-Mail-Dienste ist eine längerfristige Speicherung von Verbindungsdaten nicht erforderlich und damit unzulässig, da die Daten nicht zu Abrechnungszwecken benötigt werden.

2.4 Inhaltsdaten

Die Beurteilung der Rechtmäßigkeit zur Erhebung, Verarbeitung und Nutzung von Inhaltsdaten bei Tele- und Mediendiensten richtet sich nach den jeweiligen spezialgesetzlichen Regelungen (z.B. die Erhebung von Sozialdaten nach den Vorschriften des Sozialgesetzbuches, Auskünfte zum Meldewesen nach dem Meldegesetz etc.) und nach dem Bundesdatenschutzgesetz. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, sind zusätzlich zu beachten.

3. Anbieter (Provider)

Welche Daten zu welchem Zweck ein Provider erheben, verarbeiten und nutzen darf, hängt vom angebotenen Dienst und den jeweiligen Tarifmodellen ab. In jedem Fall ist zu beachten, dass beim Angebot mehrerer Dienste die rechtliche Beurteilung für jeden Dienst separat zu betrachten ist. Auch darf nicht eine Zusammenführung von z. B. Bestandsdaten aus den Bereichen des Telekommunikations- und des Teledienstes erfolgen.

3.1 Zugangs-Anbieter (Access-Provider)

Die Aufgabe des Zugangs-Providers liegt darin, den Zugang zu Informationen bzw. Diensten gegen Entgelt zu vermitteln bzw. die entsprechenden Inhalte an den Nutzer durchzuleiten. Nach § 2 Abs. 2 Nr. 3 TDG ist das Angebot zur Nutzung des Internets oder weiterer Netze ein Teledienst. Dies wurde bisher von den meisten Datenschutzaufsichtsbehörden so interpretiert, dass hierunter auch die reine Zugangsvermittlung (access providing) fällt. In der Praxis wird diese Auffassung hingegen überwiegend abgelehnt und das access providing in erster Linie als Telekommunikationsdienst angesehen (vgl. HansOLG Hamburg MMR 2000, 611, 613). Aus folgenden Gründen ist dieser Auffassung nunmehr zuzustimmen:

Der Gesetzgeber hatte bei der Regelung des § 2 Abs.2 Nr. 3 TDG in erster Linie das Angebot von Navigationshilfen und Suchmaschinen, nicht aber die reine Zugangsvermittlung im Sinn. Zudem sprechen auch technische Gründe dafür, die mit der Vermittlung des Zugangs verbundene Datenübertragung als Telekommunikationsdienst anzusehen. Nach dem OSI-Referenzmodell, das der Kommunikation im Internet zugrunde gelegt wird, wird erst auf der Ebene des Transmission Control Protocol (TCP) die virtuelle Verbindung zwischen den beteiligten Endgeräten hergestellt. TCP wird der Schicht 4 (Transportschicht) des OSI-Modells zugeordnet. Daraus folgt, dass Schicht 4 sowie alle darunter liegenden Schichten (auch die der Schicht 3 zugeordnete IP-Ebene) zum technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten zu zählen sind und damit als Telekommunikation i. S. v. § 3 Nr. 16 TKG betrachtet werden müssen. Dagegen unterliegen nach dem Hypertext Transport Protocol (http) übermittelte Informationen als Nutzungsdaten dem Tele- und Mediendiensterecht. Soweit der Zugangs-Anbieter seine Dienste mit der von § 3 Nr. 5 TKG geforderten Nachhaltigkeit anbietet, besteht grundsätzlich die Verarbeitungsbefugnis für Bestands- und Nutzungsdaten nach der TDSV. Bestandsdaten dürfen lediglich in dem Umfang gespeichert werden, wie sie für das Vertragsverhältnis erforderlich sind und zum Zwecke der Abrechnung benötigt werden. Zur Vermittlung erforderliche Verbindungsdaten (auch die IP-Adresse) dürfen nur für die Phase der Inanspruchnahme gespeichert werden. Sie sind nach der Inanspruchnahme grundsätzlich unverzüglich, spätestens aber am Tage nach Beendigung der Verbindung nach § 6 Abs. 2 Satz 2 TDSV zu löschen, es sei denn, einzelne Verbindungsdaten werden zu den in §§ 7 bis 10 TDSV genannten Zwecken (insbesondere Abrechnungszwecken) benötigt. Im einzelnen ist dies abhängig von dem Tarifmodell, nach dem die Abrechnung erfolgt. Im Falle einer Flatrate dürfen keine Verbindungsdaten gespeichert werden, da für die Nutzung ein Pauschalpreis zu bezahlen ist. Erfolgt die Abrechnung dagegen nach Zeit- oder Mengentarifen, so sind entweder die Zeittakte oder aber die Mengendaten zu speichern. Um die Zuordnung der für die Abrechnung gespeicherten Verbindungsdaten zu den jeweiligen Nutzenden herzustellen, muss darüber hinaus ein eindeutiges Zuordnungsmerkmal (Bestandsdatum), also entweder die Telefonnummer oder die User-ID, mitgespeichert werden. Eine Speicherung beider Zuordnungsmerkmale ist unter dem Gebot der Datensparsamkeit nicht zulässig.

Die Frage, ob IP-Nummern personenbezogen sind, wird kontrovers diskutiert. Sie ist deshalb von großer Bedeutung, weil an verschiedenen Stellen des Internet (insb. bei Access Providern, Content Providern, Hosting Services) IP-Adressen – teilweise zusammen mit anderen Nutzungsdaten - protokolliert werden.

Zugangs-Provider (Access Provider) können – unabhängig von der bei der Vergabe der IP-Adressen verwendeten Technik, also auch bei dynamischer Vergabe, die IP-Nummer einzelnen Nutzenden zuordnen. Sie sind somit personenbezogene Daten. Dies gilt auch, wenn der Zugang (Access) beispielsweise über das LAN eines Unternehmens bzw. einer Behörde erfolgt oder über Firewallsysteme eine Adressumsetzung erfolgt.

Betrachtet man die Möglichkeiten anderer Anbieter (beispielsweise Inhalts-Anbieter) eine Identifikation anhand der IP-Adresse vorzunehmen, so sind hier die Möglichkeiten der Zusammenführung der personenbezogenen Daten im Internet zu berücksichtigen. Mit Hilfe Dritter ist es bereits jetzt ohne großen Aufwand in den meisten Fällen möglich, Internet-Nutzer und -Nutzerinnen auf Grund ihrer IP-Adresse zu identifizieren. Wenn z. B. für Inhalte-Anbieter der Personenbezug von IP-Adressen verneint und das TDDSG bzw. die TDSV nicht für anwendbar erklärt werden, hätte dies nicht nur die mit dem Grundrechtsschutz unvereinbare Konsequenz, dass der Diensteanbieter die Daten unbegrenzt selbst verarbeiten oder nutzen könnte, sondern er dürfte diese Daten auch ohne Restriktionen an Dritte übermitteln, die ihrerseits die Möglichkeit hätten, den Nutzer aufgrund der IP-Adresse zu identifizieren. Es bedarf keiner näheren Begründung, dass dies dem Schutzgedanken des Datenschutzrechts diametral zuwiderlaufen würde. Dynamische IP-Adressen sind daher personenbezogene Daten, da sie durch Zusammenführung mit den dahinter stehenden Zuordnungstabellen den Rückschluss auf bestimmbare Personen zulassen (vgl. §§ 3 Abs.1 BDSG, 1 Abs.2 TDDSG).

Auf jeden Fall sind statische IP-Adressen personenbezogene Daten, da diese einen direkten und andauernden Bezug zu den Nutzenden enthalten und auf diesen ohne Weiteres rückschließen lassen. Beim Zugangsanbieter (und nur bei diesem) gehören sie allerdings zu den Bestandsdaten (s. o. 2.1)

Als Folge dessen sind für das Erheben, Verarbeiten, Nutzen und auch Löschen von IP-Adressen die Vorschriften für Verbindungs- bzw. Nutzungsdaten anzuwenden.

3.2 Proxybetrieb

Inhalte, die von Nutzern aus dem Internet abgerufen wurden, werden von Betreibern von Proxy-Diensten auf Proxy-Servern zwischengespeichert und können bei wiederholtem Zugriff derselben oder anderer Nutzer ohne erneute Inanspruchnahme anderer Internet Provider dem Nutzer zugestellt werden. Deshalb kann von ihnen das Surfverhalten der Nutzer einschließlich der dabei übertragenen Inhalte nachvollzogen werden.

Hinsichtlich der Einordnung dieser Dienste gilt das oben unter 3.1 zu den Zugangsanbietern Gesagte entsprechend. Bis einschließlich zur TCP-Ebene ist das Betreiben eines Proxy-Dienstes als Übermittlung von Nachrichten Telekommunikation i. S. v. § 3 Nr. 16 TKG.

Bei Betreibern von Proxydiensten gem. § 10 TDG dürften, sofern dieser Dienst nicht in Verbindung mit anderen Diensten angeboten wird, keine Bestandsdaten anfallen.

Verbindungs- bzw. Nutzungsdaten dürfen nur gespeichert werden, sofern sie zur Erbringung der Leistung erforderlich sind. Dies können allenfalls die URL (Nutzungsdatum) bzw. die IP-Adresse (Verbindungsdatum) von angefragten Angeboten sein. Eine darüber hinaus gehende Speicherung dieser Daten, insbesondere die IP-Adresse der Nutzer oder Nutzerinnen, ist unzulässig, da sie zur Erbringung des Proxy-Dienstes nicht erforderlich sind. Eine Speicherung von Inhaltsdaten kann unter Bezug auf § 10 Ziffer 3 TDG für maximal 24 Stunden toleriert werden. Eine darüber hinaus gehende Speicherung ist nicht erforderlich und dementsprechend unzulässig.

3.3 Inhalts-Anbieter (Content-Provider)

Bei Inhalts-Providern können sowohl Bestandsdaten als auch Nutzungsdaten anfallen. Bestandsdaten dürfen gespeichert werden, soweit es sich um Identifikationsangaben handelt. Des weiteren wird auf die Ausführungen zu den Bestandsdaten unter 3.1 verwiesen.

Welche Nutzungsdaten im einzelnen gespeichert werden dürfen, ist von dem jeweiligen Dienst abhängig. Auch hier gilt das Erforderlichkeitsprinzip, d.h., im Falle eines kostenlosen Angebots dürfen keine Nutzungsdaten gespeichert werden, ansonsten nur die Daten , die zur Abrechnung erforderlich sind. Wird beispielsweise für das Herunterladen von Dokumenten abgerechnet, so darf nur der Preis des Dokumentes gespeichert werden, nicht aber seine Bezeichnung.

3.4 Webhosting

Beim sogenannten Webhosting überträgt der Anbieter eines Dienstes die technische Abwicklung seines Angebotes einem Dritten (host). Dieser Dienstleister kann auf unterschiedliche Weise in die Abläufe einbezogen sein. Bei der Verarbeitung personenbezogener Daten im Rahmen des Angebots (etwa bei elektronischen Bestellungen) handelt es sich im Regelfall um Datenverarbeitung im Auftrag des Diensteanbieters, der als Auftraggeber die Verantwortung für die personenbezogenen Daten des Nutzers trägt (§ 11 BDSG). Er ist Adressat aller Datenschutzrechte, die Betroffene (z.B. auf Auskunft) geltend machen können. Soweit der Betreiber des Hosting-Service in eigener Verantwortung personenbezogene Daten erhebt, verarbeitet oder nutzt (z.B. in Logdateien), treffen ihn selbst auch datenschutzrechtliche Pflichten (z.B. zur Information des Nutzers, § 4 Abs.3 BDSG).

4 Übermittlung von Daten an Strafverfolgungsbehörden und Nachrichtendienste

Das Fernmeldegeheimnis gem. Art. 10 GG, § 85 TKG schützt die Inhalte und auch die "näheren Umstände der Telekommunikation" (Verbindungsdaten). Das Grundrecht beschränkt ferner die Verwen-

dung und Weitergabe von Daten, die unter Aufhebung des Fernmeldegeheimnisses erlangt worden sind. Ferner schützt Art. 10 GG, § 85 TKG die gesamte Telekommunikation einschließlich der auf ihr basierenden Dienste. Soweit weitere personenbezogene Daten, wie etwa Bestandsdaten, betroffen sind, ist der Schutz aus dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) einschlägig. Wegen der Grundrechtsrelevanz von Ermittlungshandlungen im Rahmen der Strafverfolgung bedarf es für die Erhebung von personenbezogenen Daten in jedem Falle spezieller gesetzlicher Befugnisse.

Generell gilt, dass Anbieter weder berechtigt noch verpflichtet sind, vorauseilend für Zwecke der Strafverfolgung oder der Nachrichtendienste personenbezogene Daten zu speichern, die sie nach den oben beschriebenen Bestimmungen von TKG, TDSV, TDDSG und MDStV nicht verarbeiten dürften.

4.1 Zugangs-Anbieter (Access Provider)

Da es sich bei den Zugangs-Anbietern wie unter 3.1 ausgeführt um Anbieter von Telekommunikationsdiensten handelt, richtet sich die Herausgabe von **Bestandsdaten** nach § 89 Abs. 6 TKG. Die für den Dienst erhobenen Bestandsdaten dürfen nach Maßgabe dieser Vorschrift im Einzelfall auf Ersuchen an die zuständigen Stellen übermittelt werden, soweit dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgabe der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des militärischen Abschirmdienstes sowie des Zollkriminalamtes erforderlich ist. Eine richterliche Anordnung ist nicht erforderlich. Darunter fallen auch Auskünfte über Inhaber statischer IP-Adressen, da dies zu den Bestandsdaten des Nutzers gehört. Allerdings darf nicht über alle Bestandsdaten Auskunft verlangt werden, sondern nur solche, die einen spezifischen Telekommunikationsbezug aufweisen (also zwar z. B. Name und Anschrift, nicht aber Bankverbindung des Nutzers). Auskünfte über Inhaber dynamischer IP-Adressen können hingegen nicht nach § 89 Abs. 6 TKG erlangt werden, da es sich insoweit um Verbindungsdaten handelt (s. u.).

Die bei der Nutzung eines Zugangs-Dienstes entstehenden **Verbindungsdaten** unterliegen als “nähere Umstände der Telekommunikation” dem Fernmeldegeheimnis nach § 85 TKG. Die Herausgabe von Verbindungsdaten über die zugrunde liegende Telekommunikation erfolgt aufgrund der §§ 100g und 100h Strafprozessordnung (StPO), die den Zugriff auf Verbindungsdaten gegenüber der früheren Rechtslage nach § 12 Fernmeldeanlagengesetz (FAG) teilweise beschränken, teilweise aber auch erweitern. So kann ein Richter (und bei Gefahr im Verzug die Staatsanwaltschaft) diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, zur Auskunft über die Verbindungsdaten verpflichten. Voraussetzung ist, dass bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von erheblicher Bedeutung, insbesondere eine Katalogstraftat nach § 100a Satz 1 StPO, oder mittels einer Endeinrichtung eine beliebige Straftat begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat. Die Anordnung darf nur Verbindungsdaten des Beschuldigten oder eine der sonstigen in § 100a StPO genannten Personen betreffen und kann (im Gegensatz zum bisherigen Rechtszustand) auch für zukünftige Telekommunikationsverbindungen angeordnet werden.

Als Verbindungsdaten zu betrachten sind gem. § 100g Abs. 3 StPO im Falle einer Verbindung Berechtigungskennungen, Kartennummern, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung, Beginn und Ende der Verbindung nach Datum und Uhrzeit, vom Kunden in Anspruch genommene Telekommunikationsdienstleistung, Endpunkte festgeschalteter Verbindungen, ihr Beginn und ihr Ende nach Datum und Uhrzeit. Aus der Formulierung “im Falle einer Verbindung” folgt, dass Daten über erfolglose Verbindungsversuche, die nach § 85 Abs.1 Satz 3 TKG ebenfalls dem Telekommunikationsgeheimnis unterliegen, nicht an die Strafverfolgungsbehörden herauszugeben sind. Für einen Zugangsanbieter bedeutet dies konkret, dass er Auskunft über folgende Verbindungsdaten erteilen muss: verwendetes Protokoll (z. B. http), IP-Nummer bzw. Domain-Name von Quell- und Zielserver, Datum und Uhrzeit des Abrufes. Außerdem muss er Auskünfte über Inhaber dynamischer IP-Adressen erteilen. Dazu gehört sowohl die Information, welche IP-Adressen innerhalb eines bestimmten Zeitraumes einem bekannten Nutzer zugewiesen waren bzw. zukünftig zugeordnet werden, als auch wem eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war.

100g StPO ermöglicht jedoch nur die Herausgabe von Verbindungsdaten, nicht den strafverfolgungsbehördlichen Zugriff auf Inhaltsdaten der Kommunikation. Inhaltsdaten sind in diesem Zusammenhang nicht nur die eigentlichen Inhalte der aufgerufenen Internet-Seiten, sondern auch solche Bestandteile

der URL (Uniform Resource Locator), die inhaltliche Angaben aufweisen. Demzufolge kann von einem Zugangsanbieter im Rahmen von § 100g StPO nur eine Auskunft über bestimmte Teilkomponenten der URL – namentlich Bezeichnung des Dienstes (http, ftp, pop etc.), des Hosts (IP-Adresse bzw. Domain-Name) und ggf. Port-Nummer – verlangt werden. Alle weiteren Bestandteile der URL wie Dateipfade, Inhalte von Anfragen oder Web-Formularen sind Inhalte der Telekommunikation und dürfen nur gem. §§ 100a, b StPO herausgegeben werden, wenn zuvor der Richter oder bei Gefahr im Verzuge die Staatsanwaltschaft mit binnen drei Tagen einzuholender richterlicher Bestätigung wegen des Verdachts einer in § 100a StPO genannten Katalogtat die Überwachung der Telekommunikation für die Zukunft angeordnet haben. Die Hilfsbeamten der Staatsanwaltschaft (Polizei) können diese Auskunft nicht verlangen.

4.2 E-Mail-Dienst

Die für den E-Mail-Dienst erhobenen **Bestandsdaten** dürfen – ebenso wie beim Zugangs-Anbieter – nach Maßgabe des § 89 Abs.6 TKG im Einzelfall auf Ersuchen an die zuständigen Stellen übermittelt werden, soweit dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgabe der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des militärischen Abschirmdienstes sowie des Zollkriminalamtes erforderlich ist. Eine richterliche Anordnung ist nicht erforderlich. Der E-Mail-Anbieter kann insbesondere Auskunft über die Zuordnung einer bestimmten Person zu einer bestimmten E-Mail-Adresse erteilen.

Inhaltsdaten und **Verbindungsdaten** von E-Mails unterliegen dem Fernmeldegeheimnis. Zu den Inhaltsdaten gehören auch der Betreff und die Bezeichnung von Dateianlagen. Die Überwachung der Inhalte ist dem entsprechend nur auf Basis der einschlägigen spezialgesetzlichen Eingriffsnormen zulässig. Rechtsgrundlage für diese Maßnahmen finden sich in den §§ 100a ff StPO, § 39 Außenwirtschaftsgesetz (AWG) und dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10). Die Anordnung nach § 100 a StPO darf nur durch den Richter oder bei Gefahr im Verzuge auch durch die Staatsanwaltschaft, nicht aber durch deren Hilfsbeamte, getroffen werden. Die angeordneten Maßnahmen berechtigen nicht zum Zugriff auf vergangene Telekommunikationsvorgänge.

Für die Weitergabe der **Verbindungsdaten** bei E-Mail-Diensten an die Strafverfolgungsbehörden gelten die §§ 100g, 100h StPO. Daten mit Inhaltsbezug (etwa Betreff, Bezeichnung von Dateianlagen) dürfen auf Grund dieser Regelungen (vgl. § 100g Abs.3 StPO) nicht an Strafverfolgungsbehörden übermittelt werden (s. o. 4.1).

Nach der Rechtsprechung des BGH stellt ein Zugriff von Strafverfolgungsbehörden auf Inhalte von E-Mail-Postfächern ebenfalls eine Telekommunikationsüberwachung dar. Das Eindringen in E-Mail-Systeme des Anbieters kann nicht auf die strafprozessualen Befugnisse der Beschlagnahme von Gegenständen oder zur Durchsuchung von Räumen gestützt werden, insbesondere weil der Zugriff anders als bei den vorgenannten Maßnahmen im Regelfall heimlich erfolgt und auch die zukünftige Kommunikation umfasst. Dies gilt auch dann, wenn z. B. ein Webmail-Anbieter Kopien bereits durch den Nutzer vom Server abgerufener E-Mails auf seinem Server speichert. Anders als bei einem Anrufbeantworter oder den auf dem PC des Nutzers gespeicherten abgerufenen E-Mails gilt hier weiterhin das Fernmeldegeheimnis, weil dies noch Bestandteil des vom Anbieter angebotenen E-Mail-Dienstes ist und der Nutzer zu Recht darauf vertraut, dass das Fernmeldegeheimnis für die gesamte Dauer der Erbringung des Dienstes (langfristige Bereithaltung von E-Mails auch zum wiederholten Abruf) gilt.

4.3 Inhalts-Anbieter (Content Provider)

§ 6 Abs. 5 Satz 5 TDDSG erlaubt es den Diensteanbietern, nach Maßgabe der hierfür geltenden Bestimmungen der Strafprozessordnung, Auskunft an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung zu erteilen.

Bestandsdaten im Bereich der Tele- und Mediendienste dürfen nur aufgrund einer Beschlagnahmeanordnung, die vom Richter und bei Gefahr im Verzuge auch durch die Staatsanwaltschaft oder ihre Hilfsbeamten erlassen werden kann, gem. §§ 94 ff. Strafprozessordnung (StPO) herausgegeben werden.

Inhaltsdaten, die bei der Nutzung von Tele- und Mediendiensten anfallen und mittels Telekommunikation übermittelt werden, unterliegen ebenso wie die Inhaltsdaten der Telekommunikation dem Fernmeldegeheimnis. Sie können durch die Strafverfolgungsbehörden nur mittels Überwachung und Aufzeichnung der Telekommunikation ermittelt werden. Rechtsgrundlagen für diese Maßnahmen finden sich in den §§ 100a ff StPO, § 39 Außenwirtschaftsgesetz (AWG) und dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10). Die Anordnung im Strafverfahren darf nur durch den Richter und bei Gefahr im Verzuge auch durch die Staatsanwaltschaft mit binnen drei Tagen einzuholender richterlichen Bestätigung erfolgen. Die angeordneten Maßnahmen berechtigen nur zum Zugriff auf zukünftig übertragene Inhalte.

4.4 Befugnisse der Nachrichtendienste

Mit dem Terrorismusbekämpfungsgesetz vom 9. 1. 2002 sind (befristet bis zum 10.1.2007) zusätzliche Erhebungsbefugnisse der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes (BND) und des Militärischen Abschirmdienstes (MAD) bei Anbietern von Telekommunikations- und Telediensten (nicht Mediendiensten) geschaffen worden. Die Nachrichtendienste dürfen im Einzelfall zur Erfüllung ihrer Aufgaben und unter der Voraussetzung, dass tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand bestimmte Staatsschutzdelikte oder Kapitalverbrechen plant, begeht oder begangen hat, von denjenigen, die geschäftsmäßig Telekommunikations- oder Teledienste erbringen oder daran mitwirken, unentgeltlich Auskünfte über Telekommunikationsverbindungsdaten und Teledienstenutzungsdaten einholen. Dies setzt eine Anordnung des Bundesinnenministeriums bzw. einer entsprechenden obersten Landesbehörde oder (im Fall des BND) des Chefs des Bundeskanzleramtes voraus. Die Auskunft kann auch in Bezug auf eine zukünftige Nutzung dieser Dienste verlangt werden. Eine Auskunftspflicht der Diensteanbieter gegenüber den Nachrichtendiensten besteht jedoch nicht, da der Gesetzgeber (anders als im Strafprozessrecht) einen entsprechenden Grundrechtseingriff nicht angeordnet hat.

Die Nachrichtendienste dürfen nur Auskunft über folgende Daten verlangen: Berechtigungskennungen, Kartennummern, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung, Beginn und Ende der Verbindung nach Datum und Uhrzeit, Angaben über die Art der vom Kunden in Anspruch genommenen Telekommunikations- und Teledienst-Dienstleistungen, Endpunkte festgeschalteter Verbindungen, ihr Beginn und ihr Ende nach Datum und Uhrzeit (§§ 8 Abs.8 Satz 3 BVerfSchG, 8 Abs.3a Satz 3 BNDG, 10 Abs.3 Satz 3 MADG).
Anbieter von Tele-, Medien- oder Telekommunikationsdiensten werden durch die Strafprozessordnung oder das Recht der Nachrichtendienste (Verfassungsschutzgesetze des Bundes und der Länder, BNDG, MADG) weder berechtigt noch verpflichtet, generell Daten über ihre Nutzer auf Vorrat zu erheben oder zu speichern, die sie zu keinem Zeitpunkt für ihre eigenen Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen (§§ 100a ff. StPO; 8 Abs.8 BVerfSchG; 3 Abs.1, 5 Abs.1 G 10; 8 Abs.3a BNDG; 10 Abs.3 MADG; 39, 40 AWG) Nachrichteninhalte aufzuzeichnen und bestimmte Daten, die sie ursprünglich für eigene Zwecke benötigt haben und nach dem Multimedia- oder Telekommunikationsrecht löschen müssten, weiter vorzuhalten und den Strafverfolgungsbehörden oder Nachrichtendiensten zu übermitteln.

Die Landesämter für Verfassungsschutz können Auskünfte über Telekommunikationsverbindungsdaten und Teledienstenutzungsdaten nur dann einholen, wenn die Landesgesetzgeber das Antragsverfahren, die Beteiligung der G 10-Kommission, die Verarbeitung der erhobenen Daten und die Mitteilung an den Betroffenen sowie eine parlamentarische Kontrolle gleichwertig wie im Bundesverfassungsschutzgesetz geregelt haben.