

Der Landesbeauftragte für den Datenschutz  
Mecklenburg-Vorpommern



# **Datenschutzfragen der Präsentation von öffentlichen Stellen im Internet**

## **Orientierungshilfe**

Stand: 2002

# Inhalt

<b>1 Einleitung</b> .....	<b>3</b>
<b>2 Allgemeine Rechtsgrundlagen</b> .....	<b>3</b>
<b>3 Zulässige Inhalte von Internetangeboten</b> .....	<b>3</b>
3.1 Unterschiede zu Veröffentlichungen in herkömmlichen Medien.....	3
3.2 Sachdarstellungen ohne Personenbezug .....	3
3.3 Mitarbeiterdaten.....	4
3.4 Weitere personenbezogene Veröffentlichungen.....	4
<b>4 Erforderliche Maßnahmen bei der Veröffentlichung im Internet</b> .....	<b>5</b>
4.1 Technische Maßnahmen.....	5
4.2 Organisatorische Maßnahmen .....	5
4.3 Durchführung und Kontrolle .....	6
<b>5 Umgang mit den Daten der Nutzer von Internetangeboten</b> .....	<b>6</b>
5.1 Rechtsgrundlagen .....	6
5.2 Tele- und Mediendienste.....	7
5.3 Inhaltliche Anforderungen .....	7
5.4 Folgerungen.....	8
<b>6 Online-Datenschutz-Prinzipien</b> .....	<b>8</b>
6.1 Begriff .....	8
6.2 Gründe für die Veröffentlichung .....	8
6.3 Form der Veröffentlichung .....	8
6.4 Inhalt .....	8

# 1 Einleitung

Behörden und andere öffentliche Einrichtungen veröffentlichen in zunehmendem Maß Informationen auf Web-Servern in Form so genannter Homepages. Welche Informationen veröffentlicht werden dürfen und welche technischen und organisatorischen Maßnahmen dabei erforderlich sind, ist jedoch nicht immer hinreichend bekannt. Das kann dazu führen, dass schutzwürdige Informationen im Internet unberechtigt allgemein zugänglich gemacht werden und so gegen Datenschutzbestimmungen verstoßen wird.

Diese Orientierungshilfe informiert darüber, welche Daten öffentliche Stellen im Internet veröffentlichen dürfen und welche rechtlichen, technischen und organisatorischen Anforderungen dabei zu erfüllen sind. Bereichsspezifische Regelungen können in einzelnen Teilen zu geringfügig abweichenden Forderungen führen.

## 2 Allgemeine Rechtsgrundlagen

Im Landesdatenschutzgesetz von Mecklenburg-Vorpommern (DSG M-V) ist geregelt, dass öffentliche Stellen personenbezogene Daten nur dann verarbeiten dürfen, wenn dies nach den Vorschriften dieses Gesetzes oder anderer Rechtsvorschriften zulässig ist oder wenn der Betroffene eingewilligt hat (§ 7 Abs. 1 DSG M-V).

Die Vorschriften des Landesdatenschutzgesetzes sind nach § 2 Abs. 4 Satz 1 DSG M-V nur dann anwendbar, wenn nicht besondere Rechtsvorschriften die Verarbeitung personenbezogener Daten regeln.

Die Einwilligung eines Betroffenen in die Verarbeitung seiner Daten ist nur wirksam, wenn sie den Anforderungen des § 8 DSG M-V genügt. Der Einwilligung muss eine ausreichende Unterrichtung über die vorgesehenen Nutzungsmöglichkeiten und die damit verbundenen Risiken vorausgehen.

Personenbezogene Daten sind gemäß § 3 Abs. 1 DSG M-V Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener).

## 3 Zulässige Inhalte von Internetangeboten

### 3.1 Unterschiede zu Veröffentlichungen in herkömmlichen Medien

Bei der Entscheidung, welche Daten in das Internet eingestellt werden sollen, müssen die Aspekte berücksichtigt werden, die bei anderen Medien nicht oder nicht in vergleichbarer Form vorhanden sind:

- Das Internet hat einen ständig wachsenden, unbegrenzten und weltweiten Adressatenkreis.
- Jede auch nur kurzzeitige Veröffentlichung kann durch Spiegelung auf anderen Web-Servern auf Dauer gespeichert werden.
- Durch Manipulation der Daten können Veröffentlichungen verfälscht werden, ohne dass die Nutzer es bemerken.
- Suchmaschinen im Internet erfassen im Laufe der Zeit alle verfügbaren Angebote und ermöglichen es jedermann, Daten dieser Angebote nach Stichwörtern oder Namen zusammenzuführen, so dass Personenprofile entstehen können. Oft haben die Betroffenen bei der Erteilung ihrer Zustimmung zur Veröffentlichung ihrer Daten in einem einzelnen Angebot oder bei Erstellung ihrer Homepages daran nicht gedacht.
- Selten bestehen gerichtlich durchsetzbare Ansprüche auf Löschung, Korrektur oder Gegendarstellung, da viele Betreiber ihren Sitz im Ausland haben und damit anderem Recht unterliegen, das diese Ansprüche möglicherweise nicht oder nur in abgeschwächter Form kennt.

### 3.2 Sachdarstellungen ohne Personenbezug

Sachdarstellungen ohne Personenbezug sind datenschutzrechtlich unproblematisch. Beispiele für zulässige Veröffentlichungen sind:

- Hinweise zu den Aufgaben der Behörde,
- Angaben zur Erreichbarkeit der Behörde und zu den Öffnungszeiten,
- Bereitstellen von Informationsmaterial und Formularen,
- Einstellen von Rechtsvorschriften,
- Übersichten und Organigramme ohne Personennamen.

### 3.3 Mitarbeiterdaten

Maßgeblich für die Verarbeitung von Mitarbeiterdaten ist § 35 DSGVO M-V. Nach § 35 Abs. 2 Nr. 3 DSGVO M-V ist die Übermittlung von Daten der Beschäftigten einer öffentlichen Stelle an Personen und Stellen außerhalb des öffentlichen Bereichs zulässig, wenn Art oder Zielsetzung der einem Beschäftigten übertragenen Aufgabe oder der Dienstverkehr es erfordert. Hierunter fällt grundsätzlich auch die Information, welcher Bedienstete der richtige Ansprechpartner für das Anliegen des Bürgers ist. Die uneingeschränkte Veröffentlichung von Telefonverzeichnissen und Geschäftsverteilungsplänen mit den Namen **aller** bei der Behörde beschäftigten Mitarbeiter ist hingegen unzulässig. Für die Veröffentlichung im Internet kommen lediglich Daten folgender Personenkreise in Betracht:

- die obere Leitungsebene einer Behörde,
- die Mitarbeiter mit Außenkontakten, die als offizielle Ansprechpartner fungieren (dies ist bei lediglich innerdienstlichen Aufgaben wie Registratur, Botendienst oder zentralem Schreibdienst in der Regel ausgeschlossen),
- wissenschaftliches Personal im Hochschulbereich (dies gilt aber nicht für wissenschaftliche Hilfskräfte),
- weitere Mitarbeiter nur mit deren Einwilligung und nur dann, wenn die Veröffentlichung der Aufgabenerfüllung dient.

Nachdem festgelegt wurde, von welchen Personen Informationen im Internet veröffentlicht werden sollen, ist zu entscheiden, welche Daten im Einzelnen eingestellt werden. Grundsätzlich zulässig sind nur folgende Angaben:

- Name,
- Funktion und Tätigkeitsbereich,
- Haus-, Post- und E-Mail-Adresse,
- dienstliche Telefon- und Faxnummern.

Weitergehende Daten oder Fotos dürfen nur mit Einwilligung des Mitarbeiters veröffentlicht werden und nur, sofern dies der Aufgabenerfüllung dient. Eine Veröffentlichung der Privatanschrift des Bediensteten ist auf jeden Fall unzulässig. Generell ist aber zu empfehlen, jeden Mitarbeiter vorab darüber zu informieren, welche Daten von ihm im Internet veröffentlicht werden sollen, und ihn gegebenenfalls um seine Zustimmung und Änderungsvorschläge zu bitten. Ist beabsichtigt, Daten einer größeren Zahl von Mitarbeitern im Internet zu veröffentlichen, so sollte das auf der Grundlage einer Dienstvereinbarung erfolgen.

### 3.4 Weitere personenbezogene Veröffentlichungen

- Angaben der **Mitglieder von Gremien** dürfen generell nur aufgenommen werden, wenn sie vorab ihr Einverständnis in die Veröffentlichung erklärt haben (z. B. Mitbestimmungsgremien von Schulen). Namen und Funktion allgemein gewählter Mitglieder eines Organs (z. B. Landtag, kommunale Vertretungskörperschaften) dürfen auch ohne deren Zustimmung in dem Internetangebot erscheinen. Weitergehende Angaben dürfen nur mit Einwilligung dieser Personen eingestellt werden.
- Die Bereitstellung von Sitzungsunterlagen oder **Protokollen der kommunalen Organe** ist zulässig, soweit sie den öffentlichen Teil betreffen und Personenbezüge entfernt wurden.
- Die Präsentation von **Gewerberegisterdaten** ist nicht zulässig.
- Die allgemein zugängliche Veröffentlichung von **Forschungsergebnissen**, die Einzelpersonen betreffen, ist nur zulässig, wenn die Daten vor ihrer Veröffentlichung anonymisiert oder hinreichend pseudonymisiert wurden, so dass es außenstehenden Dritten auch mit Zusatzwissen nicht möglich ist, einen Personenbezug herzustellen. Gegebenenfalls müssen auch weitere Daten zusätzlich abstrahiert oder verändert werden, indem etwa das Geburtsdatum durch das Lebensalter oder exakte Ortsbezeichnungen durch regionale Angaben ersetzt werden. Von der Aufnahme sensibler Daten in das Internet (z. B. umfassende

medizinische Befundberichte mit zusätzlichen, für die Identifizierung geeigneten Daten wie Aufnahmezeit, Behandlungsgrund oder Behandlungszeit) ist auch dann abzurufen, wenn konkret identifizierende Daten wie Name, Adresse oder Geburtsdatum nicht beigefügt sind.

## 4 Erforderliche Maßnahmen bei der Veröffentlichung im Internet

### 4.1 Technische Maßnahmen

Um eine sichere und datenschutzgerechte Veröffentlichung von Informationen auf Web-Servern zu gewährleisten, sind folgende technische Maßnahmen zu treffen:

- Entwicklungs- und Produktionsumgebung sind strikt voneinander zu trennen. Dies bedeutet, dass auf dem Web-Server nur solche Daten gespeichert werden, die tatsächlich zur Veröffentlichung bestimmt sind.
- Der Web-Server soll so konfiguriert werden, dass eine Anzeige der Verzeichnisstruktur („Directory-Listing“) nicht möglich ist.
- Auf dem Web-Server sollten nur virtuelle Verzeichnisse verwendet werden, die die tatsächlichen Verzeichnisnamen verbergen.
- Verzeichnisse, die nur einem begrenzten Besucherkreis zugänglich sein sollen, sind vor unbefugtem Zugriff zu sichern, beispielsweise mit Passwörtern. In diesem Fall muss darauf geachtet werden, dass
  - entweder die Verwendung von Einmalpasswörtern möglich ist oder eine gesicherte Übertragung der Mehrfachpasswörter erfolgen kann und
  - der Web-Server zur Präsentation der Information in einen abgesicherten Übertragungsmodus (S-HTTP) wechselt, um die personenbezogenen Daten durch kryptographische Verschlüsselungsverfahren sichern zu können.
- Die Schreibrechte auf den Server sind auf das unabdingbare Maß zu beschränken und abzusichern.
- Um Angriffe auf den Web-Server zu erschweren, sollten nur die unbedingt erforderlichen Dienste beziehungsweise Protokolle auf dem Server aktiviert werden.
- Auf die Verwendung aktiver Inhalte (JavaScript, Java und ActiveX) sowie auf die Ablage von Cookies sollte verzichtet werden, da restriktiv konfigurierte Firewallsysteme die aktiven Komponenten aus Sicherheitsgründen ausfiltern und ansonsten unnötige Risiken für die zugreifenden Rechner entstehen.
- Links auf Homepages von Personen oder Institutionen sollten nur mit dem ausdrücklichen Einverständnis der Eigentümer gesetzt werden; keinesfalls kann das Einrichten einer eigenen Seite als allgemeine Zustimmung zur Aufnahme in Linklisten gewertet werden.
- Elektronische, zum Ausdruck bestimmte Formulare sollten in einem Format angeboten werden, das von Abrufenden möglichst nicht verfälscht werden kann.
- Die Eingabe von personenbezogenen Daten in elektronische Formulare sollte mit einem Online-Dialogverfahren nur dann möglich sein, wenn die Datenübertragung durch Verschlüsselung und gegebenenfalls elektronische Unterschrift ausreichend gesichert ist.

### 4.2 Organisatorische Maßnahmen

Neben technischen Vorkehrungen sind auch organisatorische Maßnahmen zu treffen. Insbesondere dürfen personenbezogene Daten im Internet in der Regel nur veröffentlicht werden, wenn folgende Vorgaben erfüllt sind:

- Es ist festzulegen und zu dokumentieren, wer zuständig ist für
  - die Installation und die Pflege des Web-Servers,
  - die Pflege der auf dem Web-Server gespeicherten Informationsangeboten und
  - die Freigabe der auf den Web-Server zu übernehmenden Informationen.
- Unter Beteiligung des behördlichen Datenschutzbeauftragten sollten Richtlinien zur Veröffentlichung im Internet erstellt werden, in denen vor allem geregelt ist,
  - welche Arten von personenbezogenen Daten gegebenenfalls eingestellt werden können und in welchem Umfang dies geschehen darf und

- welche Maßnahmen darüber hinaus möglicherweise erforderlich sind.
- Werden Daten von Mitarbeitern der eigenen Behörde veröffentlicht, ist die Regelung zur Mitbestimmung des Personalrates bei Informations- und Kommunikationsnetzen in § 70 Abs. 1 Nr. 5 Personalvertretungsgesetz zu beachten.
- Ist es nicht möglich, personenbezogene Daten mit entsprechenden Sicherungsmaßnahmen zu übermitteln, sind die Abrufenden ausdrücklich auf die mit der Übertragung verbundenen Risiken und die Freiwilligkeit der Nutzung hinzuweisen. Dies gilt auch, wenn E-Mail-Adressen veröffentlicht werden.

### 4.3 Durchführung und Kontrolle

Bei der Umsetzung der in den beiden vorangehenden Abschnitten dargestellten Maßnahmen sind folgende Aspekte zu berücksichtigen:

- Vor der Übertragung von personenbezogenen Daten auf den Web-Server sollte der behördliche Datenschutzbeauftragte die Einhaltung der oben erläuterten Richtlinien prüfen.
- Vor der erstmaligen Bereitstellung der Internetangebote und danach in unregelmäßigen Zeitabständen sollte der Datenschutzbeauftragte die Darstellung personenbezogener Daten daraufhin prüfen, ob die notwendigen schriftlichen Einverständniserklärungen vorliegen und dabei eine ausreichende Unterrichtung der Betroffenen über die vorgesehenen Nutzungsmöglichkeiten und die damit verbundenen Risiken erfolgt ist.
- Werden die zu veröffentlichenden Seiten automatisch erzeugt (z. B. aus Datenbanken heraus), ist besondere Sorgfalt geboten, weil Datenfelder und Dateninhalte weitgehend automatisch übernommen werden. Neben der Browser-Darstellung ist auch der Quelltext der Seite auf Konformität mit den Richtlinien zu überprüfen.
- Soweit möglich, sollten für die Veröffentlichung vorgesehene Dateien auf personenbezogene Daten nicht nur manuell, sondern auch automatisiert untersucht werden (beispielsweise durch Abgleich mit der Namensliste aller Mitarbeiter).
- Das Kopieren von Dateien aus der Entwicklungsumgebung auf den Web-Server muss sehr sorgfältig überwacht werden.
- Vor dem Kopieren ganzer Verzeichnisse müssen diese genau daraufhin durchsucht werden, ob sie Dateien enthalten, die nicht für die Veröffentlichung bestimmt sind. Solche Dateien sind vorher zu entfernen.
- Das Kopieren von Daten sollte unmittelbar nach dem Abschluss anhand der eventuell automatisch erzeugten Protokolldateien auf Korrektheit geprüft werden.

## 5 Umgang mit den Daten der Nutzer von Internetangeboten

### 5.1 Rechtsgrundlagen

Für den Umgang mit den personenbezogenen Daten der Nutzer von im Internet angebotenen Diensten – wozu auch der Zugang zum Internet selbst gehört – gibt es folgende bereichsspezifische Vorschriften, die den allgemeinen Datenschutzgesetzen vorgehen:

- das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG) für Teledienste und
- der Mediendienste-Staatsvertrag (MDStV) für Mediendienste.

Dabei ist aber zu berücksichtigen, dass die vorstehenden Normen nur den Umgang mit den personenbezogenen Daten regeln, die aufgrund der Nutzung des Internet anfallen (Dienste-Ebene). Die Datenschutzgesetze und auch sonstiges „Offline“-Recht gelangen (wieder) zur Anwendung, wenn es um von der eigentlichen Internetnutzung unabhängige inhaltliche Fragen geht, etwa um die Veröffentlichung von Namenslisten oder um die Daten in einem Bestellformular für ein materielles Gut (Inhaltsebene).

## 5.2 Tele- und Mediendienste

**Teledienste** sind auf Telekommunikation basierende, elektronische Informations- und Kommunikationsdienste, die für eine **individuelle Nutzung** von kombinierbaren Daten bestimmt sind (§ 2 Abs. 1 TDG). Beispiele für Teledienste sind gemäß § 2 Abs. 2 TDG unter anderem:

- Angebote im Bereich der Individualkommunikation (z. B. Telebanking),
- Angebote zur Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht (Verkehrs- und Wetterdatendienste, Verbreitung von Wareninformationen),
- Angebote zur Nutzung des Internet oder weiterer Netze.

**Mediendienste** sind auf Telekommunikation basierende, an die **Allgemeinheit gerichtete** Informations- und Kommunikationsdienste (§ 2 Abs. 1 Satz 1 MDSStV). Darunter fallen nach § 2 Abs. 2 MDSStV insbesondere:

- Fernsehverkauf (Teleshopping),
- Verbreitung von Messergebnissen in Text oder Bild,
- Verteildienste in Form von Fernsehtext, Radiotext und vergleichbaren Textdiensten.

Die Abgrenzung zwischen Tele- und Mediendiensten ist oft schwierig, aber meist entbehrlich, da die Regelungen des TDG und des TDDSG einerseits sowie des MDSStV andererseits inhaltlich weitgehend identisch sind.

Internetangebote öffentlicher Stellen sind in der Regel als Teledienste anzusehen. Eine Ausnahme stellt die Veröffentlichung von Presseerklärungen dar, diese sind als Mediendienste einzustufen.

## 5.3 Inhaltliche Anforderungen

Aus den Vorschriften über die Tele- und Mediendienste ergeben sich umfangreiche Anforderungen für die Anbieter solcher Dienste. Insbesondere sind die folgenden Vorgaben einzuhalten:

- Es besteht eine Pflicht zur so genannten Anbieterkennzeichnung (§ 6 TDG, § 10 MDSStV). Der Nutzer muss erkennen können, wer einen Tele- oder Mediendienst anbietet.
- Der Anbieter darf die Erbringung von Diensten nicht von einer Einwilligung des Nutzers in die Verarbeitung und Nutzung seiner Daten für andere Zwecke abhängig machen (§ 3 Abs. 4 TDDSG, § 17 Abs. 4 MDSStV).
- Der Nutzer ist vor Beginn des Nutzungsvorgangs über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten zu unterrichten; der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein (§ 4 Abs. 1 TDDSG, § 18 Abs. 1 MDSStV).
- Der Anbieter hat dem Nutzer die Inanspruchnahme von Diensten anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist; der Nutzer ist über diese Möglichkeit zu informieren (§ 4 Abs. 6 TDDSG, § 18 Abs. 6 MDSStV).
- Nutzerprofile sind nur zulässig (§ 6 Abs. 3 TDDSG, § 19 Abs. 4 MDSStV), wenn
  - sie für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Dienste verwendet werden sollen,
  - der Diensteanbieter den Nutzer auf sein Widerspruchsrecht hingewiesen hat,
  - der Nutzer der Erstellung von Nutzerprofilen nicht widersprochen hat und
  - die Nutzungsprofile nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.
- Der Anbieter hat Nutzungsdaten frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung zu löschen, soweit es sich nicht um Abrechnungsdaten handelt (§ 6 Abs. 4 Satz 1 TDDSG, § 19 Abs. 5 Satz 1 MDSStV).
- Der Nutzer ist berechtigt, jederzeit die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten unentgeltlich beim Diensteanbieter einzusehen (§ 4 Abs. 7 TDDSG, § 20 Abs. 1 MDSStV).
- Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen (§ 4 Abs. 5 TDDSG, § 18 Abs. 5 MDSStV).
- Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen unter anderem sicherzustellen (§ 4 Abs. 4 Satz 1 TDDSG, § 18 Abs. 4 Satz 1 MDSStV), dass
  - der Nutzer seine Verbindung mit dem Diensteanbieter jederzeit abbrechen kann,

- die anfallenden personenbezogenen Daten unmittelbar nach dem Ende der Nutzung des Dienstes gelöscht werden, soweit sie nicht für Abrechnungszwecke oder für Zwecke der Datensicherheit erforderlich sind,
- die angebotenen Dienste gegen Kenntnisnahme Dritter geschützt in Anspruch genommen werden können,
- die personenbezogenen Daten über die Inanspruchnahme verschiedener Dienste durch einen Nutzer getrennt verarbeitet und nur zusammengeführt werden, soweit dies für Abrechnungszwecke erforderlich ist.

## 5.4 Folgerungen

Die Pflichten der Diensteanbieter haben unter anderem folgende Konsequenzen:

- Bei kostenlosen Zugriffen auf Internetseiten dürfen im Allgemeinen keine personenbezogenen Daten des Nutzers, etwa seine E-Mail-Adresse oder seine IP-Nummer, protokolliert werden.
- Werden personenbezogene Daten des Nutzers erhoben, so muss er in der Regel auf den entsprechenden Internetseiten genau über Art, Umfang, Ort und Zweck der Erhebung, der Verarbeitung und der Nutzung seiner Daten unterrichtet werden (siehe dazu Punkt 6).
- Nutzungsstatistiken sollten sparsam angelegt werden und einen geringen Detaillierungsgrad aufweisen. Sie dürfen grundsätzlich nur anonym oder durch Aggregieren von (rechtmäßig erlangten) Individualdaten gewonnen werden.
- Viele Verstöße gegen die oben genannten Pflichten stellen Ordnungswidrigkeiten dar, die mit Geldbußen bis zu 250.000 € geahndet werden können.

## 6 Online-Datenschutz-Prinzipien

### 6.1 Begriff

Online-Datenschutz-Prinzipien sind eine umfassende Erklärung zu Grundsätzen und Verfahrensweisen einer Institution hinsichtlich der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten, die im Zusammenhang mit der Bereitstellung und Nutzung eines Informationsangebotes im Internet auftreten. Das Merkmal „Institution“ ist dabei sehr weit zu verstehen und nicht auf Behörden beschränkt.

### 6.2 Gründe für die Veröffentlichung

Online-Datenschutz-Prinzipien müssen veröffentlicht werden, wenn personenbezogene Daten der Nutzer während der Nutzung der Internetseiten gesammelt werden, sofern die Nutzer nicht anderweitig unterrichtet werden. Dies gilt insbesondere bei der Verwendung von Cookies oder der Protokollierung personenbezogener Nutzerdaten.

Auch wenn der Nutzer von sich aus personenbezogene Daten preisgibt – etwa bei der Nutzung von Angeboten zur Online-Registrierung, beim Versenden von E-Mails an die Institution oder beim Ausfüllen von Online-Formularen – sollte er über die Verwendung seiner Daten informiert werden.

Selbst wenn keine oder nur anonyme Daten der Nutzer gespeichert werden, ist die Bekanntmachung von Online-Datenschutz-Prinzipien empfehlenswert. Denn durch diese Information werden beim Benutzer eventuell vorhandene Bedenken und Befürchtungen hinsichtlich der Verarbeitung seiner Daten zerstreut.

### 6.3 Form der Veröffentlichung

Online-Datenschutz-Prinzipien sollten vor oder auf der eigentlichen Begrüßungsseite veröffentlicht werden. Hierfür geeignet wären beispielsweise ein entsprechender Text auf dieser Seite oder ein Link über eine aussagekräftige Schaltfläche. Außerdem müssten diese Hinweise von jedem angebotenen Formular und möglichst auch von jeder Internetseite des Angebotes aus direkt erreichbar sein. Vor jedem Setzen eines Cookies oder einer anderen Aktion auf Seiten des Nutzers oder des Anbieters, die zu einer Speicherung von personenbezogenen Daten des Nutzers führt, sollten die Online-Datenschutz-Prinzipien automatisch zur Kenntnisnahme angeboten werden.

### 6.4 Inhalt

Online-Datenschutz-Prinzipien müssen in der Regel über folgende Aspekte Auskunft geben:

- Art, Verwendungszweck und Aufbewahrungsdauer der gespeicherten personenbezogenen Daten,
- Behandlung von E-Mail-Adressen (z. B. Weitergabe an bestimmte Institutionen),
- Protokollierung personenbezogener Daten (Zweck, Umfang und Dauer),
- Verwendung von Cookies (Umfang, Behandlung und Verwendung der Daten, Möglichkeit des Abschaltens).

Sie sollten auch über die nachstehenden Punkte informieren:

- Einbindung eines externen Dienstleisters bei der Erstellung der Internetseiten oder beim Betrieb des Servers,
- Maßnahmen zur Überprüfung, Richtigstellung und Löschung personenbezogener Daten,
- Angebote zur Wahrung der Sicherheit und Vertraulichkeit personenbezogener Daten (beispielsweise kryptographische Verfahren),
- verbleibende Restrisiken bei der Übertragung freiwillig preisgebener Daten,
- Kontaktperson für weiterführende Fragen.