

## Orientierungshilfe für Anbieter von Telemedien

Einleitung .....	2
Wer ist Diensteanbieter? .....	2
Was sind Telemedien? .....	2
Was haben Diensteanbieter zu beachten? .....	2
Impressumpflicht.....	2
Links auf fremde Inhalte .....	3
Umgang mit personenbezogenen Daten .....	3
Was sind personenbezogene Daten? .....	3
Grundsätzliches zur Verarbeitung personenbezogener Daten .....	3
Datengeheimnis .....	4
Datenschutzbeauftragter .....	4
Verfahrensbeschreibung .....	4
Auftragsdatenverarbeitung.....	4
Technische und organisatorische Maßnahmen .....	4
<i>Verschlüsselung bei der Verarbeitung von personenbezogenen Daten</i> .....	4
Welche speziellen Pflichten ergeben sich aus dem TMG für die Verarbeitung von personenbezogenen Daten? .....	4
<i>Vor Beginn der Nutzung von Telemedien</i> .....	4
<i>Wenn personenbezogen Daten mit elektronischer Einwilligung verarbeitet werden</i> ...	4
<i>Technische und organisatorische Vorkehrungen des Diensteanbieters</i> .....	4
Einwilligung zur Verarbeitung von personenbezogener Daten.....	5
Transparenzanforderungen.....	5
Reichweitenmessung / Webstatistik / Speicherung von IP-Adressen .....	5
Newsletter .....	6

## Einleitung

Diese Handreichung richtet sich an alle Bürger Niedersachsens, die privat oder geschäftlich im Internet als Diensteanbieter Telemedien anbieten. Dies soll eine Orientierungshilfe für die Realisierung eines rechtssicheren Internetauftritts sein. Der Schwerpunkt liegt hier bei den Belangen des Datenschutzes.

## Wer ist Diensteanbieter?

Diensteanbieter im Sinne des Telemediengesetzes ist jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt ([§ 2 Abs. 1 Nr. 1 Telemediengesetz \(TMG\)](#)). Eine Unterscheidung zwischen privater oder geschäftlicher Nutzung findet sich hier nicht.

## Was sind Telemedien?

Telemedien sind nach [§ 1 Abs. 1 TMG](#) alle elektronischen Informations- und Kommunikationsdienste, die weder Rundfunk noch reine Telekommunikationsdienste oder telekommunikationsgestützte Dienste (s. [§ 3 Nr. 24 und 25 Telekommunikationsgesetz \(TKG\)](#)) sind. Die Abgrenzung kann im Einzelfall schwierig sein. Telemedien sind zum Beispiel<sup>1</sup>:

- Online-Angebote von Waren/Dienstleistungen mit unmittelbarer Bestellmöglichkeit (z. B. Angebote von Verkehrs-, Wetter-, Umwelt- oder Börsendaten, Newsgroups, Chatrooms, elektronische Presse, Fernseh-/ Radiotext, Teleshopping),
- Video auf Abruf, soweit es sich nicht nach Form und Inhalt um einen Fernsehdienst im Sinne der Richtlinie 89/552/EWG (Richtlinie Fernsehen ohne Grenzen) handelt, der also zum Empfang durch die Allgemeinheit bestimmt ist und nicht auf individuellen Abruf eines Dienstleistungsempfängers erbracht wird. Solche Dienste unterliegen der Rundfunkregulierung durch die Länder. Hierbei orientiert sich die Einordnung an den europarechtlichen Vorgaben, die inzwischen durch die Rechtsprechung des EuGH (Mediakabel-Entscheidung, Rechtssache C 89/04 vom 2. Juni 2005, Abl. C 182/16 vom 23. Juli 2005) konkretisiert wurden,
- Online-Dienste, die Instrumente zur Datensuche, zum Zugang zu Daten oder zur Datenabfrage bereitstellen (z. B. Internet-Suchmaschinen) sowie alle Online-Angebote, die über das Internet abrufbar sind (insbesondere Online-Angebote von Waren/Dienstleistungen mit unmittelbarer Bestellmöglichkeit, Teleshopping, Angebote von Verkehrs-, Wetter-, Umwelt- oder Börsendaten, Newsgroups, Chatrooms, elektronische Presse, Foren, Video auf Abruf und alle sonstigen WWW-Angebote)
- die kommerzielle Verbreitung von Informationen über Waren-/Dienstleistungsangebote mit elektronischer Post (z. B. Werbe-Mails).

## Was haben Diensteanbieter zu beachten?

### Impressumpflicht

Telemedien sind im Rahmen der Gesetze zulassungs- und anmeldefrei ([§ 4 TMG](#)). Es ergeben sich allerdings aus den TMG Pflichten für Diensteanbieter. Hier gibt es zunächst nach [§ 5 TMG](#) die allgemeinen Informationspflichten. Nach [§ 6 TMG](#) gibt es darüber hinaus besondere Informationspflichten bei kommerziellen Kommunikationen und gegebenenfalls Angaben nach [§ 2 der Verordnung über Informationspflichten für Dienstleistungserbringer \(DL-InfoV\)](#).

In Niedersachsen ist das [niedersächsische Landesamt für Verbraucherschutz und Lebensmittelsicherheit](#) (LAVES) zuständig für die Überwachung der Einhaltung der Impressumspflichten für Telemedien nach dem [Rundfunkstaatsvertrag \(RStV\)](#), dem

---

<sup>1</sup> [Deutscher Bundestag, 16. Wahlperiode, Drucksache 16/3078 vom 23.10.2006](#)

[Telemediengesetz \(TMG\)](#) sowie dem [Nds. Pressegesetz \(PresseG\)](#). Da ein Webimpressum grundsätzlich bei allen Angeboten von Telemedien erforderlich ist und seit dem 01.03.2007 der RStV und das TMG eine „gestaffelte Impressumspflicht“ für Telemedien vorsieht, prüfen Sie am besten mittels dieser [Handreichung](#) des [LAVES](#), ob Ihr Impressum den Anforderungen des RStV und des TMG gerecht wird.

### **Links auf fremde Inhalte**

Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich ([§ 7 Abs. 1 TMG](#)). Diensteanbieter sollten einen unbrauchbaren Disclaimer nach dem Schema „*Mit Urteil vom 12. Mai 1998 hat das Landgericht Hamburg...*“ vermeiden.

Eine Klausel mit einer pauschalen Distanzierung ist kein Freibrief für eine Veröffentlichung. Sie ist keine Distanzierung, sondern vielmehr eine nicht verantwortete Weitergabe und damit eine eigene Verbreitung. Zudem gibt es im deutschen Rechtssystem keine pauschale Distanzierung von jeglicher Verantwortung für eigene Taten.

Diensteanbieter sind für verlinkte rechtswidrige Inhalte aber nur dann verantwortlich, wenn sie von den Inhalten Kenntnis haben. Sie sind ausdrücklich nicht verpflichtet aktiv nach rechtswidrigen Inhalten zu suchen, haben aber bei Kenntnis umgehend zu reagieren. Finden sich also auf einer verlinkten und zunächst unbeanstandeten fremden Seite später rechtswidrige Inhalte, so haftet derjenige, der diese fremde Seite verlinkt hat, wenn ihm nachzuweisen ist oder wenn es deutliche Indizien dafür gibt, dass er von den neuen rechtswidrigen Inhalten Kenntnis hatte. Genauso haftet der Diensteanbieter nur für rechtswidrige Inhalte von Nutzern innerhalb seines Telemediendienstes, wenn er Kenntnis erlangt hat und nicht angemessen darauf reagiert.

### **Umgang mit personenbezogenen Daten**

Wenn Diensteanbieter innerhalb Ihres Telemedienangebotes personenbezogene Daten erheben, ergeben sich daraus eine Vielzahl von zusätzlichen Verpflichtungen für sie.

### **Was sind personenbezogene Daten?**

Nach [§ 3 Abs. 1 BDSG](#) sind das Einzelangaben über persönlich oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person. Hierunter fallen z. B. Angaben wie Name, Post-Adresse, E-Mail-Adresse, Telefonnummer aber auch die IP-Adresse.

### **Grundsätzliches zur Verarbeitung personenbezogener Daten**

Gemäß [§ 3a Bundesdatenschutzgesetz](#) (BDSG) gibt es die Pflicht zur Datenvermeidung und Datensparsamkeit: *„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.“*

Im Datenschutzrecht gilt ein „Verbot mit Erlaubnisvorbehalt“, d. H. es ist alles verboten, was nicht ausdrücklich erlaubt ist<sup>2</sup>. Erlaubt ist die Erfassung, Verarbeitung oder Nutzung personenbezogener Daten nur wenn:

- und soweit das BDSG dies erlaubt,
- eine andere Rechtsvorschrift dies vorschreibt / erlaubt oder
- der Betroffene freiwillig und gemäß [§ 13 Absatz 2 TMG](#) bewusst und eindeutig eingewilligt hat

---

<sup>2</sup> [§ 4 Absatz 1 BDSG](#)

## Datengeheimnis

Alle MitarbeiterInnen, die mit automatisiert verarbeiteten personenbezogenen Daten in Berührung kommen, sind auf das Datengeheimnis zu verpflichten<sup>3</sup>.

## Datenschutzbeauftragter

Die Bestellung eines [betrieblichen Datenschutzbeauftragten](#) bei nicht-öffentlichen Stellen ist erforderlich wenn:

- Sie Verfahren vornehmen, die der [Vorabkontrolle](#) unterliegen;
- personenbezogene Daten automatisiert erhoben, verarbeitet oder genutzt werden und damit mindestens zehn Personen beschäftigen.
- personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Beschäftigte hiermit beschäftigt sind<sup>4</sup>.

## Verfahrensbeschreibung

Eine Verfahrensbeschreibung oder auch Verfahrensdokumentation wird für die Vorabkontrolle nach [§ 4d Abs. 5 und 6 BDSG](#) benötigt und ist für jedes Verfahren von der verantwortlichen Stelle dem Beauftragten für den Datenschutz zur Verfügung zu stellen<sup>5</sup>. Darüber hinaus dient sie auch der Umsetzung des „Jedermannrechts“<sup>6</sup>:

Der Beauftragte für den Datenschutz (oder - falls keiner bestellt ist - die verantwortliche Stelle) macht die Angaben nach [§ 4e Satz 1 Nr. 1 bis 8 BDSG](#) auf Antrag jedermann in geeigneter Weise verfügbar. Eine Verfahrensbeschreibung ist bei der Verarbeitung von personenbezogenen Daten immer zu erstellen und vorzuhalten.

Ein Vordruck für die Verfahrensbeschreibung zum Herunterladen finden Sie [hier](#) und Ausfüllhinweise für die Erstellung einer Verfahrensdokumentation [hier](#).

## Auftragsdatenverarbeitung

Soweit Dritte als Auftragsdatenverarbeiter gem. [§ 11 BDSG](#) (z.B. Hoster, Provider etc.) für die verantwortliche Stelle tätig werden, ist das Verfahren im Verfahrensverzeichnis der verantwortlichen Stelle aufzunehmen. Verantwortlich für die personenbezogenen Daten bleibt weiterhin der Auftraggeber. Weitere Hinweise zur Auftragsdatenverarbeitung sich [hier](#).

## Technische und organisatorische Maßnahmen

Laut [§ 9 BDSG](#) gilt: „Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

In der Anlage zu [§ 9 Satz 1 BDSG](#) werden diese Maßnahmen näher ausgeführt. Es handelt sich dabei um: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und die Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Weitergehende Informationen und Checklisten hierzu finden sich [hier](#).

Gemäß [§ 13 Abs. 7 TMG](#) haben Diensteanbieter, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig

---

<sup>3</sup> [§ 5 BDSG](#)

<sup>4</sup> [§ 4f BDSG](#)

<sup>5</sup> [§ 4g Abs. 2 Satz 1 BDSG](#)

<sup>6</sup> [§ 4g Abs. 2 Satz 2 BDSG](#)

angebotene Telemedien durch technische und organisatorische Vorkehrungen<sup>7</sup> sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und diese gegen Verletzungen des Schutzes personenbezogener Daten und gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Diese Vorkehrungen müssen den Stand der Technik berücksichtigen.

### ***Verschlüsselung bei der Verarbeitung von personenbezogenen Daten***

Eine Maßnahme für Zugangskontrolle, Zugriffskontrolle und Weitergabekontrolle von personenbezogenen Daten ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

### **Welche speziellen Pflichten ergeben sich aus dem TMG für die Verarbeitung von personenbezogenen Daten?**

Der Diensteanbieter darf personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat und er darf für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.<sup>8</sup>

### ***Vor Beginn der Nutzung von Telemedien***

Diensteanbieter haben den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten gemäß [§ 13 TMG](#) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist.

Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für die Nutzer des Telemediums jederzeit abrufbar sein.

### ***Wenn personenbezogenen Daten mit elektronischer Einwilligung verarbeitet werden***

Diensteanbieter haben die Nutzer ihres Telemediendienstes vor Erklärung der Einwilligung auf das Recht zum Widerruf der Einwilligung nach [§ 13 Abs. 2 Nr. 4 TMG](#) hinzuweisen. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein (Spätestens wenn der Nutzer seine persönlichen Daten eingibt, muss die Belehrung deutlich eingeblendet werden. Der Vorgang darf erst dann fortgesetzt werden können, wenn der Nutzer die Belehrung akzeptiert hat. Die Einwilligung muss nachprüfbar gespeichert werden.).

### ***Technische und organisatorische Vorkehrungen des Diensteanbieters***

Diensteanbieter haben durch technische und / oder organisatorische Vorkehrungen sicherzustellen, dass

- der Nutzer die Nutzung des Dienstes jederzeit beenden kann,
- die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht werden,
- der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,

---

<sup>7</sup> Eine Maßnahme nach § 13 Abs. 7, Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

<sup>8</sup> [§ 12 TMG](#)

- die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,
- Nutzungsdaten verschiedener Telemedien nach [§ 15 Abs. 2 TMG](#) nur für Abrechnungszwecke zusammengeführt werden können und
- Nutzungsprofile nach [§ 15 Abs. 3 TMG](#) nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

### **Einwilligung zur Verarbeitung von personenbezogener Daten**

Die Anforderungen hieran werden von den [§§ 4a, 28 Abs. 3a BDSG](#), sowie im Fall einer elektronischen Einwilligung zusätzlich von den [§§ 13 Abs. 2 u. 3 TMG, § 94 TKG](#) festgelegt. Danach muss eine Einwilligung, um rechtliche Relevanz zu erreichen, freiwillig erteilt worden sein. Sind mit der Nichterteilung evtl. negative Folgen für den Betroffenen verbunden, so muss er hierauf ausdrücklich hingewiesen werden. Die Erklärung muss hinreichend bestimmt sein bzgl. folgender Angaben enthalten: beteiligte Daten verarbeitende Stellen, verfolgter Zweck und Art der Daten. Die Erklärung muss schriftlich abgegeben werden und, wenn dies in Zusammenhang mit anderen Erklärungen erfolgt, besonders hervor gehoben sein. An Stelle der konventionellen schriftlichen Einwilligung ist auch eine elektronische Erklärung möglich. Auch diese muss bewusst vor Beginn der zu erlaubenden Datenverarbeitung abgegeben werden, eindeutig sein, protokolliert werden und widerrufbar sein. Auf die Widerrufbarkeit muss hingewiesen werden, und der Inhalt der Einwilligung muss für den Betroffenen jederzeit abrufbar sein.

Die praktischen Anforderungen an elektronische Einwilligungen sind rechtlich noch nicht endgültig geklärt. In jedem Fall gilt hier, dass ein Logfile in dem IP-Adresse mit Timestamp<sup>9</sup> gespeichert ist nicht genügt.

### **Transparenzanforderungen**

Nach [§ 13 Abs. 1 S. 1 TMG](#) hat ein Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung in Staaten außerhalb des EU/EWR-Raumens in allgemein verständlicher Form zu unterrichten.

- Es besteht die Pflicht zur Unterrichtung sofern Cookies zur Reidentifizierung von Nutzenden nach [§ 13 Abs. 1 S. 2 TMG](#) gesetzt werden.
- Es besteht die Pflicht zum Hinweis auf das bestehende Widerrufsrecht bei Einwilligungen zur Datenverarbeitung von personenbezogenen Daten.
- Es besteht die Hinweispflicht im Fall von Profilbildungen nach [§ 15 Abs. 3 TMG](#).
- Nach [§ 13 Abs. 6 S. 2 TMG](#) sind die Nutzenden über die Möglichkeit der Nutzung bzw. der Bezahlung in anonymer bzw. pseudonymer Form zu unterrichten.
- Es besteht das Erfordernis einer bewussten und eindeutigen Einwilligungserteilung nach [§ 13 Abs. 2 Nr. 1 TMG](#).
- Gemäß [§ 13 Abs. 2 Nrn. 3, 4 TMG](#) muss der Nutzende den Einwilligungsinhalt, also die Datenschutzerklärung jederzeit abrufen und seiner Einwilligung zur Verarbeitung von personenbezogenen Daten jederzeit widersprechen können.
- Nach [§ 13 Abs. 8 TMG](#) besteht die Pflicht zur Auskunfterteilung bei Anfragen zur Person oder zum Pseudonym.

### **Reichweitenmessung / Webstatistik / Speicherung von IP-Adressen**

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzerinnen und

<sup>9</sup> Ein Wert, der einem Ereignis einen eindeutigen Zeitpunkt zuordnet.

Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin<sup>10</sup>, dass bei Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des TMG zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden<sup>11</sup>. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes. Auch durch das sogenannte Browser Fingerprinting ist eine Profilbildung möglich. Denn neben der Browser-Art und -Version werden u. a. auch Angaben über installierte Plugins und alle auf dem Rechner installierten Schriftarten weitergegeben<sup>12</sup>.

Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:

- Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen<sup>13</sup>.
- Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden<sup>14</sup>. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.
- Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen<sup>15</sup>.
- Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.
- Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, informierter und eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist (Löschung des letzten Oktetts).

Werden pseudonyme Nutzungsprofile durch einen Auftragnehmer erstellt, sind darüber hinaus die Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung durch die Anbieter einzuhalten<sup>16</sup>.

Eine gezielte Aktivierung der Protokollierung ist zulässig, wenn sie im Einzelfall erforderlich ist, um die Funktionsfähigkeit der Webseite wiederherzustellen (z.B. bei einem DDoS-Angriff<sup>17</sup>). Nach Wiederherstellung der Funktionsfähigkeit müssen diese Daten aber umgehend gelöscht werden und sind zu keinem anderen Zweck weiterzuverwenden.

## Newsletter

Werbung über E-Mail ist ohne vorliegende Einwilligung nur erlaubt, wenn:

- ein Kundenverhältnis besteht **und**
- die E-Mail-Adresse im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistungen erhoben wurde **und**

---

<sup>10</sup> [Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 26./27. November 2009 in Stralsund](#)

<sup>11</sup> [§ 15 Nr. 3 Satz 1](#)

<sup>12</sup> Auf der Seite <http://panoptickick.eff.org> kann man testen, welche Informationen der eigene Browser beim Fingerprinting weitergibt.

<sup>13</sup> [§ 15 Nr. 3 Satz 2](#)

<sup>14</sup> [§ 15 Nr. 3 Satz 3](#)

<sup>15</sup> [§ 15 Nr. 3 Satz 2](#)

<sup>16</sup> [§ 11 BDSG](#)

<sup>17</sup> [Distributed Denial of Service](#)

- nur Werbung für eigene ähnliche Produkte und Dienstleistungen erfolgt **und**
- der Kunde der Verwendung für Werbezwecke nicht widersprochen hat **und**
- bei Erhebung der E-Mail-Adresse sowie in jeder Werbenachricht deutlich auf die Möglichkeit des jederzeitigen Widerspruchs hingewiesen wird.

Von allen Empfängern, die mit einem E-Mail-Newsletter angeschrieben werden, muss ein ausdrückliches Einverständnis vorliegen. Ansonsten ist die E-Mail Spam und sie stellt nach [§ 7 Abs. 2 Nr. 3 Gesetz gegen den unlauteren Wettbewerb \(UWG\)](#) eine unzumutbare Belästigung dar. Die ausdrückliche Einwilligung kann schriftlich, telefonisch oder per Online-Formular eingeholt werden. Wie und wann die Einwilligung erhalten wurde, sollte immer protokolliert werden.

Für die Online-Anmeldung an einen Newsletterdienst gibt es mehrere Anmeldeverfahren, die sich in der Praxis durchgesetzt haben. Allerdings entsprechen nur zwei dieser Verfahren den Anforderungen des [§ 13 Abs. 2 TMG](#), nämlich Double-Opt-In und Confirmed Opt-In.

Beim Double-Opt-In-Verfahren füllt der Abonnent ein Online-Anmeldeformular aus. Anschließend erhält er eine Willkommensnachricht, in der sich ein Link befindet. Erst wenn der Abonnent diesen Link anklickt, ist die Anmeldung abgeschlossen. Vorteil dieses Verfahrens ist, dass ein Missbrauch (z. B. eine Anmeldung in fremdem Namen) so gut wie ausgeschlossen ist.

Beim Confirmed-Opt-In-Verfahren ist die Registrierung bereits mit dem Ausfüllen des Online-Anmeldeformulars abgeschlossen. Der Abonnent erhält eine Registrierungsbestätigung; in dieser Mail befindet sich eine Abmeldemöglichkeit, mit der er seine Anmeldung widerrufen kann. Dieses Verfahren protokolliert die Anmeldung (wie in [§ 13 Abs. 2 TMG](#) vorgesehen), es ist aber nicht so missbrauchssicher wie die Double-Opt-In-Variante. Der Bundesgerichtshof hat in einem Urteil<sup>18</sup> die Anforderungen an Double-Opt-In spezifiziert.

Für alle Zusatzdienste – also z.B. weitere E-Mail-Werbung aus einem Unternehmen oder im Auftrag von Drittunternehmen – muss der Empfänger explizit seine Einwilligung erteilen. Wegen des Koppelungsverbots ([§ 12 Abs. 3 TMG](#)) ist es wichtig, dass der Abonnent solche Zusatzdienste auch ablehnen kann.

Der Abonnent muss den Newsletterdienst jederzeit wieder abbestellen können (Widerrufsrecht nach [§ 13 Abs. 4 Nr. 1 TMG](#)). Jeder Newsletter muss einen Abmeldelink enthalten.

Der Landesbeauftragte für den Datenschutz Niedersachsen

Prinzenstraße 5

30159 Hannover

Telefon 0511 120-4500

Fax 0511 120-4599

Ihre Ansprechpartner:

E-Mail an [poststelle@fd.niedersachsen.de](mailto:poststelle@fd.niedersachsen.de) schreiben

Stand: 16.02.2016

---

<sup>18</sup> BGH, 10.02.2011 - I ZR 164/09