



Grundlagen der Web-Entwicklung

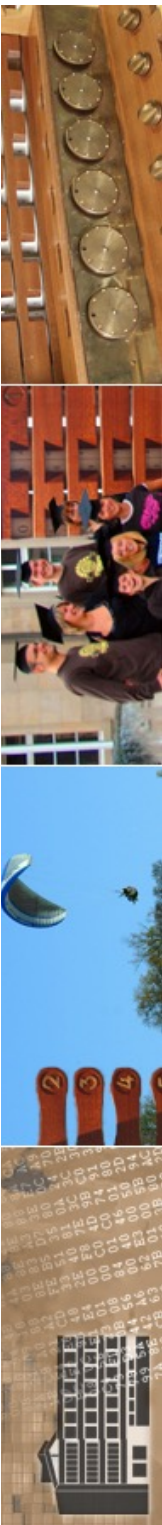
INF3172

Rechtliche Aspekte „rund um
das Web“

Thomas Walter

25.01.2024

Version 1.0

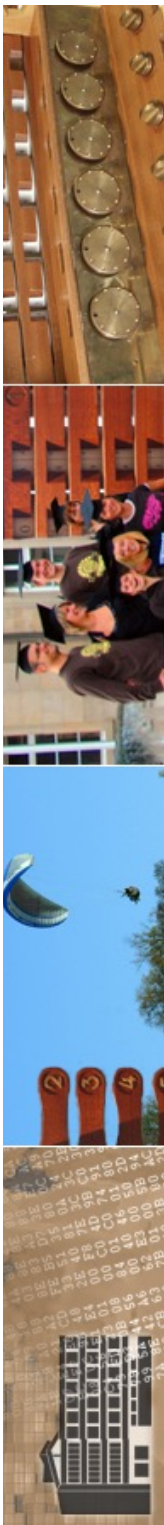




akuelles

- Klausur

**Donnerstag, den 08. Februar 2024 ab
08.00h (st) auf der Morgenstelle**





Inhalt

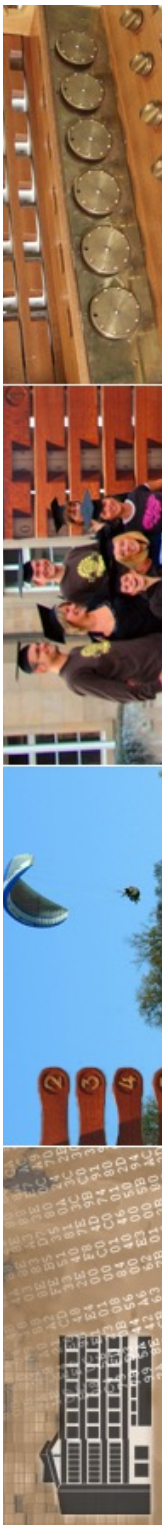
- Teledienste und Mediendienste
- Rechtliche Anforderungen Teledienste/Mediendienste
- TKG: Telekommunikationsgesetze
- Bundesdatenschutzgesetz BDSG und Landesdatenschutzgesetz LDSG
- **EU-Datenschutzgrundverordnung (EU-DSGVO)**
- Landespersonalvertretungsgesetz LPVG
- Urheberrecht UrhG





Quellen

- wie immer (sehr) zahlreiche Quellen im Netz
- Literatur
 - Martin Geppert/Ernst-Olav Ruhle/Fabian Schuster:
Handbuch Recht und Praxis der Telekommunikation
 - Bert Eichhorn: Internet-Recht
 - **Gesetzestexte** (frei, online)
 - auf Aktualität achten
- Informationsseiten der Landesdatenschutzbeauftragten
- spezielle Foren, auch DFN





Vorbemerkung

- diese Vorlesung soll Ihnen eine Übersicht über den Themenbereich geben
- die hier zusammengestellten Informationen entsprechen dem Wissensstand des Dozenten, sind für Sie aber nur Anhaltspunkte; Sie können sich nicht auf die Information berufen, sondern müssen ggf. genauere Informationen zu Rate ziehen.





Vorbemerkungen

- *welche Gesetze sind denn überhaupt relevant?*
 - EU-DSGVO (06.04.2016)
 - Bundesdatenschutzgesetz (BDSG, 27.04.2017/12.05.2017)
 - Landesdatenschutzgesetz Baden-Württemberg (LDSG, 18.11.2008/21.06.2018)
 - **Telemediengesetz (TMG, 31.5.2010)**
 - Teledienstegesetz (TDG, 10.11.2006)
 - Teledienstedatenschutzgesetz (TDDSG, 26.2.2007)
 - Mediendienste-Staatsvertrag (MDStV, außer Kraft)
 - **Telekommunikationsgesetz (TKG, 22.12..2011)**
 - Personalvertretungsgesetz BW (PersVG/LPVG, 11.10.2005)
 - Urheberrecht (UrhG, 17.12.2008)
 - ...und darüber zahlreiche weitere Gesetze





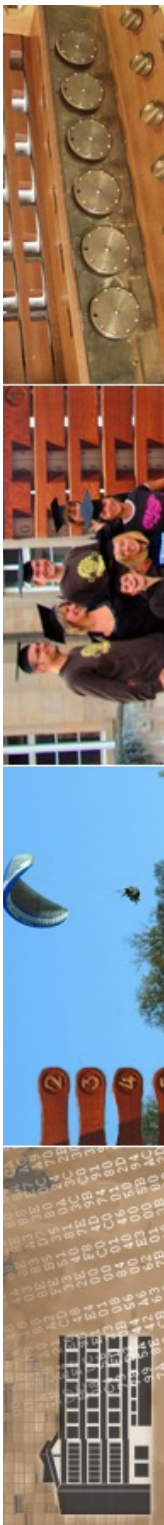
konkret

- TKG

- regelt Wettbewerb im Bereich der Telekommunikation, wesentlich verändert in Folge 9-11 in Erweiterungen (Vorratsdatenspeicherung, Kinderpornographie)

- TMG/TDG/TDDSG/Mediendienstestaatsvertrag

- Ziel: einheitliche wirtschaftliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste, Schutz personenbezogener Daten bei Telediensten





konkret

- **BDSG/LDSG**

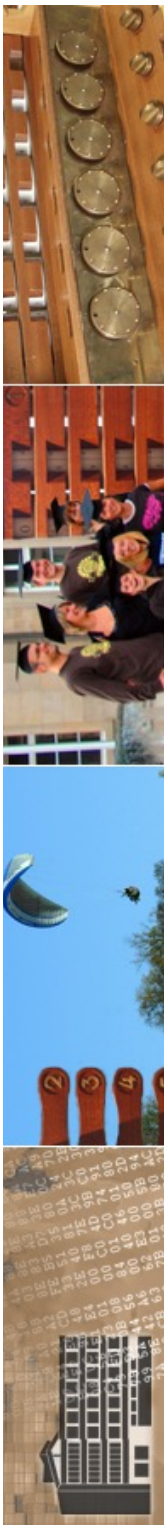
- Ziel: den einzelnen zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seiner Persönlichkeit nicht beeinträchtigt wird: Selbstbestimmung und das Recht an den eigenen Daten

- **EU-DSGV**

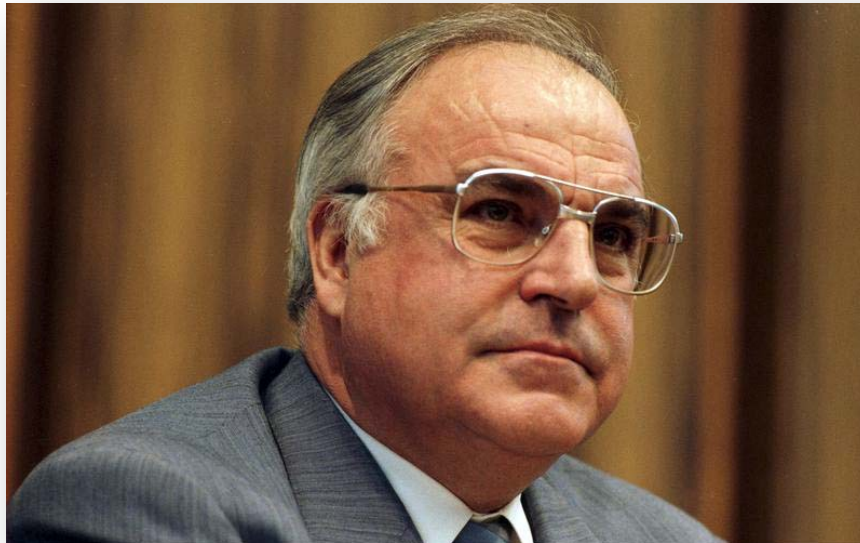
- Ziel: Vereinheitlichen der Verarbeitung personenbezogener Daten in der EU

- **PersVG**

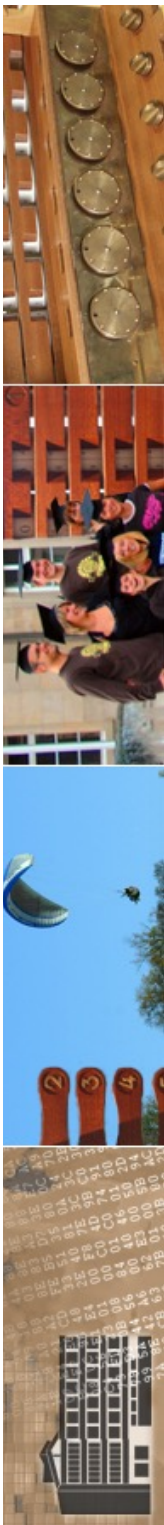
- Mitsprache/Zustimmungspflicht der Personalräte



Auslöser



- „Volkszählung“ 1987
 - Recht auf informelle Selbstbestimmung
- die "Datenautobahn" führte zu einer zentralen Gesetzesinitiative auf Bundesebene ab ~ 1997





ZENDAS: www.zendas.de



ZENDAS

Zentrale Datenschutzstelle der
baden-württembergischen Universitäten

[Home](#) [Sitemap](#) [Kontakt](#) [Datenschutzerklärung](#) [Impressum](#) [Suche](#)

[Druckversion: [HTML](#)]

- ▶ [Wir über uns](#)
- ▶ [Recht](#)
- ▶ [Themen](#)
- ▶ [Stichworte A-Z](#)
- ▶ [Service](#)
- ▶ [Anfragetool](#)
- ▶ [Schulungen/ Veranstaltungen](#)
- ▶ [Links](#)
- ▶ [Login](#)

Suche:

[Erweiterte Suche](#) ▶

Benutzer:

Universität Tübingen

Bundesland:

Baden-Württemberg

Netzwerk:

IPv4

[Nutzungsbedingungen](#) ▶

ZENDAS Newsletter 01/2021 verfügbar

▶▶ Unser Newsletter 01/2021 ist
seit dem 28.01.2021
verfügbar.

[Mehr Infos](#) ▶▶



Herzlich Willkommen

Die Zentrale Datenschutzstelle der baden-württembergischen Universitäten bietet Ihnen Informationen rund um das Thema "Datenschutz in der Hochschule" und unterstützt die Universitäten des Landes Baden-Württemberg und ihre Vertragspartner in allen rechtlichen und technisch-organisatorischen Fragestellungen des Datenschutzes.



Coronavirus und Datenschutz

Vielleicht sind Grundrechte nie so wichtig wie in Krisen. Auch das Coronavirus sollte nicht dazu führen, dass der Datenschutz gar keine Berücksichtigung mehr findet. Finden Sie auf unserer neuen Webseite ein paar Links zu weiterführenden Informationen... [mehr...](#) ➡

Videokonferenzen

In Zeiten wie diesen gefragt wie nie: Videokonferenzsysteme. Doch nicht nur der schnelle, unkomplizierte Einsatz ist wichtig. Mit den datenschutzrechtlichen Belangen, die bei der Nutzung von Videokonferenzsystemen auch Beachtung finden müssen, beschäftigt sich unsere neue Webseite: [mehr...](#) ➡

Brexit: Datenschutzrechtliche Regelung?

Wer hätte es noch gedacht? Ganz ungeregelt geht der Brexit nun doch nicht über die Bühne. In letzter Minute wurde ein Handels- und Zusammenarbeitsabkommen zwischen dem Vereinigten Königreich und der Europäischen Union geschnürt. [mehr...](#) ➡


Copyright 2020 by ZENDAS





LfdI Baden-Württemberg

[Startseite](#) [Datenschutz](#) [Impressum](#) [Inhalt](#)

Suche 



Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

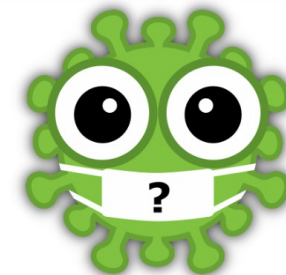
[Über uns](#) [Datenschutz](#) [Informationsfreiheit](#) [Infothek](#) [KULTur](#) [Bildungszentrum](#) [Kontakt](#) [Service](#)



P
A
N
D
A
T
E
N
S
C
H
U
T
Z
E
M
I
F

Tätigkeitsbericht Datenschutz 2020
8. Februar 2021

++ FAQ CORONA ++



KONTAKT

Telefon

0711 / 61 55 41 – 0
Montag bis Donnerstag von 10 bis 12
Uhr.

E-Mail

poststelle@lfdi.bwl.de

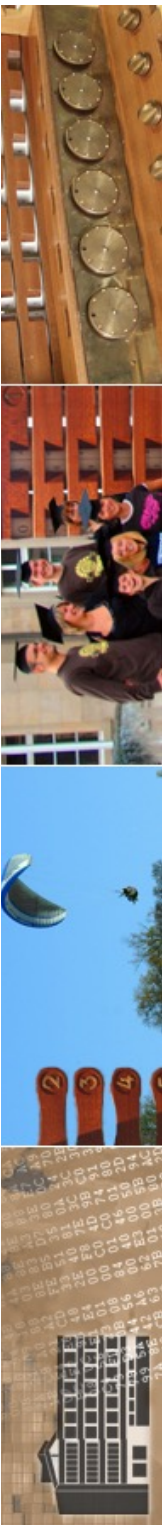
DE-Mail

poststelle@lfdi.bwl.de-mail.de



Zuständigkeit

- in diesem Bereich
 - Gesetzgebung des Bundes
 - Gesetzgebung der Länder (LDSG, PerVG, LHG)
 - Regulierung durch die EU
- teilweise komplexe Situation und uneinheitliche/widersprüchliche Urteile der Gerichte/Instanzen
- Länder hatten bis 2007 MDStV, danach Staatsvertrag für Rundfunk und Telemedien (RStV) und **TMG**





Tele- und Mediendienste

- seit 1997 gibt es in der Bundesrepublik zahlreiche gesetzliche Regelungen für das »Internet«
- Teledienste:
 - Bundesgesetze
 - elektronische Informations- und Kommunikationsdienste *für eine individuelle Nutzung*
 - Bsp: Homebanking
- Mediendienste:
 - Landesgesetze
 - elektronische Verteildienste und solche, bei denen die *redaktionelle Gestaltung zur Meinungsbildung im Vordergrund steht*
 - Bsp: Tageszeitung im Web





Rechtsgrundlagen

- **Telemediengesetz (ab 1.3.2007)**

Ablösung für:

- Mediendienstestaatsvertrag (MDStV), § 2
- Teledienstegesetz (TDG), § 2
- Teledienstedatenschutzgesetz (TDDSG), §§ 1,2





Rechtliche Anforderungen an Tele- und Mediendienste

- Anbieterkennzeichnung ("Impressums-Pflicht")
 - für den Nutzer muss erkennbar sein, mit welchen natürlichen und juristischen Personen er es auf Seite des Diensteanbieters zu tun hat
 - §5 TMG
 - Realisierung
 - Impressum auf jeder Webseite, Link auf Impressum
 - Unzureichend:
 - Nennung des Verantwortlichen ohne Anschrift
 - Nennung eines Firmennamens ohne Benennung eines Vertretungsberechtigten mit Anschrift
 - keine Nennung des Hosting-Service, soweit dieser bei der Abwicklung eines Angebotes in eigener Verantwortung personenbezogene Daten speichert



Impressum

Bitte beachten Sie: Dieses Impressum gilt auch für die offiziellen Social Media-Auftritte der Universität

Tübingen auf Facebook (<https://www.facebook.com/unituebingen>,

<https://www.facebook.com/University.of.Tuebingen>), Twitter (https://twitter.com/uni_tue), Instagram

(<https://www.instagram.com/universitaet.tuebingen/>) und YouTube

(<http://www.youtube.com/UniTuebingen>).

Allgemeine Informationen gem. § 5 TMG, § 55 RStVG

Adresse:	Eberhard Karls Universität Tübingen Geschwister-Scholl-Platz 72074 Tübingen
----------	---

Die Universität Tübingen ist eine Körperschaft des öffentlichen Rechts. Sie wird durch den Rektor Prof. Dr. Bernd Engler (E-Mail: bernd. engler [at] uni-tuebingen.de) gesetzlich vertreten

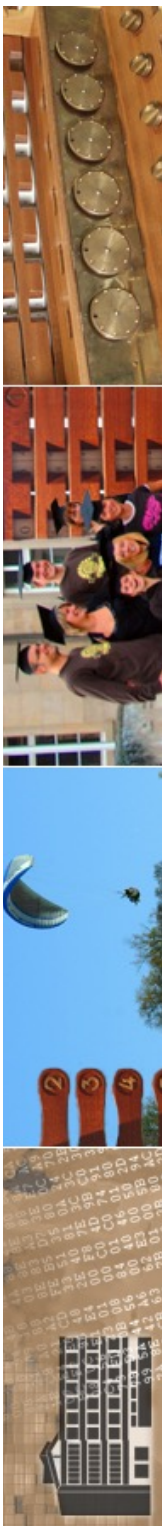
Telefonzentrale:	++49 (0) 70 71/29-0
------------------	---------------------

Fax Zentrale	++49 (0) 70 71/29-59 90
Verwaltung:	

Zentrale E-Mail-Adresse:	info [at] uni-tuebingen.de
--------------------------	----------------------------

Internet-Adresse:	http://www.uni-tuebingen.de
-------------------	---

Umsatzsteuer-Identifikationsnummer:	gemäß § 27a Umsatzsteuergesetz: DE812383453
-------------------------------------	---



1. Externe Links

Diese Webseite der Universität Tübingen enthält auch entsprechend gekennzeichnete Links [↗](#) oder Verweise auf Websites Dritter. Durch den Link vermittelt die Universität Tübingen lediglich den Zugang zur Nutzung dieser Inhalte. Eine Zustimmung zu den Inhalten den verlinkten Seiten Dritter ist damit nicht verbunden. Die Universität Tübingen übernimmt daher keine Verantwortung für die Verfügbarkeit oder den Inhalt solcher Websites und keine Haftung für Schäden oder Verletzungen, die aus der Nutzung – gleich welcher Art – solcher Inhalte entstehen. Hierfür haftet allein der Anbieter der jeweiligen Seite.

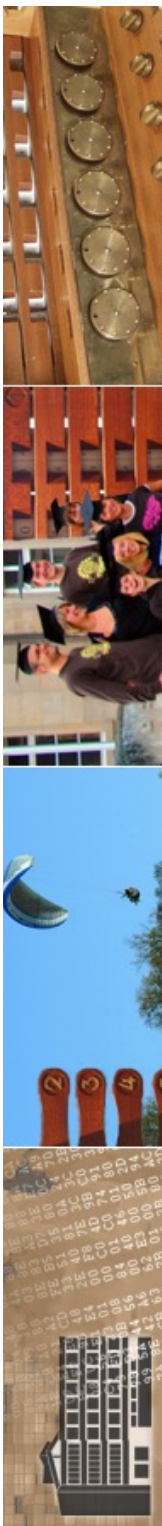
Bei der erstmaligen Verknüpfung mit einem anderen Internetangebot hat die Redaktion dessen Inhalt daraufhin überprüft, ob durch ihn eine mögliche zivilrechtliche oder strafrechtliche Verantwortlichkeit ausgelöst wird. Dort nachträglich eingebundene Inhalte können jedoch leider nicht überprüft werden. Der Verweis auf dieses Angebot wird unverzüglich aufgehoben werden, sobald die Redaktion feststellt oder von anderen darauf hingewiesen wird, dass ein bestimmtes Angebot, zu dem ein Link bereitgestellt wurde, eine zivil- oder strafrechtliche Verantwortlichkeit auslöst.

2. Urheberrecht

Copyright (c), Universität Tübingen. Alle Rechte vorbehalten.

Alle auf dieser Website veröffentlichten Inhalte (Layout, Texte, Bilder, Grafiken, Video- und Tondateien usw.) unterliegen dem Urheberrecht. Jede vom Urheberrechtsgesetz nicht zugelassene Verwertung bedarf vorheriger ausdrücklicher Zustimmung der Universität Tübingen. Dies gilt insbesondere für Vervielfältigung, Bearbeitung, Übersetzung, Einspeicherung, Verarbeitung bzw. Wiedergabe von Inhalten in Datenbanken oder anderen elektronischen Medien und Systemen. Fotokopien und Downloads von Web-Seiten für den privaten, wissenschaftlichen und nicht kommerziellen Gebrauch dürfen hergestellt werden.

Das Urheberrecht für die Wort-Bild-Marke liegt ausdrücklich bei der Universität Tübingen.





3. Haftungsausschluss

Die Informationen auf dieser Website wurden nach bestem Wissen und Gewissen sorgfältig zusammengestellt und geprüft. Es wird jedoch keine Gewähr – weder ausdrücklich noch stillschweigend – für die Vollständigkeit, Richtigkeit oder Aktualität sowie die jederzeitige Verfügbarkeit der bereit gestellten Informationen übernommen. Eine Haftung für Schäden, die aus der Nutzung oder Nichtnutzung der auf dieser Website angebotenen Informationen entstehen ist – soweit gesetzlich zulässig – ausgeschlossen.

Stabsstelle Hochschulkommunikation

Dr. Karl Guido Rijkhoek

Wilhelmstr. 5

72074 Tübingen

E-Mail  ord@uni-tuebingen

Telefon +49 7071 29-77854





[Impressum](#)

[Datenschutzerklärung](#)

[Barrierefreiheit](#)

Datenschutzerklärung der Eberhard Karls Universität Tübingen

Sehr geehrte Webseitenbesucherinnen und Webseitenbesucher,

vielen Dank für den Besuch unserer Webseiten! Wir schätzen Ihr Interesse an der Universität Tübingen und unseren Informationen zu Studium und Forschung.

Mittels dieser Datenschutzerklärung möchten wir Sie im Folgenden über die Datenverarbeitung Ihrer personenbezogenen Daten (im Folgenden „Daten“) informieren, die aus dem Besuch oder der Nutzung von Funktionen unserer Webseiten resultieren.

Wir bitten Sie, diese Datenschutzerklärung sorgfältig durchzulesen, bevor Sie unsere Webseiten weiter besuchen oder die auf den Webseiten enthaltenen Funktionen nutzen.

Mit dem Besuch unserer Webseiten stimmen Sie den im Folgenden beschriebenen Verarbeitungen und Nutzungen Ihrer Daten zu.

Unsere Datenschutzerklärung ist nur für unsere Webseiten gültig und nicht für die Webseiten Dritter.

Datenschutz und Datensicherheit

Der Schutz Ihrer Privatsphäre ist uns ein wichtiges Anliegen. Zum Schutz Ihrer Daten trifft die Universität Tübingen eine Vielzahl an technischen und organisatorischen Maßnahmen, um eine unbefugte Kenntnisnahme und Weitergabe, Manipulation, Verlust und unbefugte Löschung wirksam verhindern zu können.





LG Hamburg - mit Willkür zur Verlinkungs-Angst

12. Dezember 2016 – Daniel Hermsdorf

Das Landgericht Hamburg bestärkt fragwürdige urheberrechtliche Kriterien für Hyperlinks im Internet

Es ist ein bizarres Beispiel von Weltferne, unpraktischem Verständnis und Verlust bestehender juristischer Kriterien: Das Landgericht Hamburg hat erstinstanzlich Links auf widerrechtlich hochgeladene Inhalte im Internet unter Strafe gestellt. Der konkrete Fall betrifft eine Fotomontage, in der der Urheber eines bildlichen Bestandteils mit Creative-Commons-Lizenz nicht angegeben war.

Das Gravierendste für die Informationsfreiheit dürfte sein: Nun ist dieser Spuk erst einmal in der Welt. Juristische Sanktionen sind angstausslösend. Wer die Rechtslage nicht genau einschätzen kann und/oder den falschen Verhältnissen trotzen will, wird auf Verlinkung nun wohl öfter einfach verzichten.

INHALT

1. LG Hamburg - mit Willkür zur Verlinkungs-Angst


2. Ein weiteres Detail der (Un-)Verhältnismäßigkeit





Warum heise online derzeit keine Links zum LG Hamburg setzt

UPDATE

 heise online 09.12.2016 13:57 Uhr - Holger Bleich

 vorlesen

Nach dem Linkhaftungsurteil des Landgerichts Hamburg: Verlagsjustiziar Joerg Heidrich hat für heise online nachgeforscht, ob sich der Verlag in Abmahngefahr begibt, wenn er Links zum Online-Auftritt des LG Hamburg setzt.

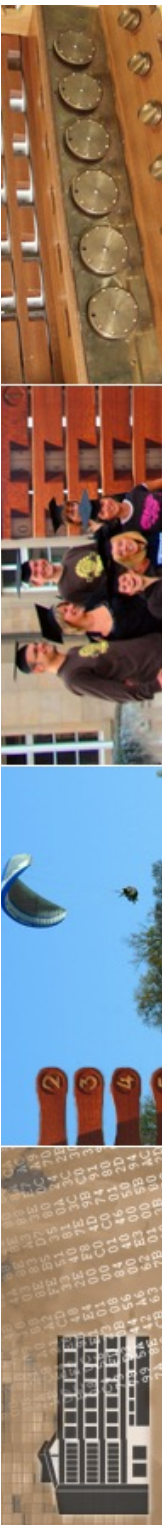
Laut einer [Entscheidung des Landgerichts \(LG\) Hamburg](#) haftet der Betreiber einer gewerblich betriebenen Website auch ohne Kenntnis für urheberrechtsverletzende Inhalte, die er verlinkt. Dem Linksetzenden obliege die Pflicht einer "zumutbaren Nachforschung zur Frage der Rechtmäßigkeit der Zugänglichmachung".

Diese Rechtsprechung trifft auch redaktionelle Angebote wie heise online. Der Verlagsjustiziar der Heise Medien GmbH & Co. KG hat deshalb am gestrigen Donnerstag Abend begonnen nachzuforschen, ob sich heise online in Abmahngefahr begibt, wenn es Links zum Online-Auftritt des LG Hamburg setzt. Weil die Nachforschung bisher ohne Ergebnis blieb, muss heise online bis auf weiteres darauf verzichten, Links zum LG Hamburg zu setzen.



Impressum

- Vorlagen/Generatoren für ein Impressum u.a. unter:
 - <http://www.e-recht24.de/impressum-generator.html>





teilen

354



mitteilen



tweet



teilen

★★★★☆ (3764 Bewertungen, 4.40 von 5)

Erstellen Sie kostenlos ein Impressum für Ihre Website

Haben Sie bereits Ihre Websites DSGVO-konform angepasst?

Egal, ob Unternehmer, Webdesigner oder Agentur. Erstellen Sie schnell und einfach **DSGVO-konforme Datenschutzerklärungen** mit dem **eRecht24 Premium Datenschutzgenerator** und sichern Sie sich und Ihre Kunden gegen Abmahnungen ab.

JETZT DSGVO-KONFORME DATENSCHUTZERKLÄRUNG ERZEUGEN

Support

Ihre Vorteile:

- ✓ In 3 Minuten zum rechtssicheren Impressum
- ✓ Für alle Websites und Unternehmensformen geeignet
- ✓ kostenlos und anonym

Über 1 Million Nutzer seit 2012:

- 😊 "Sehr praktisch! Ich nutze es immer wieder für die Websites meiner Kunden. Danke, für dieses tolle kostenlose Tool!"
- 😊 "Respekt! e-recht24.de weiss, was Webmaster brauchen."
- 😊 "Sehr übersichtlich, gute Lesbarkeit und ein ausgezeichneter Service. Danke dafür!"



Bildschirmfoto





Datenschutzerklärung



Stand: 24.05.2018

Verantwortlich im datenschutzrechtlichen Sinne

Zugriff: Die ganze Welt

Universität Stuttgart
Keplerstraße 7
70174 Stuttgart
Deutschland

Telefon: +49 711 685 0
E-Mail: poststelle@uni-stuttgart.de

Datenschutzbeauftragter

Zugriff: Die ganze Welt

Datenschutzbeauftragter der Universität Stuttgart
Breitscheidstraße 2
70174 Stuttgart
Deutschland

Telefon: +49 711 685 83687
E-Mail: datenschutz@uni-stuttgart.de

Allgemeines zur Datenverarbeitung

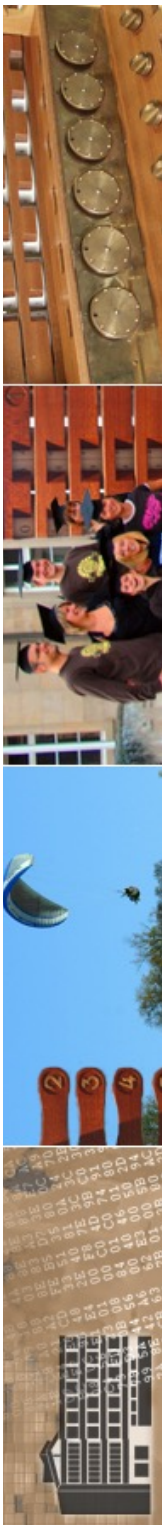
Zugriff: Die ganze Welt

Beim Zugriff auf eine Seite aus dem Web-Angebot von ZENDAS und beim Abruf einer Datei werden von unserem Webserver keine personenbezogenen Daten protokolliert, insbesondere werden IP-Adressen unmittelbar nach deren Erfassen verkürzt gespeichert. Konkrete Informationen zu diesem Verfahren finden Sie [hier](#) ➡

Nicht ausgeschlossen werden kann, dass eine Protokollierung an den aktiven Komponenten durch andere Stellen innerhalb der Universität Stuttgart erfolgt und durch eine Zusammenführung der bei ZENDAS und diesen Stellen vorhandenen Protokollierungen ein Personenbezug hergestellt werden könnte. Informationen zur Datenverarbeitung finden Sie sogleich auf dieser Seite unter der Überschrift „Datenerhebung beim Aufruf von Webseiten aus dem ZENDAS-Angebot“.

Soweit bei einzelnen Funktionen auf unseren Seiten (wie z.B. Newsletteranmeldung) personenbezogene Daten erhoben werden, erfolgt die Angabe dieser Daten ausdrücklich freiwillig oder die Erhebung erfolgt auf Grundlage einer Rechtsvorschrift, die dies erlaubt. Über die Erhebung und weitere Verwendung Ihrer Daten werden Sie an der entsprechenden Stelle informiert.

Informationen zur Ihren Rechten finden Sie am Ende dieser Webseite unter der Überschrift „Ihre Rechte“.





Zweck, Kategorien von Daten und berechtigte Interessen

1. An den aktiven Netzwerk-Komponenten der Universität Stuttgart werden auch beim Aufruf von Webseiten Datum und Zeitstempel , IP-Adresse + Port (Quelle), IP-Adresse + Port (Ziel), Anzahl der Datenpakete (TCP) sowie die Menge der übertragenen Daten je Verkehrsbeziehung (Aufruf) protokolliert (NetFlows). Die Daten werden dort nur vorübergehend und zugriffsgeschützt auf einem Sicherheitssystem gespeichert . Dies geschieht zum Zweck Störungen und Angriffe zu erkennen und zu beheben bzw. abzuwehren.
2. Um die Qualität unserer Webseiten zu verbessern, protokolliert unser Webserver zu statistischen Zwecken bei jedem Aufruf unserer Webseiten Datum, Uhrzeit, auf die ersten beiden Bytes reduzierte IPv4-Adresse oder auf die ersten 32 Bit gekürzte IPv6-Adresse, aktuell abgerufenes Dokument, vorheriges abgerufenes Dokument (ohne Request-Parameter - Ausnahme: Es erfolgt die Speicherung des Request-Parameters "q", der die Suchbegriffe von Google gespeichert hat), Größe der Datei (in Bytes), HTTP Status Code, bei Zugriffen aus IP-Bereichen der Kooperationspartner und Abokunden von ZENDAS außerdem: Hochschule und berechtigte Zugriffsebene. Da die IP- Adresse unmittelbar nach deren Erfassen verkürzt gespeichert wird, lässt sich für uns allein aus diesen Daten kein Personenbezug herstellen. Es ist selbstverständlich, dass eine Zusammenführung dieser Daten mit den unter 1. genannten Daten während deren kurzfristigen Speicherung nicht stattfindet, es sei denn, es liegen tatsächliche Anhaltspunkte für eine Störung des ordnungsgemäßen Betriebs oder für eine missbräuchliche Nutzung vor. Die Daten werden nur anonymisiert (durch die Kürzung der IP-Adresse und nach Löschung der unter 1 genannten Daten) ausgewertet.
3. Grundsätzlich wird beim Besuch der ZENDAS-Webseiten kein Cookie gesetzt. Eine Ausnahme bildet u.a. ein Zugriff aus IP-Bereichen unserer Info-Server Abonnenten und Kooperationspartner. Hier wird beim ersten Zugriff ein SESSION-Cookie gesetzt. In diesem wird eine eindeutige ID gespeichert. Auf dem Server werden zusammen mit dieser ID verschiedene Informationen verknüpft. Diese sind abhängig von der Art des Zugangs und von der konkreten Nutzung der Webseite. Der Umfang dieser Informationen umfasst maximal „Login“, „Hochschule“, „Bundesland“, „Rolle“, „Gruppe“, „Letzte besuchte Seite“, „Letztes Suchwort“. Diese Informationen werden ausschließlich für die an den jeweiligen Info-Server Abonnenten oder Kooperationspartnern angepasste Anzeige der Webseiten verarbeitet.
Auch beim Einloggen mit Username/Passwort wird ein Cookie gesetzt (konkrete Informationen zu diesem Cookie finden Sie auf der Login-Seite).

In den genannten Zwecken liegt auch unser berechtigtes Interesse an der Datenverarbeitung nach Art. 6 Abs. 1 lit. f Datenschutzgrund-Verordnung (DS-GVO).

Rechtsgrundlage

Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DS-GVO.

Empfänger

Sofern wegen Angriffs auf die informationstechnischen Systeme der Universität Stuttgart Ermittlungsmaßnahmen eingeleitet werden, können die unter 1. genannten Daten an staatliche Ermittlungsorgane weitergegeben werden. Dasselbe gilt, wenn entsprechende Behörden oder Gerichte Anfragen an die Universität richten und die Universität dazu verpflichtet ist, diesen Folge zu leisten.



Dauer der Speicherung

1. Die an den aktiven Netzwerk-Komponenten der Universität Stuttgart protokollierten Daten werden nach 7 Tagen gelöscht.
2. Der Session-Cookie wird beim Schließen Ihres Browsers automatisch von Ihrem Rechner gelöscht. Die auf dem Webserver gespeicherten Daten werden automatisch nach 2 Stunden Inaktivität gelöscht.

Folgen der Nichtangabe, Widerspruchs- bzw. Beseitigungsmöglichkeit

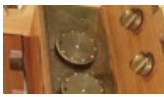
Die Erfassung der Daten zur Bereitstellung der Website und die Speicherung der Daten in Logfiles ist für den Betrieb der Internetseite zwingend erforderlich. Nutzer, die nicht möchten, dass ihre Daten wie beschrieben verarbeitet werden, können die Webseiten von ZENDAS nicht nutzen.

Cookies werden auf dem Rechner des Nutzers gespeichert und von diesem an unsere Seite übermittelt. Daher haben Sie als Nutzer – unabhängig von den vorstehend aufgeführten Speicherfristen- auch die volle Kontrolle über die Verwendung von Cookies. Durch eine Änderung der Einstellungen in Ihrem Internetbrowser können Sie die Übertragung von Cookies deaktivieren oder einschränken. Bereits gespeicherte Cookies können jederzeit gelöscht werden. Dies kann auch automatisiert erfolgen. Werden Cookies für unsere Website deaktiviert, können möglicherweise nicht mehr alle Funktionen der Website vollumfänglich genutzt werden.

Ihre Rechte

Zugriff: Die ganze Welt

- ▶▶ Sie haben das Recht, von der Universität Stuttgart Auskunft über die zu Ihrer Person gespeicherten Daten zu erhalten und/oder unrichtig gespeicherte Daten berichtigen zu lassen.
- ▶▶ Sie haben darüber hinaus das Recht auf Löschung oder auf Einschränkung der Verarbeitung oder ein Widerspruchsrecht gegen die Verarbeitung.
- ▶▶ Außerdem haben Sie in dem Fall, in dem Sie uns eine Einwilligung zur Verarbeitung Ihrer personenbezogener Daten erteilt haben, das Recht, die Einwilligung jederzeit zu widerrufen, wobei die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt wird. Bitte wenden Sie sich dazu an ZENDAS <https://www.zendas.de/kontakt.html> ➡
- ▶▶ Sofern die Datenverarbeitung auf einer Einwilligung oder auf einem Vertrag beruht, weisen wir Sie an der entsprechenden Stelle darauf hin. Erfolg die Datenverarbeitung zudem mithilfe automatisierter Verfahren, steht Ihnen gegebenenfalls ein Recht auf Datenübertragbarkeit zu (Art. 20 DS-GVO).
- ▶▶ Sie haben das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten gegen die Rechtsvorschriften verstößt. Eine solche Aufsichtsbehörde ist beispielsweise der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.



Mitmachen ▾

Vorschlagen ▾

Informieren ▾



© dpa

▶ | ● ○ ○ ○ ○ ○ ○ ○ 1/6

KULTUR

Sanierung des Stuttgarter Opernhouses

Das Opernhaus in Stuttgart muss saniert und erweitert werden. Bis zum 16. Januar 2020 konnten Sie an der Online-Beteiligung teilnehmen. Vielen Dank für Ihre Kommentare!





Sie sind hier: »Startseite »Mitmachen »LP 16 »Anpassung Datenschutzgesetz

Neufassung des Landesdatenschutz- gesetzes



► [Zur aktuellen Phase](#)



DATENSCHUTZ

 [Text vorlesen](#)

Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679

KONTAKT



Ministerium für
Inneres,
Digitalisierung und

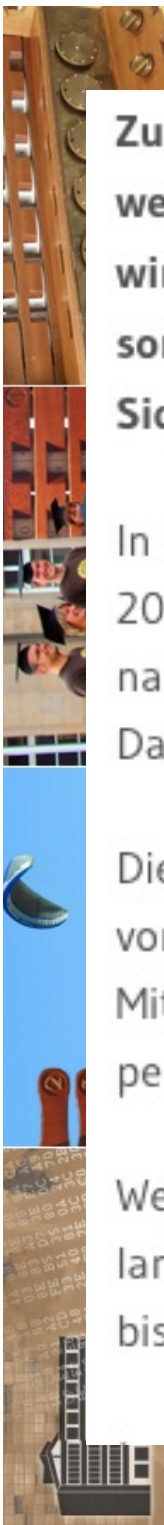


Zur Anpassung an europäisches Recht muss das Landesdatenschutzgesetz neu gefasst werden. Der Gesetzentwurf enthält ergänzende Regelungen zur EU-Verordnung. Hierbei wird das Recht auf informationelle Selbstbestimmung in Einklang gebracht mit den sonstigen grundrechtlich geschützten Freiheiten einerseits und den Anforderungen der Sicherheit und der Verwaltung andererseits.

In allen Mitgliedstaaten der Europäischen Union gilt ab dem 25. Mai 2018 die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Datenschutz-Grundverordnung unmittelbar.

Die Verordnung schafft damit ein verbindliches Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten in allen Mitgliedstaaten, das auch alle öffentlichen Stellen zu beachten haben, soweit sie personenbezogene Daten im Anwendungsbereich der Verordnung verarbeiten.

Wegen des Anwendungsvorrangs des europäischen Rechts ergibt sich die Notwendigkeit, die landesrechtlichen Datenschutzregelungen an die Verordnung (EU) 2016/679 anzupassen. Das bisherige Landesdatenschutzgesetz wird daher aufgehoben.



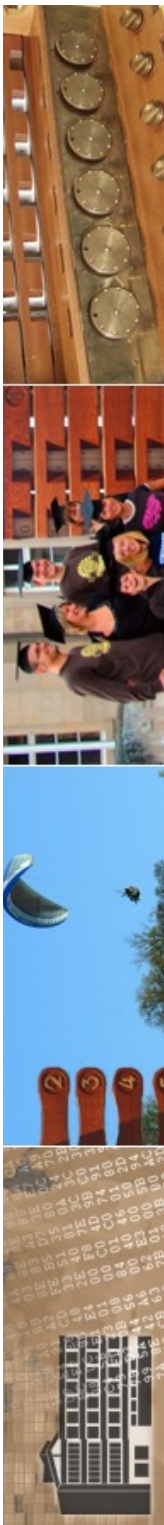


personenbezogene Daten

- Prinzip:

**Die Erhebung und Verarbeitung
personenbezogener Daten ist nicht zulässig**

- aber...



Personenbezogene Daten

- Grundsatz: Personenbezogene Daten dürfen von Diensteanbietern zur Durchführung von Telediensten nur erhoben, verarbeitet und genutzt werden, soweit dies eine Rechtsvorschrift erlaubt oder der Nutzer eingewilligt hat.

- §12 TMG
- § 4a Abs. 1 BDSG
- §4 Abs. 1 LDSG





28.10.2014 12:48

Speicherung von IP-Adressen: BGH hat Fragen an den EuGH

In einem Verfahren um die Speicherung der IP-Adressen von Besuchern einer Website schaltet der Bundesgerichtshof wie erwartet den Europäischen Gerichtshof ein. Der soll vor allem eine Frage klären: Sind IP-Adressen personenbezogene Daten?

Im Rechtsstreit um die Speicherung dynamischer IP-Adressen durch die Bundesregierung hat der Bundesgerichtshof (BGH) das Revisionsverfahren ausgesetzt und legt dem Europäischen Gerichtshof (EuGH) **wie erwartet [1]** zwei Fragen zur Auslegung der EG-Datenschutz-Richtlinie vor. So sollen die Brüsseler Richter unter anderem entscheiden, ob IP-Adressen "personenbezogene Daten" sind (Az. VI ZR 135/13).

Es geht um eine Klage des Kieler Piratenpolitikers Patrick Breyer gegen die Bundesrepublik Deutschland. Der Schleswig-Holsteinische Landtagsabgeordnete will dem Bund verbieten lassen, IP-Adressen von Besuchern von Websites des Bundes über die Dauer der Nutzung



EuGH korrigiert Urteil zum Datenschutz von IP-Adressen

12.01.2017 19:06 Uhr – Stefan Krempl

 vorlesen



(Bild: dpa, Thomas Frey)

Der Europäische Gerichtshof hat klargestellt, dass IP-Adressen personenbeziehbar und damit besonders geschützt sind, wenn etwa bei einem Cyberangriff Ermittler anhand der Logfiles Bestandsdaten vom Provider einholen können.



EuGH korrigiert Urteil zum Datenschutz von IP-Adressen

12.01.2017 19:06 Uhr - Stefan Krempl

Der Europäische Gerichtshof hat klargestellt, dass IP-Adressen personenbeziehbar und damit besonders geschützt sind, wenn etwa bei einem Cyberangriff Ermittler anhand der Logfiles Bestandsdaten vom Provider einholen können.

Das Urteil des Europäischen Gerichtshofs [1] (EuGH) im Fall des Datenschutzaktivisten und Piraten Patrick Breyer gegen die Bundesrepublik Deutschland hat vielfach zu der Annahme geführt, dass eine IP-Adresse nur personenbezogen und damit datenschutzrechtlich speziell geschützt sei, wenn der Anbieter eines Telemediendienstes wie einer Webseite den Inhaber der Internetkennung selbst identifizieren könne. Beobachter sahen den Datenschutz im Netz damit "in Trümmern" [2], da der Personenbezug nun etwa durch "geschickte Vertragsgestaltung" ausgeschlossen werden könnte.

Der Kläger hat auf Antrag [3] seines Anwalts Meinhard Starostik nun aber erreichen können, dass der EuGH das Urteil in der deutschen Sprachfassung in einem kleinen, aber entscheidenden Punkt wegen Schreib- beziehungsweise Übersetzungsfehlern **berichtigt hat** [4]. Die Luxemburger Richter stellen damit klar, dass es für den Personenbezug von IP-Adressen ausreicht, wenn sich der Anbieter von Online-Mediendiensten insbesondere bei Cyberattacken an die zuständige Ermittlungsbehörde wenden kann. Dieser obliege es dann, "die nötigen Schritte" zu unternehmen, "um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten".

Zuordnung nicht auszuschließen

Ordnungshüter können demnach in der Regel anhand zumindest kurzfristig verfügbarer Logfiles Name und Anschrift zu der Netzkennung hinter einem Angreifer beim Provider anfordern. Nur die Strafverfolger müssten also die IP-Adresse zuordnen können, nicht schon etwa der Betreiber einer Webseite selbst. Ob dem tatsächlich so ist, muss der Bundesgerichtshof (BGH) als die Instanz, die den Streit dem EuGH vorgelegt hat, nun nach wie vor selbst noch prüfen.

Breyer geht davon aus, dass die erwähnte Zuordnung zumindest hierzulande in Bezug auf deutsche Nutzer mithilfe einer **Bestandsdatenauskunft** [5] stets möglich beziehungsweise zumindest nicht auszuschließen sei. IP-Adressen unterlägen so praktisch "immer dem Datenschutz" und dürften nur bei "berechtigtem Interesse" gespeichert werden. "Gut so", kommentierte der Jurist die Korrektur gegenüber *heise online*, "denn das Recht auf informationelle Selbstbestimmung muss auch vor falschem Verdacht, unberechtigten Abmahnungen" sowie dem Klau, Verlust und Missbrauch von Daten schützen. Dies gehe nicht, wenn das Risiko von Rechtsverstößen völlig ausgeblendet werde.



LDSG §4 (1)

- ***§4 Zulässigkeit der Datenverarbeitung***
 - (1) Die Verarbeitung personenbezogener Daten ist nur zulässig,
 1. wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder
 2. soweit der Betroffene eingewilligt hat.
 - (...)





DSGVO Art. 6

Artikel 6

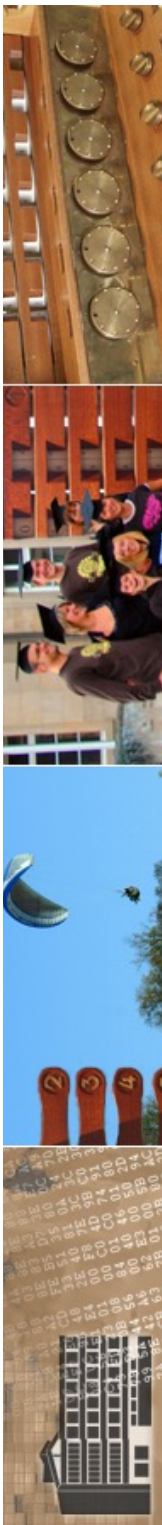
Rechtmäßigkeit der Verarbeitung

- (1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
- a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
 - b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
 - c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
 - d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
 - e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
 - f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.



Einwilligung

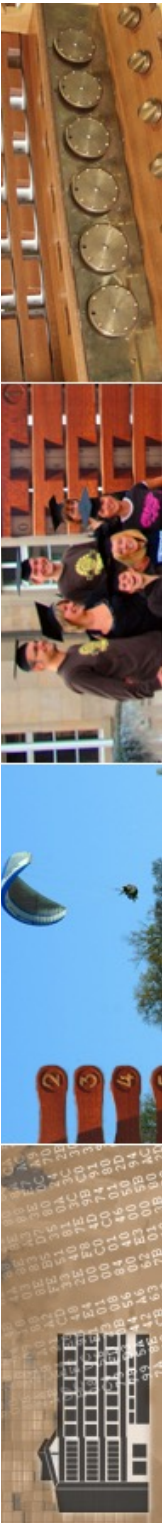
- mit Einwilligung des Nutzers ist zulässig:
 - Erhebung und Verarbeitung personenbezogener Bestandsdaten für Zwecke der Beratung, der Werbung, der Marktforschung
 - Teilnehmerverzeichnis
 - Erhebung Emailadresse für Zusendung von Newslettern
- Unzulässig:
 - obligatorische Erhebung von Daten, die für die Erbringung des Dienstes *nicht* erforderlich sind
 - pauschale Einwilligung in die Nutzung der erhobenen Daten für andere Zwecke in AGB oder Nutzungsbedingungen





Form der Einwilligung

- Einwilligung elektronisch oder schriftlich
 - § 4 Abs. 2 TDDSG
 - § 12 TMG
 - §4 Abs. 2 - 7 LDSG
 - Realisierung:
 - Anbieter sendet Email an Nutzer, dieser antwortet per Email
 - Einwilligungserklärung in Fenster, Anklicken eindeutiger Button





Unzureichende Einwilligung

- unzureichend:
 - nur Information anstelle von ausdrücklicher Einwilligung
 - Einwilligungserklärung, die nicht ausdrücklich bestätigt werden muß
 - fehlender Hinweis, daß die Daten freiwillig sind
 - Auskunft nur auf schriftliche Anfrage des Nutzers





weiteres zur Einwilligung

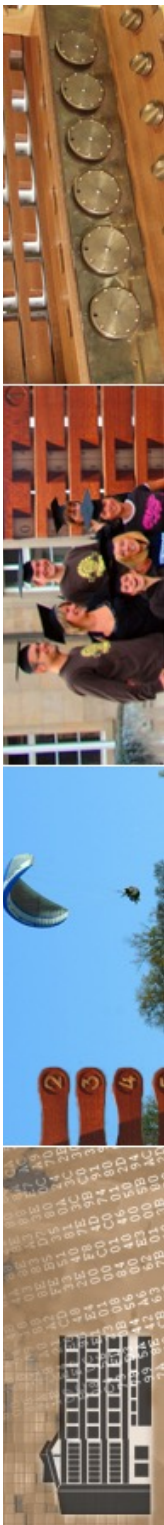
- es muss nachvollziehbar sein, ob und ggf. *welche* Einwilligung erteilt wurde
- die Einwilligung muss vom Nutzer abrufbar sein
- Nutzer hat *jederzeit* das Recht, eine Einwilligung zu *widerrufen*
- wenn elektronische Einwilligung, dann muss auch Widerruf in elektronischer Form angenommen werden





anonyme und pseudonyme Nutzungsmöglichkeiten

- Daten, die unter Pseudonymen gespeichert werden, sind auch personenbezogen
- Cookies für Bildung von Nutzungsprofilen unter Pseudonym: Nutzer sind zu informieren
 - § 3 Abs. 6 BDSG
 - § 3a BDSG
 - § 4 Abs. 6 TDDSG





Auskunftsrecht

- der Nutzer hat ein umfassendes Recht auf Auskunft über die Daten, die der Anbieter über ihn gespeichert hat. Dieses Recht bezieht sich auch auf den logischen Aufbau einer Datensammlung.
 - § 4 Abs. 7 TDDSG
 - § 6 Abs. 1 BDSG
 - § 11 LDSG
- in EU-DSGVO weiter ausgebaut





DSGVO Art. 15

Artikel 15

Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

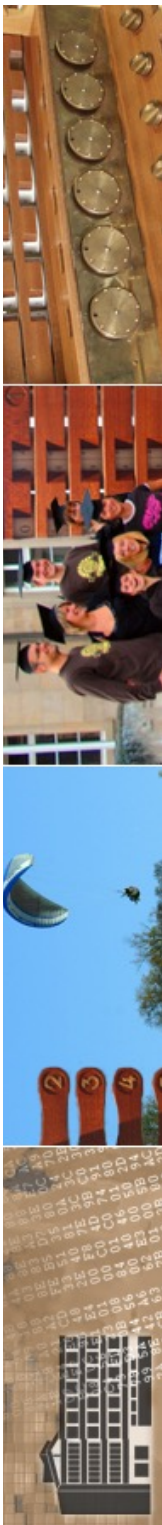
- a) die Verarbeitungszwecke;
- b) die Kategorien personenbezogener Daten, die verarbeitet werden;
- c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.





Weiterleitung an Dritte

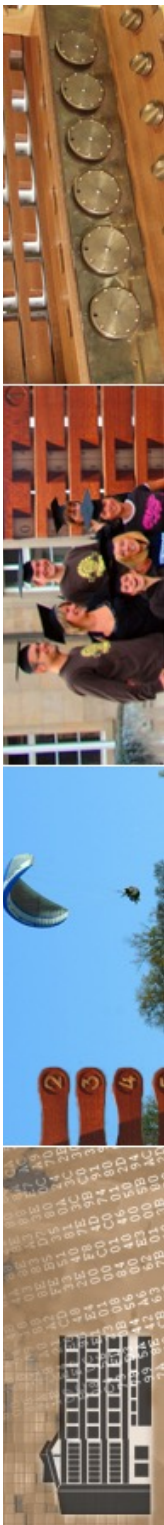
- Weiterleitung über Links: Nutzer nicht mehr in der Lage zu erkennen, dass er von einem Diensteanbieter zu anderem wechselt
- Anbieter von Tele- und Mediendiensten sind *verpflichtet*, dem Nutzer die Weiterleitung an Dritte anzuzeigen
 - TMG
 - § 3 TDG
 - § 7 TDG
 - § 4 Abs. 5 TDDSG
 - § 13 Abs. 3 MDStV





Realisierung

- Weitervermittlung (Link) innerhalb eines Erklärungsfensters
- Kennzeichnung externer Links durch spezielle Grafik
- Bannerwerbung mit dem Hinweis »Anzeige« (wie bei Printmedien)
- unzureichend:
 - lediglich optische Hervorhebung von Links ohne Trennung intern/extern
 - Verzicht auf Nennung des Anbieters, an den weitervermittelt wird
 - Hinweis auf Weiterleitung in AGB





Benutzerordnungen

- vielfältig an Hochschulen (Rechenzentren) und bei Providern verbindliche Benutzerordnungen, so dass sich der Betreiber des Servers (Hosting) rechtlich absichert
- Tübingen: Informationsdienstverordnung





Informationsdienste-Ordnung

Allgemeine Verwaltungs- und Benutzungsordnung für alle Informationsdienste auf elektronischen Anlagen der Universität Tübingen (Informationsdienste-Ordnung) vom 19. Oktober 1998

veröffentlicht in den "Amtlichen Mitteilungen der Universität Tübingen", Jahrgang 24 – Nr. 9 – 26. November 1998

Gemäß §§ 7 Abs. 2, 20 Abs. 2 Nr. 7, 28 Abs. 5 des Universitätsgesetzes Baden-Württemberg in der Fassung vom 10.01.1995 hat die Eberhard-Karls-Universität Tübingen durch Beschluß des Verwaltungsrats vom 04.02.1998 folgende Verwaltungs- und Benutzungsordnung erlassen.

Das Ministerium für Wissenschaft, Forschung und Kunst hat seine Zustimmung mit Erlaß vom 12. Oktober 1998, Az.: 16-515.8/34, erteilt.

§ 1 Geltungsbereich

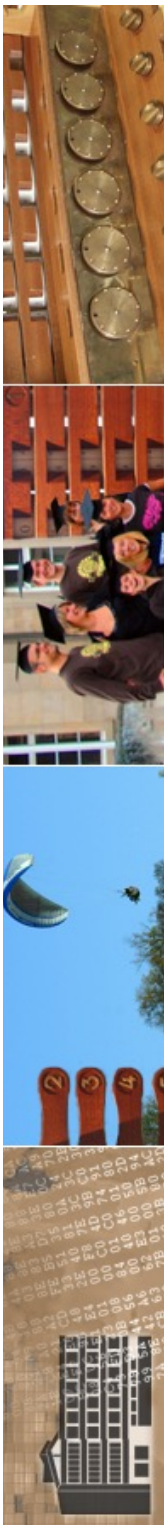
§ 2 Technische Einrichtung für den zentralen Informationsdienst für offizielle Informationen (Uni-Informationsdienst)

§ 3 Informationsbereitstellung im Uni-Informationsdienst

§ 4 Technische Einrichtung für Persönliche Homepages

§ 5 Informationsbereitstellung in Persönlichen Homepages

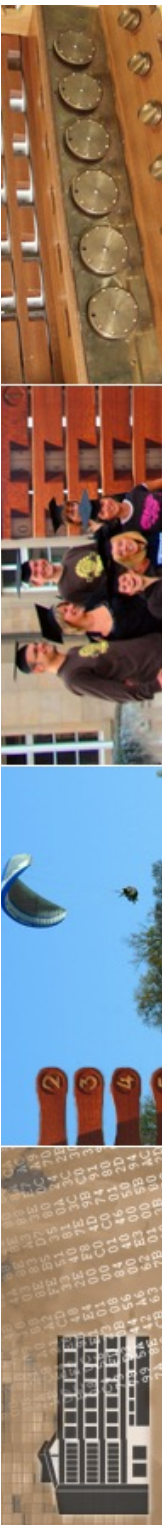
§ 6 Pflichten der Informationsanbieter





Datenschutz

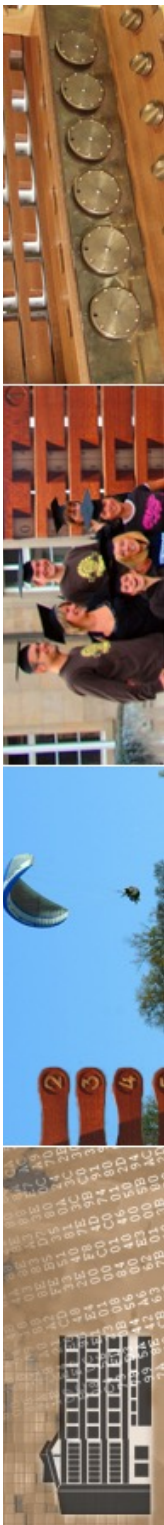
- komplexes, sich rasch anpassende Thematik
 - weitere Homogenisierung innerhalb der EU durch EU-Richtlinien
- Grundsätze: keine Datenhaltung auf Vorrat, nur die notwendigen Daten erheben/vorhalten (BDSG)
- Datenschutz ist *konstruktives* Instrumentarium zum Schutz des Individuums





BDSG und LDSG

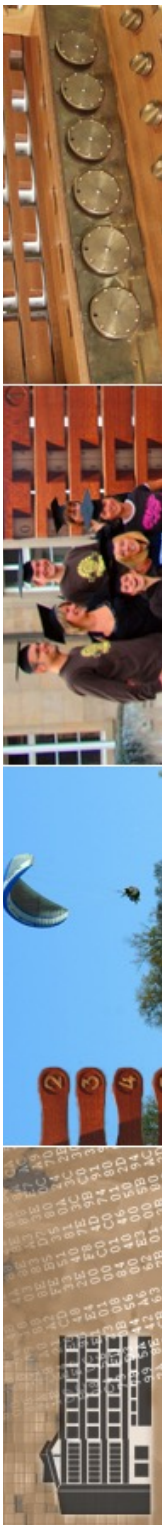
- BDSG: Einrichtungen des Bundes und der privaten Wirtschaft
- LDSG: Landeseinrichtungen und Kommunen
 - durch Behörden und sonstige öffentliche Stellen des Landes, der Gemeinden und Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts





die EU

- „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“
Datenschutz-Grundverordnung
 - Verabschiedet 02. Mai 2016 / 24. Mai 2016
 - Umsetzungsfrist: 2 Jahre
 - http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.DEU&toc=OJ:L:2016:119:TOC

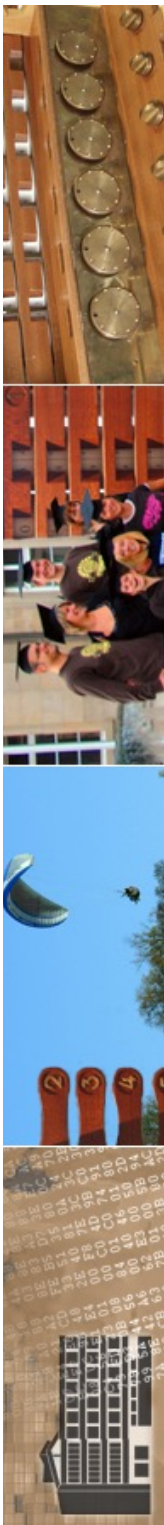




EU-

Datenschutzgrundverordnung

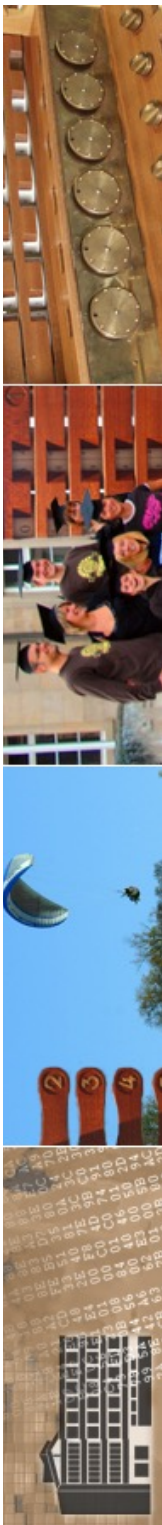
- EU-DSG
- <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE>
- Verordnung „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“





Allgemeines I

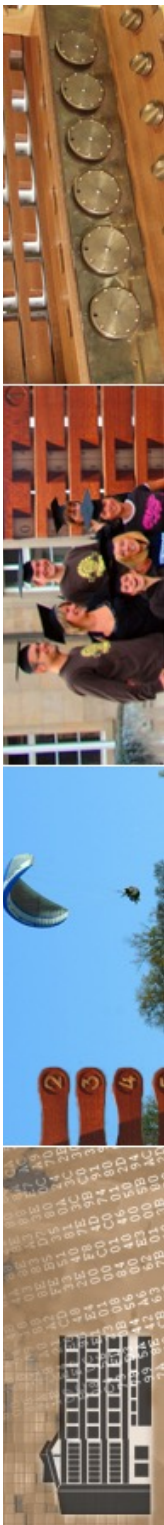
- Offizieller Name
„Verordnung 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“
- Löst Richtlinie 95/46/EG („EU-Datenschutz-Richtlinie“) ab





Allgemeines II

- Veröffentlicht am 4.5.2016, in Kraft getreten am **25.5.2016**
- Gilt direkt in allen Mitgliedsstaaten, keine Umsetzungsgesetze wie bei Richtlinien, daher einheitlicher Datenschutz europaweit

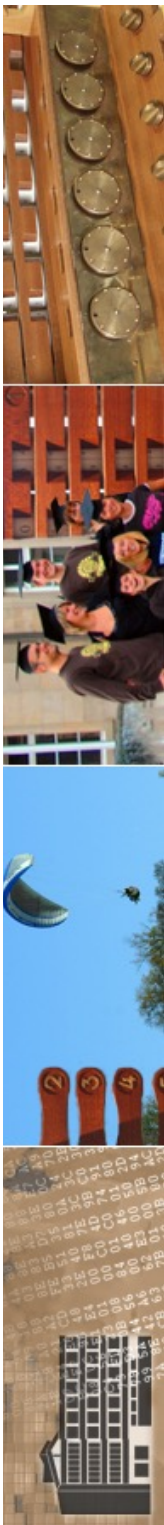




Änderungen I

- Marktortprinzip (Art. 3)

DSGVO gilt für alle Unternehmen, die in Europa Waren oder Dienstleistungen anbieten, auch für nicht-europäische Unternehmen (Amazon, Facebook, Microsoft, Google, ...)



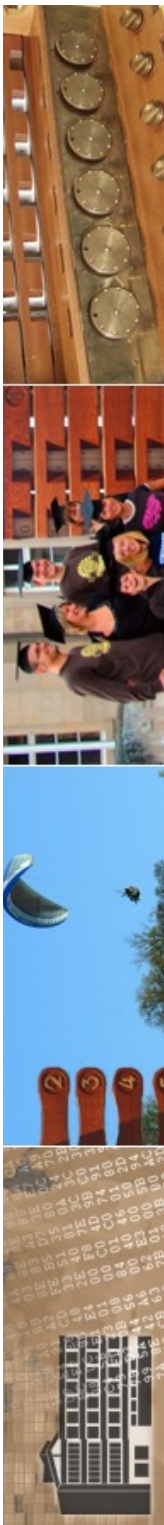


Änderungen II

- Privacy by Design, Privacy by Default (Art. 25)

Standardeinstellungen müssen datenschutzfreundlich sein;

Neue Anwendungen müssen datensparsam konzipiert werden





Änderungen III

- **Recht auf Vergessenwerden (Art. 17)**
Recht auf Löschen aller Daten bei einem Unternehmen, die nicht mehr notwendig sind
- **Recht auf Datenübertragbarkeit (Art. 20)**
Recht auf Export aller bei einem Unternehmen vorhandenen Daten in einem „strukturierten, gängigen, maschinenlesbaren Format“



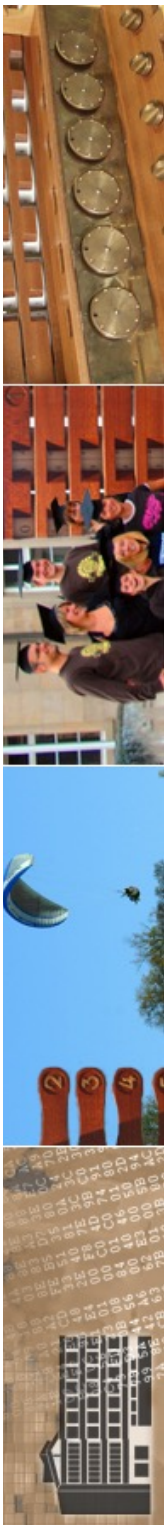


Änderungen IV

- ***Empfindliche Geldbußen*** möglich (Art. 83)

Bis zu 20 Millionen Euro oder 4% des Vorjahresumsatzes, je nachdem, welcher Wert höher ist

Bisher in Deutschland maximal 300.000€





Grundprinzip

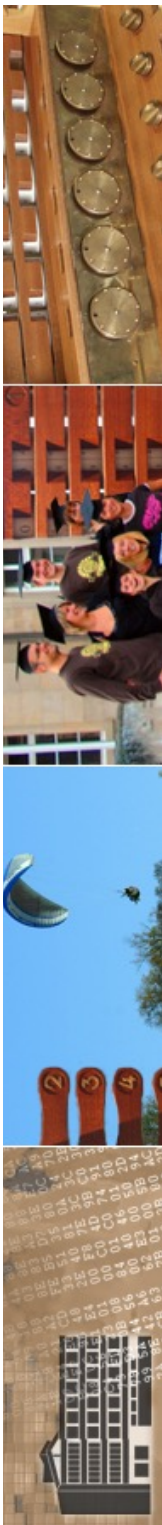
- in der EU-DSGVO wie bisher
 - die Verarbeitung personenbezogener Daten ist untersagt
 - Ausnahmen in Art. 6
 - Einwilligung
 - Rechtsgrundlage
 - ...





AV

- Auftrags(daten)verarbeitung: ADV
 - „Klassiker“
 - u.a. geregelt in LDSG §85a
 - wichtig: AV-Vertrag
 - besonders kritisch wird es, wenn Daten *außerhalb EU* gelangen





Safe Harbor

- Datenschutz-Vereinbarung zwischen EU und USA
- Übermittlung personenbezogener Daten in USA damit möglich
 - u.a. sind IBM, Microsoft, Amazon, Google, HP und Facebook beigetreten
- vom EuGH 2015 gekippt
- Nachfolge EU-US Privacy Shield
 - gekippt von EuGH 2020 durch „Schems-II“





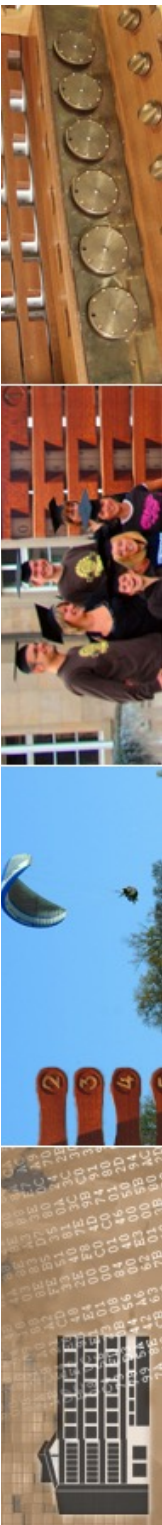
Schrems II

- Sommer 2020: Urteil „Schrems-II“ des EuGH

Praktische Auswirkungen der Rechtsprechung des EuGH auf den internationalen Datentransfer (Rechtssache C-311/18 „Schrems II“)

Der Europäische Gerichtshof hat mit dem Urteil in der → [Rechtssache C-311/18 „Schrems II“](#) klargestellt, dass personenbezogene Daten von EU Bürgern nur an Drittländer außerhalb des Europäischen Wirtschaftsraums übermittelt werden dürfen, wenn sie in diesem Drittland einen im Wesentlichen gleichwertigen Schutz genießen wie in der EU. Für die USA hat er ein solches angemessenes Schutzniveau verneint.

Jeder Verantwortliche im Sinne des Datenschutzrechts ist jetzt aufgerufen, seine Datenübermittlungen in Drittländer und die hierfür genutzte Grundlage nach Kapitel V der DSGVO zu überprüfen. Datenübermittlungen in die USA, die bisher auf das EU-US Privacy Shield gestützt wurden, müssen nun durch eine Schutzmaßnahme nach Artikel 46 DSGVO abgesichert werden, da der Europäische Gerichtshof diesen Angemessenheitsbeschluss der Europäischen Kommission mit sofortiger Wirkung für unwirksam erklärt hat. Für Datenübermittlungen in die USA, wenn nötig ggf. auch für Datenübermittlungen in weitere Drittländer, ist mit zusätzlichen Maßnahmen sicherzustellen, dass die personenbezogenen Daten auch im jeweiligen Drittland stets angemessen geschützt sind. Auch eine vorbeugende Prüfung der Übermittlung nach Großbritannien mit Blick auf den sog. „Brexit“ wird bereits zum jetzigen Zeitpunkt empfohlen.





EU und USA

Neues Datenschutzabkommen in Kraft

Stand: 10.07.2023 19:22 Uhr

Die EU-Kommission hat ein neues Datenschutzabkommen zwischen den USA und der EU verabschiedet. Es ist bereits der dritte Anlauf, nachdem zwei Vorgängerregelungen vom Europäischen Gerichtshof gekippt wurden. Doch erneut zeichnet sich eine Klage ab.

Drei Jahre nach dem Aus von "Privacy Shield" ist ein neues Datenschutzabkommen zwischen der EU und den USA in Kraft getreten. Die USA gewährleisteten nun ein angemessenes Schutzniveau für personenbezogene Daten, die aus der EU an Unternehmen in Amerika übermittelt würden, teilte die EU-Kommission in Brüssel mit.



Die neue Regelung führt demnach verbindliche Garantien ein, um die zuvor vom Europäischen Gerichtshof (EuGH) geäußerten Bedenken auszuräumen. Der EuGH hatte den "Privacy Shield" für die Übermittlung von Daten aus Europa über den Atlantik im Juli 2020 mit der Begründung gekippt, dass das Datenschutzniveau in den USA nicht den Standards der EU entspreche.

Die Richter bemängelten vor allem die weitreichenden Zugriffsmöglichkeiten von US-Geheimdiensten auf Daten von Europäerinnen und Europäern. Für Unternehmen war durch das EuGH-Urteil große Rechtsunsicherheit beim Datentransfer zwischen den USA und der EU entstanden.

Von der Leyen lobt neues Abkommen

Künftig dürfen US-Geheimdienste auf die Daten nur dann zugreifen, wenn es notwendig und verhältnismäßig sei, hieß es seitens der EU-Kommission. Außerdem soll ein Gericht zur Überprüfung des Datenschutzes eingerichtet werden.

"Der neue EU-US-Datenschutzrahmen wird sichere Datenströme für Europäer gewährleisten und Rechtssicherheit für Unternehmen auf beiden Seiten des Atlantiks schaffen", sagte EU-Kommissionspräsidentin Ursula von der Leyen. Der neue Rechtsrahmen soll regelmäßig überprüft werden, so die EU-Kommission.





Trans-Atlantic Data Privacy Framework (TADPF)

Was sich beim Einsatz von US-Dienstleistern ändert

Im Jahr 2020 hat der EuGH das Datenschutzniveau in den USA als unzureichend eingestuft und damit das bestehende Privacy Shield-Abkommen als Nachfolger des Safe Harbour-Abkommens gekippt. Dies führte zu Verunsicherungen im Hinblick auf den Einsatz von US-Anbietern. Nutzer von Google, Meta, Microsoft, Amazon und Co. drohten Untersagungsverfügungen und Bußgelder von Aufsichtsbehörden.

Mit dem neuen Abkommen soll nun wieder Rechtssicherheit hergestellt werden. Dabei handelt es sich bei dem TADPF nicht um ein Gesetz, sondern um ein wichtiges Abkommen zwischen der EU-Kommission und dem US-Handelsministerium. In diesem Rahmen haben die USA bessere Schutzmaßnahmen zugunsten von EU-Bürgern eingeführt. Im Gegenzug hat die EU-Kommission ein angemessenes Datenschutzniveau in den USA festgestellt (sog. Angemessenheitsbeschluss).

Im Unterschied zum alten Privacy Shield müssen US-Unternehmen ein Selbstzertifizierungsverfahren durchlaufen, um sich auf den Angemessenheitsbeschluss berufen zu können und in einer Datenbank gelistet zu werden. Hier kann gezielt nach diesen Unternehmen gesucht werden.

TKG

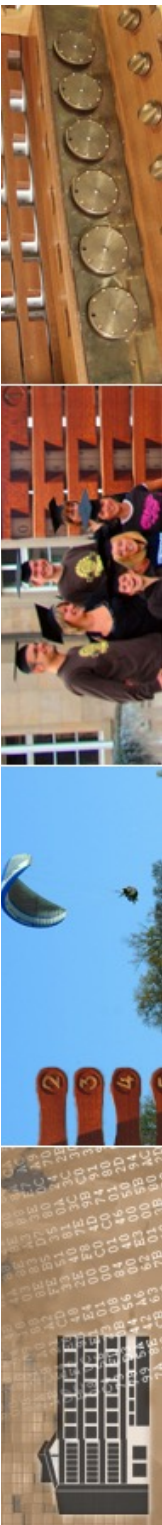
- Telekommunikationsgesetz:
 - regelt Wettbewerb im Bereich der Telekommunikation
 - Abhören von Nachrichten (§ 148): bis zu zwei Jahren Freiheitsstrafe
 - Sperrung von Internetseiten durch "Gesetz zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen"
 - nie in Kraft getreten
 - 01.12.2011 vom Bundestag aufgehoben





TKG

- TKG regelt auch die Möglichkeit der Protokollierung
 - TKG §95: Bestandsdaten dürfen erhoben und verwendet werden
 - TKG §96: Verkehrsdaten dürfen für spezielle, dort genannte Zwecke (insbesondere Abrechnung) verwendet werden, sonst nicht





Vorratsdatenspeicherung

- Anbieter der Telekommunikationsdienste waren nach TKG verpflichtet, elektronische Kommunikationsvorgänge zu registrieren, *auch ohne Anfangsverdacht auf Gefahr*
 - Gesetz zur Neuregelung der Telekommunikationsüberwachung (TKÜ und TKÜV)
 - Auskunftspflicht der TK-Anbieter
 - rechtlich sehr umstritten





Vorratsdatenspeicherung

- Nach Forderungen von EU-Kommission, CDU und CSU soll künftig nachvollziehbar werden, wer mit wem in den letzten sechs Monaten per Telefon, Handy oder E-Mail in Verbindung gestanden oder das Internet genutzt hat. Bei Handy-Telefonaten und SMS soll auch der jeweilige Standort des Benutzers festgehalten werden. In Verbindung mit anderen Daten soll auch die Internetnutzung nachvollziehbar werden.



Stoppt die Vorratsdatenspeicherung!

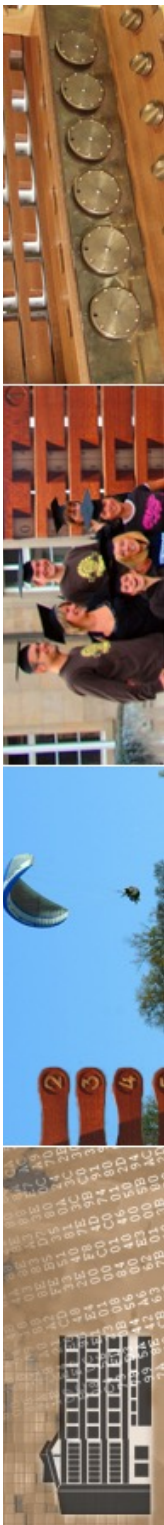
Gegen die totale Protokollierung von Telefon, Handy, E-Mail und Internet.





Vorratsdatenspeicherung

- Stand:
 - das Bundesverfassungsgericht hat am 2.3.2010 das deutsche Gesetz zur Vorratsdatenspeicherung aufgehoben
 - EU-Richtlinie hierzu war Basis für Koalitionsvertrag
 - EU-Richtlinie von EuGH mit starker Kritik am 08.04.2014 für Rechtswidrig erklärt
 - verletzt sind Art. 7 und 8 der EU-Grundrechtecharta (Recht auf Privatsphäre und Recht auf Datenschutz)
 - 20.09.2022: EuGH erklärt auch neue deutsche Gesetzgebung (wieder) für rechtswidrig





@ CSU will Vorratsdatei x

www.heise.de/newsticker/meldung/CSU-will-Vorratsdatenspeicherung-und-keine-Haftungsfreistellungen-fuer-WLAN

D800

Einloggen auf heise online

heise online

heise online

05.01.2013 10:44

CSU will Vorratsdatenspeicherung und keine Haftungsfreistellungen für WLAN-Netze

Vom 7. bis zum 9. Januar treffen sich die 44 CSU-Bundestagsabgeordneten im oberbayerischen Wildbad Kreuth, um Positionsbeschlüsse zu fassen. Einer der dazu kursierenden Entwürfe trägt den Titel "Sicher und smart in die Zukunft" und beschäftigt sich mit der "Digitalisierung des Alltags". Er sieht unter anderem den Erlass neuer Regeln für den Betrieb **offener WLAN-Netze**[1] vor, wobei "einseitige Haftungsfreistellungen" vermieden werden sollen. Mit dieser Formulierung zielt das Papier offenbar auf einen **Bundesratsvorstoß**[2] der Länder Hamburg und Berlin, die die Bundesregierung aufgefordert haben, die Anwendung des Störerhaftungsprinzips für Hotspot-Anbieter zu **überprüfen**[3].

Darüber hinaus soll das Strafrecht um den neuen Tatbestand der "Datenhehlerei" ergänzt werden. Das könnte je nach Wortlaut dazu führen, dass Behörden zukünftig weniger Daten über in Steuerparadiesen hinterzogene Gelder erwerben können. Die CSU-Landesgruppenvorsitzende Gerda Hasselfeldt betonte vorab außerdem, sie halte eine Vorratsdatenspeicherung weiterhin für "unabdingbar", um der "Kriminalität im Internet" zu begegnen.





Nach Pariser Terror-Anschlag: Rufe nach Vorratsdatenspeicherung aus SPD, CDU und CSU werden wieder lauter

vorlesen / MP3-Download



(Bild: ZDF)

Nach dem Mordanschlag auf das Satiremagazin Charlie Hebdo zeigt sich, dass die politischen Reflexe der Regierungskoalition noch gut funktionieren.

Bundesinnenminister Thomas de Maizière (CDU) unterstützt die Forderung der CSU nach möglichst rascher Wiedereinführung der Vorratsdatenspeicherung – erst recht nach dem [Terroranschlag von Paris](#). Der Vorschlag sei zwar nicht neu und keine



Vorratsdatenspeicherung 2015

- Bundestag beschließt (etwas überraschend) die „kleine“ Vorratsdatenspeicherung im Oktober 2015
 - verfassungsrechtliche Überprüfung steht aus
 - überraschende Meinungsänderung bei Heiko Maas und der SPD





Vorratsdatenspeicherung

Größtenteils harmlos? Von wegen!

Sind doch nur Metadaten. Gespeichert wird nur für ein paar Wochen. Es gilt der Richtervorbehalt. Mit solchen Aussagen wird die Vorratsdatenspeicherung gerne verharmlost.



Verwaltungsgericht Köln: Vorratsdatenspeicherung ist unvereinbar mit EU-Recht

20.04.2018 18:25 Uhr

Stefan Krempf



(Bild: dpa, Ole Spata/Archiv)

Nach dem Oberverwaltungsgericht Nordrhein-Westfalen hat nun auch das Verwaltungsgericht Köln festgestellt, dass Provider derzeit nicht verpflichtet sind, im Rahmen der Vorratsdatenspeicherung Nutzerspuren ihrer Kunden aufzubewahren.

- <https://www.heise.de/newsticker/meldung/Verwaltungsgericht-Koeln-Vorratsdatenspeicherung-ist-unvereinbar-mit-EU-Recht-4028925.html>



EuGH-Gutachter: Deutsche Vorratsdatenspeicherung verstößt gegen EU-Recht

Das allgemeine und unterschiedslose Protokollieren von Verbindungs- und Standortdaten ist nur bei einer ernststen Bedrohung für die nationale Sicherheit erlaubt.

Lesezeit: 4 Min.  In Pocket speichern

   160

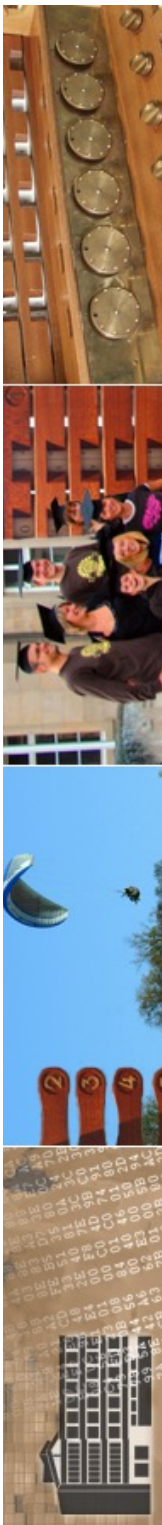


(Bild: mixmagic/Shutterstock.com)

18.11.2021 11:41 Uhr

Von Stefan Krempf

Die deutschen Vorschriften zur Vorratsspeicherung von Telefon- und Internetdaten sind unvereinbar mit dem EU-Recht. Zu diesem Resümee kommt Manuel Campos Sánchez-Bordona, Generalanwalt beim Europäischen Gerichtshof (EuGH), in seinen am Donnerstag veröffentlichten Schlussanträgen zu einem Ersuchen des Bundesverwaltungsgerichts (BVerwG).





Koalitionsvertrag: Ampel will Vorratsdatenspeicherung rechtssicher gestalten

Das neue Regierungsbündnis setzt bei der inneren Sicherheit auf Kompromisse wie die "Login-Falle" und strebt einen "umfassenden digitalen Aufbruch" an.

Lesezeit: 10 Min.  In Pocket speichern

   23

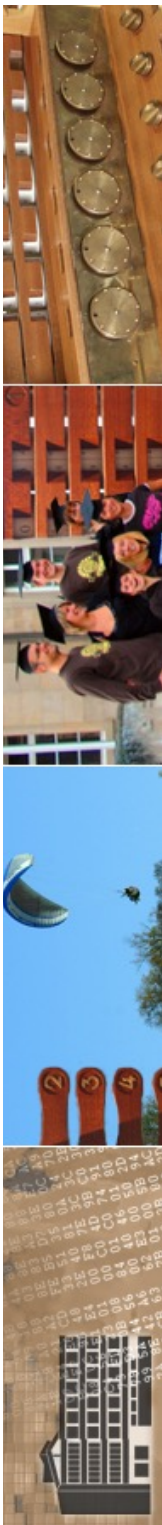


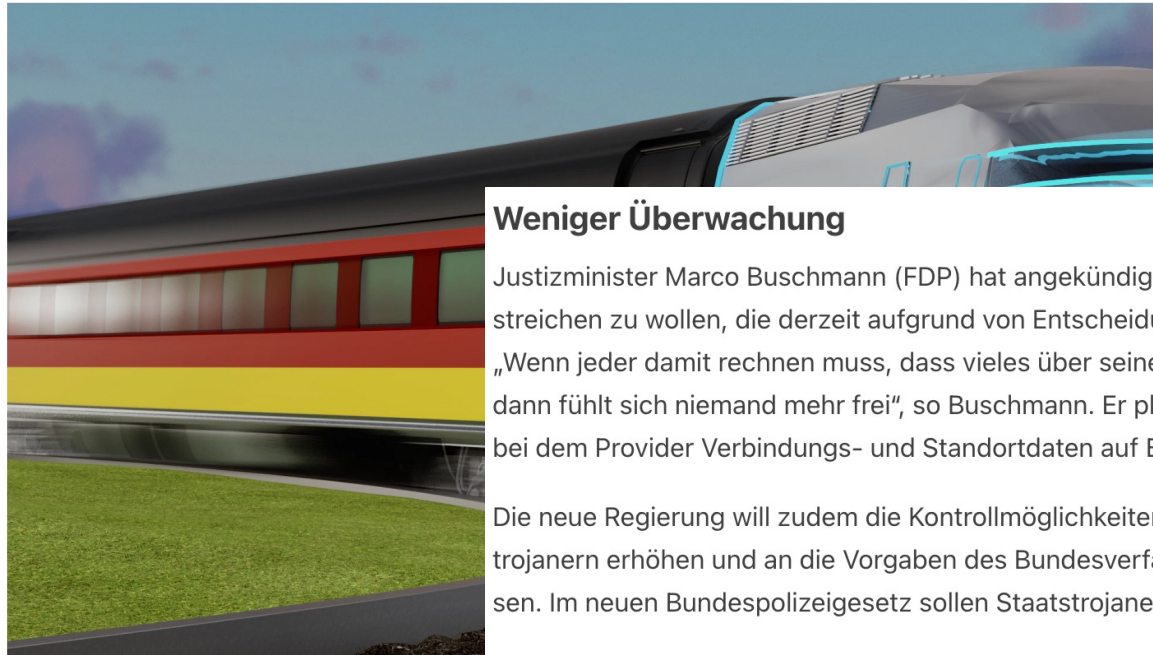
(Bild: monticello/Shutterstock.com)

18:56 Uhr

Von Stefan Krempl

SPD, Grüne und FDP haben am Mittwoch nach gut einmonatigen Verhandlungen ihren Koalitionsvertrag vorgestellt und veröffentlicht. Vor allem im Bereich der inneren Sicherheit ist der Plan von Kompromissen geprägt. So enthält er kein klares Aus für das massenhafte Sammeln von Verbindungs- und Standortinformationen oder für den Einsatz von Staatstrojanern.





Weniger Überwachung

Justizminister Marco Buschmann (FDP) hat angekündigt, die anlasslose Vorratsdatenspeicherung endgültig streichen zu wollen, die derzeit aufgrund von Entscheidungen von Verwaltungsgerichten ausgesetzt ist. „Wenn jeder damit rechnen muss, dass vieles über seine Kommunikation ohne Anlass gespeichert wird, dann fühlt sich niemand mehr frei“, so Buschmann. Er plädiert stattdessen für das Quick-Freeze-Verfahren, bei dem Provider Verbindungs- und Standortdaten auf Betreiben von Strafverfolgern „einfrieren“ müssten.

Die neue Regierung will zudem die Kontrollmöglichkeiten und Eingriffsschwellen für den Einsatz von Staatstrojanern erhöhen und an die Vorgaben des Bundesverfassungsgerichts für die Onlinedurchsuchung anpassen. Im neuen Bundespolizeigesetz sollen Staatstrojaner nicht vorkommen.

Buschmann will gemeinsam mit Faeser eine Evaluierung aller den Behörden zur Verfügung stehenden Überwachungsmaßnahmen auf den Weg bringen: die Überwachungsgesamtrechnung. Sie geht auf das Bundesverfassungsgericht zurück. Es erkannte schon im Jahr 2010, dass für die verfassungsrechtliche Bewertung von Überwachungsmaßnahmen eine isolierte Betrachtung der jeweiligen Einzelregelung zu Datenspeicherung oder Datenzugriff nicht genügt. Die Regierungen haben sich bisher aber um eine Gesamtschau der Überwachungsmaßnahmen und oftmals sogar um Details zu Einzelmaßnahmen gedrückt. Die Überwachungsgesamtrechnung verspricht hier erstmals Transparenz.

Das Gesetzgebungsverfahren soll insgesamt digitaler werden. Man will „betroffene Kreise aus der Gesellschaft [...] besser einbinden“, ein digitales Gesetzgebungsportal schaffen und öffentliche Kommentierungsmöglichkeiten erproben. Das BMDV soll außerdem neue Gesetze einem Digitalisierungsscheck unterziehen. Was genau das bedeutet, ist aber noch unklar.

Auf ins Neuland

Der „Digitale Aufbruch“ der

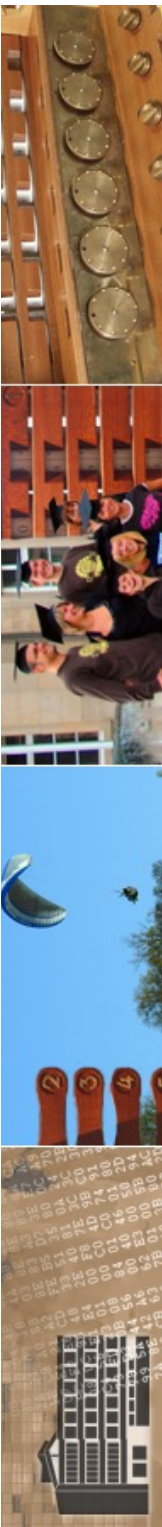
Schnelles Netz für alle, eine offenere Koalition hat sich eine anspruchsvolle zeigt, wer in der neuen Regierung für Schwerpunkte liegen.

Von Jo Bager

Die neue Regierung will „mehr Fortschritt wagen“ – und die Digitalpolitik nimmt im Koalitionsvertrag viel Raum ein. Dazu wurden die Zuständigkeiten neu geordnet. Der Posten der bisherigen Digitalstaatsministerin Dorothee Bär (CSU) fällt weg. Ein eigenes Digitalministerium gibt es ebenfalls nicht.

Bundeskanzler Olaf Scholz (SPD) hat dem Verkehrsministerium zusätzliche Digitalkompetenzen zugewiesen, es heißt jetzt „Bundesministerium für Digitales und Verkehr“ (BMDV). Minister Volker Wissing (FDP) verantwortet nun „operative Vorhaben der Digitalpolitik“. Sein Ministerium soll über ein neu zu schaffendes Digitalbudget entscheiden.





EuGH bestätigt: keine anlasslose Vorratsdatenspeicherung – mit Ausnahmen



Vorratsdatenspeicherung ist unter bestimmten Voraussetzungen möglich – wenn die nationale Sicherheit bedroht ist. Ohne Anlass widerspricht sie EU-Recht.

Lesezeit: 4 Min.  In Pocket speichern

   170



(Bild: Foto: Gerichtshof der Europäischen Union)

20.09.2022 10:54 Uhr

Von Eva-Maria Weiß

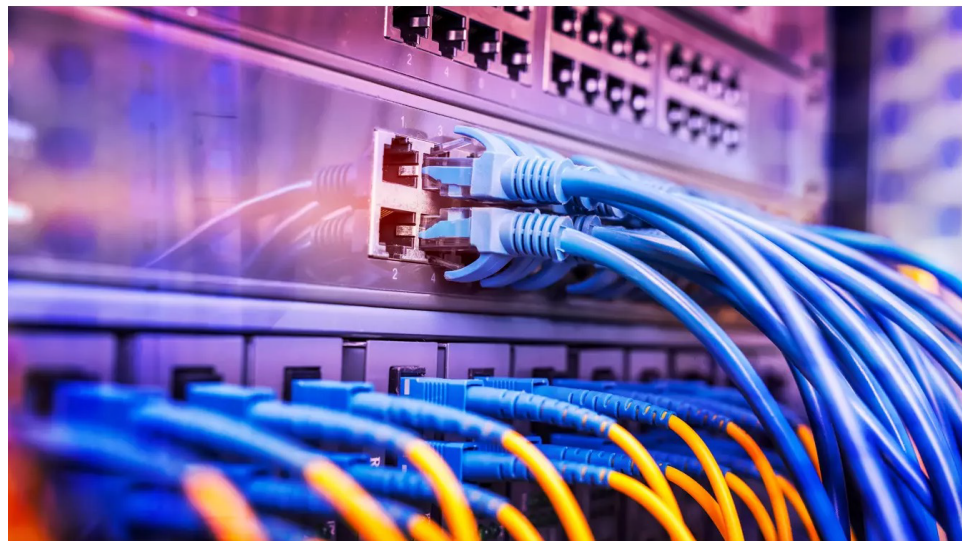
Eine allgemeine und unterschiedslose Vorratsdatenspeicherung widerspricht dem Unionsrecht, das hat der Europäische Gerichtshof (EuGH) nun in einem Urteil bestätigt – und wendet sich damit gegen die deutsche Regelung. Allerdings macht der EuGH auch den Weg frei für Ausnahmen. Verkehrs- und Standortdaten sowie IP-Adressen können gespeichert werden, "liegt eine ernste Bedrohung für die nationale Sicherheit vor".

Koalitionsstreit: Faeser will für Vorratsspeicherung von IP-Adressen kämpfen

Bundesinnenministerin Faeser sieht sich mit dem EuGH-Urteil gegen eine allgemeine Vorratsdatenspeicherung gestärkt. Sie sucht die Fehde mit dem Rest der Ampel.

Lesezeit: 6 Min.  In Pocket speichern

   41



(Bild: asharkyu/Shutterstock.com)

21.09.2022 14:34 Uhr

Von Stefan Krempl

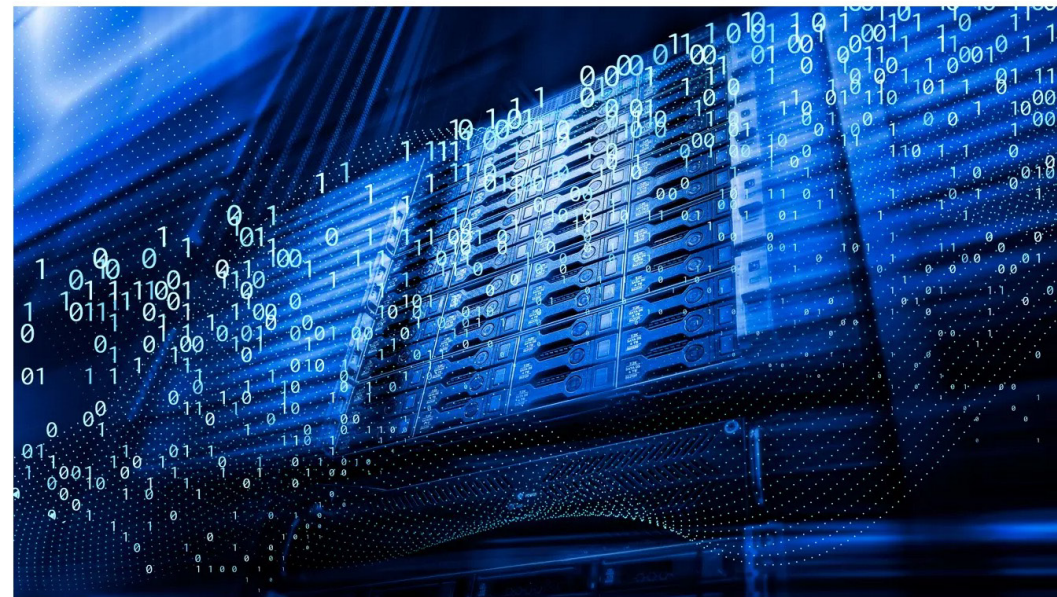
Die künftige Linie der Ampel-Koalition zum Protokollieren von Nutzerspuren im Internet birgt gewaltigen Sprengstoff für das Regierungsbündnis. So hält Bundesinnenministerin Nancy Faeser (SPD) nach dem Urteil des Europäischen Gerichtshofs (EuGH) gegen eine allgemeine Vorratsdatenspeicherung unerbittlich an ihrer Forderung fest, zumindest IP-Adressen weiterhin anlasslos für einen gewissen Zeitraum aufzubewahren. Grüne und FDP drängen dagegen darauf, Verbindungs- und Standortdaten nur noch im Verdachtsfall quasi einzufrieren ("Quick Freeze").

Nach EuGH-Urteil: Bayern drängt auf Vorratsspeicherung von IP-Adressen

In der Ampel stehen nach dem EuGH-Urteil fast alle Zeichen auf das Einfrieren von Verkehrsdaten bei Verdacht (Quick Freeze). Doch es gibt Gegenstimmen.

Lesezeit: 7 Min.  In Pocket speichern

   247



(Bild: Timofeev Vladimir/Shutterstock.com)

20.09.2022 13:21 Uhr

Von Stefan Krempl

Nach dem erneuten Nein des Europäischen Gerichtshofs (EuGH) zu einer allgemeinen anlasslosen Vorratsdatenspeicherung geht die Debatte über Alternativen hierzulande in die Vollen. Bürgerrechtler, Datenschützer und die Internetbranche machen Druck, das seit Jahren umstrittene Instrument endgültig zu beerdigen sowie Verbindungs- und Standortdaten nur noch im Verdachtsfall zu erheben. Gerade aus Bayern kommen aber andere Töne.

Überwachung: EuGH erklärt Vorratsdatenspeicherung in Bulgarien für rechtswidrig

Auch das sechsmonatige Protokollieren von Nutzer Spuren in Bulgarien ist nicht mit dem EU-Recht vereinbar, hat der Europäische Gerichtshof am Freitag geurteilt.

Lesezeit: 2 Min. In Pocket speichern

16



(Bild: Zolnierek/Shutterstock.com)

19.11.2022 17:33 Uhr

Von Stefan Krempf

Eine weitere nationale Vorschrift zur verdachtsunabhängigen Vorratsdatenspeicherung in den EU-Mitgliedsstaaten hat keinen Bestand. Der Europäische Gerichtshof (EuGH) hat am Freitag im Lichte seiner ständigen Rechtsprechung entschieden, dass die in Bulgarien 2015 eingeführte Pflicht für Telekommunikationsanbieter zum sechsmonatigen Aufbewahren von Verbindungs- und Standortdaten dem EU-Recht widerspricht.



Ausnahme: "Schutz der nationalen Sicherheit"

Schließlich habe der Europäische Gerichtshof (EuGH) festgehalten, dass Verkehrs- und Standortdaten sehr wohl allgemein und unterschiedslos auf Vorrat gespeichert werden dürften. Und zwar dann, wenn es um den Schutz der nationalen Sicherheit, die Bekämpfung schwerer Kriminalität oder die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit gehe. "Das darf ein Justizminister der Öffentlichkeit nicht verschweigen, wenn er stattdessen das unzureichende Quick-Freeze-Verfahren aus dem eigenen Hause anpreist", sagte Wiese. Er ergänzte, wer nichts speichere, könne auch nichts einfrieren.

Das Bundesverwaltungsgericht hatte die anlasslose und flächendeckende Vorratsdatenspeicherung als vollständig europarechtswidrig eingestuft. Der am Donnerstag veröffentlichten Entscheidung lagen Klagen von zwei Telekommunikationsunternehmen zugrunde. Wegen der rechtlichen Unsicherheiten wird die Regelung seit 2017 nicht mehr genutzt. Bei der Speicherung von Verkehrs- und Standortdaten fehle eine strikte Begrenzung auf den Zweck des Schutzes der nationalen Sicherheit, hielt das Gericht fest. IP-Adressen dürften zwar zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit gespeichert werden, allerdings sei das im Telekommunikationsgesetz nicht eindeutig bestimmt.



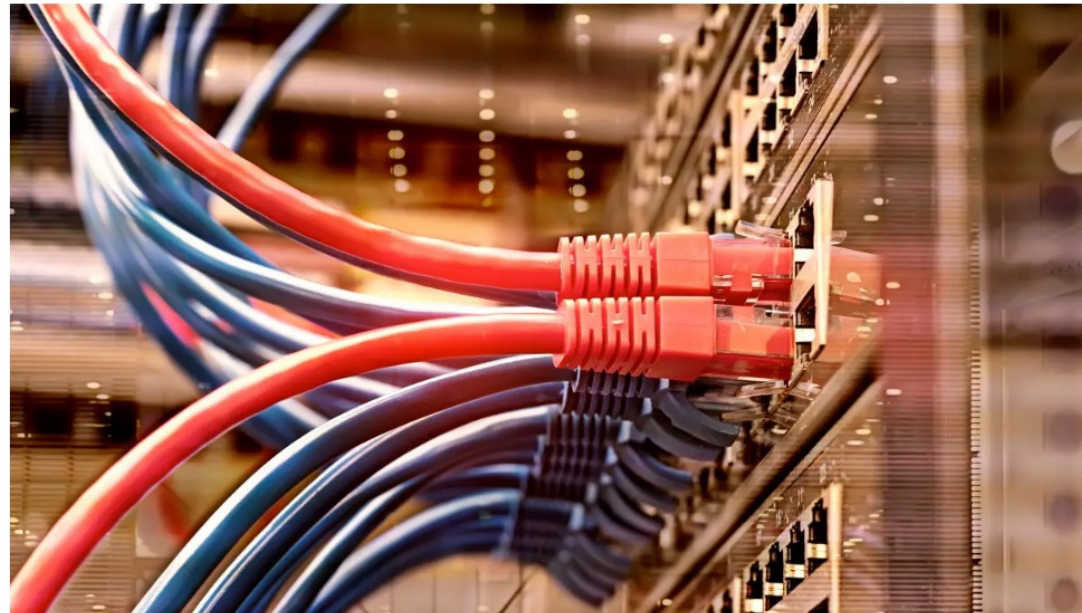


SPD-Fraktionsvize: Vorratsdatenspeicherung nicht vorschnell begraben

Hat das Bundesverwaltungsgericht die Vorratsdatenspeicherung gekippt? Der SPD-Fraktionsvize sieht im Urteil keine Absage. Er will an dem Vorhaben festhalten.

Lesezeit: 3 Min.  In Pocket speichern

   148

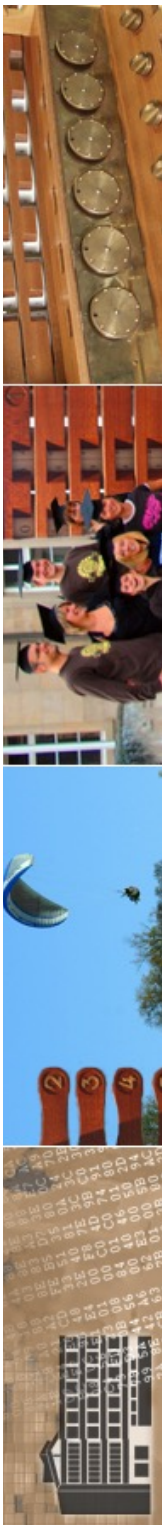


(Bild: asharkyu/Shutterstock.com)

09.09.2023 12:22 Uhr

Von Tilman Wittenhorst, mit Material der dpa

Gerade hat das Bundesverwaltungsgericht die anlasslose Vorratsdatenspeicherung (VDS) als nicht mit EU-Recht vereinbar verworfen – sie könne nach dem Urteil höchstens unter besonders schwerwiegenden Umständen zulässig sein, auf diese Beschränkung gehe das kritisierte






17.07.2013 12:51



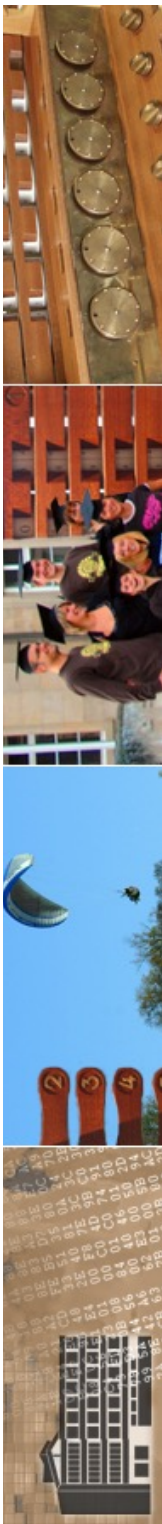
« Vorige | Nächste »

Friedrich erhebt Sicherheit zum "Supergrundrecht"

 vorlesen / MP3-Download

Bundesinnenminister Hans-Peter Friedrich (CSU) wandelt auf den Spuren seines Vorgängers Otto Schily (SPD) und räumt der Sicherheit Vorrang vor allen anderen Grundrechten einschließlich der Freiheit ein. "Sicherheit ist ein Supergrundrecht", das im Vergleich mit anderen Rechten herauszuheben sei, erklärte der Christsoziale am Dienstag nach einer Sondersitzung des Parlamentarischen Kontrollgremiums (PKG) des Bundestags zum US-Überwachungsprogramm PRISM.

Friedrich versuchte Medienberichten zufolge zwar noch, seine Aussage zu relativieren: Auch für die Sicherheit dürfe die Freiheit nicht pauschal über Bord geworfen werden. Der Begriff des "Supergrundrechts" legt aber nahe, dass die in demokratischen Verfassungen als Abwehr gegen Eingriffe des Staates verankerten Grundrechte zu Privilegien zweiter Klasse entwertet werden sollen.



Friedrich erhebt Sicherheit zum "Supergrundrecht"

heise online 17.07.2013 12:51 Uhr - Stefan Krempl

vorlesen



Bundesinnenminister Hans-Peter Friedrich (CSU) wandelt auf den Spuren seines Vorgängers Otto Schily (SPD) und räumt der Sicherheit Vorrang vor allen anderen Grundrechten einschließlich der Freiheit ein. "Sicherheit ist ein Supergrundrecht", das im Vergleich mit anderen Rechten herauszuheben sei, [erklärte](#) der Christsoziale am Dienstag nach einer Sondersitzung des Parlamentarischen Kontrollgremiums (PKG) des Bundestags zum [US-Überwachungsprogramm PRISM](#).

Friedrich versuchte Medienberichten zufolge zwar noch, seine Aussage zu relativieren: Auch für die Sicherheit dürfe die Freiheit nicht pauschal über Bord geworfen werden. Der Begriff des "Supergrundrechts" legt aber nahe, dass die in demokratischen Verfassungen als Abwehr gegen Eingriffe des Staates verankerten Grundrechte zu Privilegien zweiter Klasse entwertet werden sollen.



Dem Bundesinnenminister geht Sicherheit über alles.

Bild: BMI

Schily hatte 2005 für seine vergleichbare Linie in der Anti-Terror-Politik den [Big Brother Award für sein Lebenswerk](#) erhalten. Etliche der von dem Sozialdemokraten maßgeblich vorangetriebenen Anti-Terror-Maßnahmen seien "unverhältnismäßig, ja maßlos – sie zeigen Merkmale eines nicht erklärten Ausnahmezustands und eines autoritären Präventionsstaates, in dem letztlich Rechtssicherheit und Vertrauen verloren gehen", hatte die Jury ihre Entscheidung damals [begründet](#). "Die Unschuldsvermutung, eine der wichtigsten

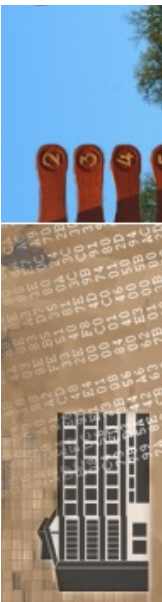


GG Art 1

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.





TK-Anbieter

- TKG: Anbieter von Telekommunikationsdiensten für die Öffentlichkeit
 - besondere Pflichten
- die Universitäten sind keine TK-Anbieter in diesem Sinne
 - ...und geben sich *große* Mühe, dass dies so bleibt, was aber nicht leicht ist...
 - Begründung: geschlossene Benutzergruppe





PersVG

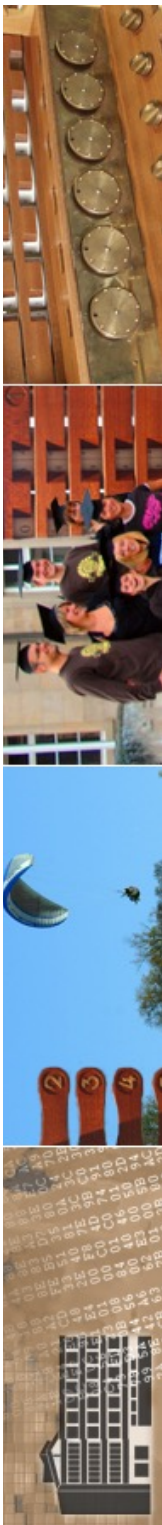
- PersVG des Bundes und der Länder regelt in diesem Zusammenhang die Einflussnahme/Mitsprache der Personal- und Betriebsräte
- BW:
 - LPVG §79: Mitbestimmung in sonstigen Angelegenheiten
Abs. 1.10: "Einführung grundsätzlich neuer Arbeitsmethoden"
 - üblich: Abschluss einer **Dienstvereinbarung**
 - LPVG § 80: Mitwirkung und Anhörung





UrhG

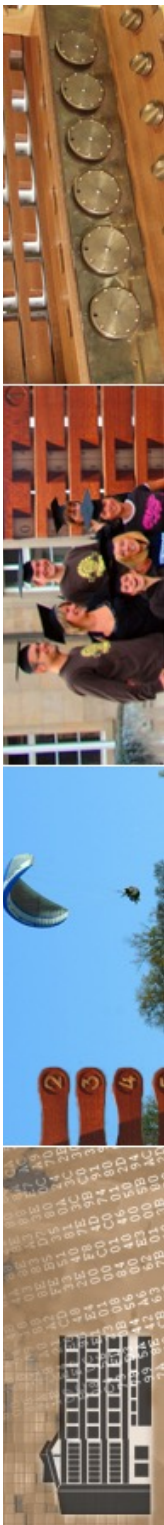
- 5.7.2007: neue Gesetzeslage ("zweiter Korb"), in Kraft seit 1.1.2008
 - §52: Wissenschaft: geringe Teile eines Werkes dürfen für abgegrenzten Benutzerkreis zugänglich gemacht werden
 - §53a: Fernversand von Artikeln (Subito)
 - UB Tü: Einzelverträge mit jeweiligem Verlag
 - Tausch über Peer-to-Peer-Netzwerke verboten





digitale Signatur

- noch ein Gesetz: Signaturgesetz (SigG, 17.7.2009)
- regelt die Möglichkeit der digitalen Signatur
- hohe Hürden in Deutschland, EU-Regelung praktikabler
- <http://www.ca.uni-tuebingen.de/>





Zentrum für Datenv... x +

← → ↻ 🏠 🌐 www.ca.uni-tuebingen.de/ca-betrieb/local-unitue-ca.html ☆ 🔍

LEISTUNGEN KONTAKT, ANTRÄGE, BERATUNG WIR ÜBER UNS INFRASTRUKTUR PROJEKTE

Authority (CA) > CA-Betrieb > Local-UNITUE-CA

Local-UNITUE-CA in der UNITUE-PKI

UNITUE-PKI der Universität Tübingen - Local-UNITUE-CA
 Die Local-UNITUE-CA ist Mitglied einer PKI im Geltungsbereich der Universität Tübingen (UNITUE-PKI). Die UNITUE-PKI ist nicht in die DFN-PKI integriert. Die Local-UNITUE-CA berücksichtigt spezifische Anforderungen im Nutzerbereich der Universität Tübingen. Dabei werden unterschiedliche Anforderungen an die Vergabeverfahren für Zertifikate durch die Einrichtung von Sub-CAs berücksichtigt.

Für die Verifikation der Zertifikatkette in der Local-UNITUE-CA ist das Root-Zertifikat der UNITUE-PKI erforderlich. Das Root-Zertifikat muss zu den Stammzertifizierungsstellen hinzugefügt werden.

[Das Root-Zertifikat hier herunterladen.](#)

Fingerprint Root-Zertifikat (SHA1)
 F6:80:51:9D:09:77:4F:DC:98:AD:92:BA:34:1D:46:D6:B7:B7:DA:32

Für die Verifikation der Zertifikatkette in der LocalSUB-UNITUE-CA01 (Webmail-Zertifikate) ist das SubCA-Zertifikat der UNITUE-PKI erforderlich. Das LocalSUB-UNITUE-CA01-Zertifikat muss zu den Zwischenzertifizierungsstellen hinzugefügt werden.

[Das LocalSUB-UNITUE-CA01-Zertifikat hier herunterladen.](#)

Fingerprint LocalSUB-UNITUE-CA01 (SHA1)
 E0:99:A0:13:EA:2F:D8:8C:5C:A8:A9:59:45:51:F9:43:A2:3E:9A:0C

Kontakt
 07071-29 70250
 hotline@zdv.uni-tuebingen.de

Betriebszustand

Schnellzugriff

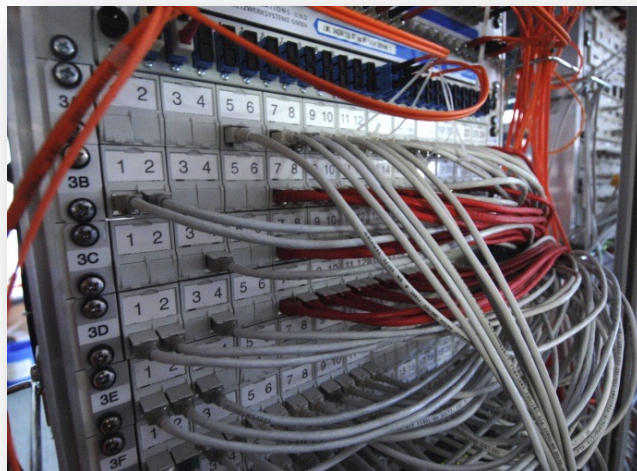
- [ZDV-Adventskalender](#)
- [Webmailer](#)
- [EPV](#)
- [Aktuelle Kurse](#)
- [Passwortänderung](#)
- [Netzkarte](#)





typisch deutsch...

- ein spezielles Problem in D ist...





- Startseite →
- Die Situation** ↓
- Das Abmahn(un)wesen →
- Abmahnwellen →
- Handlungsbedarf →
- Unsere Arbeit →
- Der Verein →
- Mitgliedschaft →
- Spenden →
- Partnerschaft →
- Impressum →
- Kontakt →

Die Situation

Das deutsche Abmahnwesen, in Art und Handhabung einmalig auf der Welt, gibt Anlass zur Sorge, denn es lädt zum Missbrauch ein. Und dieser Einladung wird auch immer wieder Folge geleistet.

Aber auch schon ohne Missbrauch ist die deutsche Abmahnpraxis ein zweifelhaftes Instrument. Ein hoher Prozentsatz der Abgemahnten war sich nicht bewusst, Rechte verletzt zu haben. Wer dies als unwahr abtut, unterstellt zugleich, dass die Deutschen durch und durch ein Volk der Diebe und Betrüger sind. Denn anders ließe es sich nicht erklären, dass so viele bisher unbescholtene Bürger (ja sogar Rechtsanwälte) wegen Urheber- und Markenrechtsverletzungen, wegen TDG und UWG in die Abmahnfalle tapen.

Mit dem Instrument der – für den Abgemahnten! – kostspieligen Abmahnung haben wir in Deutschland eine merkwürdige Methode, den Bürgern einzubläuen, was sie zu tun und zu lassen haben.

„Dog Law“ nennt Prof. Dr. Herberger schon 1999 auf dem 8. EDV-Tag in Saarbrücken kritisierend diese Einstellung: wie einem Hund vermittelt man uns das Wissen um ein Fehlverhalten hinterher durch Prügel.

Das widerspricht krass der vielzitierten Vorstellung vom „mündigen Bürger“. Ein solcher nämlich müsste *vorher* wissen, was erlaubt ist und was nicht.

Das gilt selbstverständlich auch für all die Gesetze und Verordnungen, die jemand zu befolgen hat, der einen Auftritt im Internet aufbaut:





Angeblicher DSGVO-Verstoß: Abmahnwelle wegen Google Fonts

Viele Webseitenbetreiber erhalten gerade eine Zahlungsaufforderung über 100 € wegen Verstoßes gegen die DSGVO. Was steckt dahinter und wie kann man sich wehren?

Lesezeit: 4 Min.  In Pocket speichern

   1041

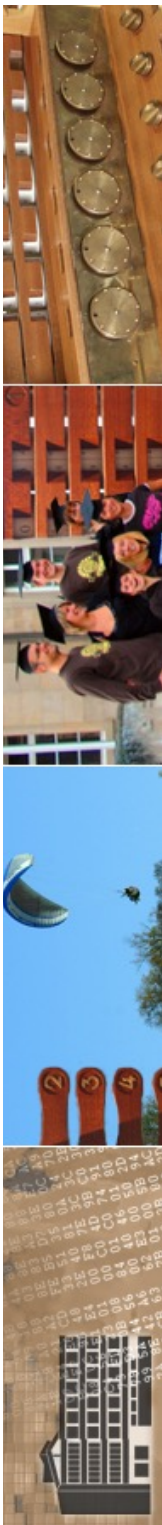


(Bild: Tom auf Pixabay)

09.08.2022 14:01 Uhr | c't Magazin

Von Joerg Heidrich

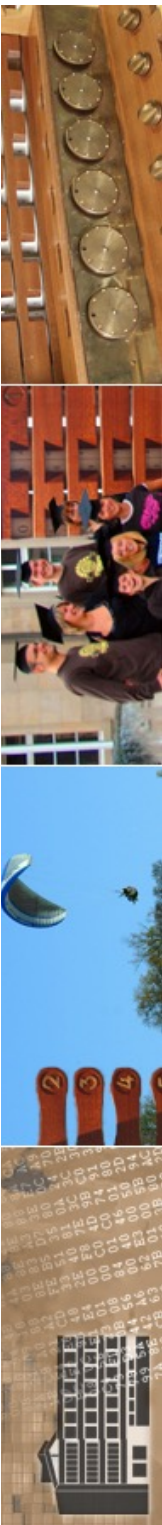
Tausende von Empfängern staunen derzeit über Forderungsschreiben, die sie in ihrem E-Mail-Postfach oder im Briefkasten vorfinden. Weil sie Googles kostenlose Fonts in ihre Websites eingebettet haben, sollen sie 100 bis knapp 500 Euro berappen.





Urheberrecht (UrhG)

- UrhG: regelt das Recht des Urhebers am eigenen Werk
 - Begriff "Werk" ist zu klären
 - nur natürliche Personen können Urheber sein
 - üblicherweise Schutz bis 70 Jahre nach Tod des Urhebers
 - amtliche Werke sind nicht geschützt (gemeinfrei)
 - an Uni Tü: größtes Problem der "Netzhygiene"





Bildnisrecht

- Besonderheit: **Recht am eigenen Bild**
(Kunst-Urhebergesetz KUG 1907/1952)
 - Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden“ KUG §22
 - Ausnahmen existieren (KUG §23)
 - Bildnisse der Zeitgeschichte
 - Personen nur als Beiwerk
 - Bildnisse von Versammlungen, ...
 - „höheres Interesse der Kunst“





Links

- Recht im DFN-Verein
 - <http://www.dfn.de/rechtimdfn>
- Universität Münster (Prof. Dr. Hören)
 - <http://www.uni-muenster.de/Jura.itm/ hoeren/>
- virtuelles Datenschutzbüro
 - <http://www.datenschutz.de>
- ZENDAS: Datenschutzstelle der Universitäten des Landes Baden-Württemberg
 - <http://www.zendas.de>



Recht im DFN

Rechtliche Aspekte der Nutzung fortgeschrittener Kommunikationsdienste

Die Nutzung des Internets und des Deutschen Forschungsnetzes als Teil des Internets wirft eine Vielfalt neuer und ungeklärter Rechtsfragen auf. Der DFN-Verein hat deshalb an der Universität Münster die Forschungsstelle Recht im DFN eingerichtet. Die Forschungsstelle Recht im DFN befasst sich mit Rechtsproblemen, die im Zusammenhang mit der Nutzung des DFN aufgeworfen werden, und stellt Ergebnisse öffentlich zur Verfügung.

Die Forschungsstelle Recht arbeitet in folgender Weise:

- **DFN-Rechtsguide und Wissensbasis**
Laufend aktualisiertes Basisdokument als Einstieg zum Thema "Recht im DFN" und umfangreiche Hintergrundinformationen zu den im DFN-Rechtsguide skizzierten Themen.
- **Empfehlungen**
Herausgabe von Handlungsempfehlungen und Mustertexten zu Rechtsproblemen, die eine Vielzahl von DFN-Einrichtungen betreffen und an denen sich die Einrichtungen orientieren können.
- **Anfragen**
Reaktion auf Anfragen zu allgemeinen rechtlichen Problemen im Zusammenhang mit der Nutzung des Netzes, die aus der Mitgliedschaft an die Forschungsstelle Recht herangetragen werden.
- **DFN-Infobrief Recht**
Herausgabe eines Infobriefs zu aktuellen Entwicklungen in Gesetzgebung und Rechtsprechung in den für die Nutzung des DFN relevanten Bereichen.
- **Stellungnahmen**
Stellungnahmen zu Gesetzesvorhaben, die die rechtlichen Rahmenbedingungen der Nutzung von elektronischen Informations- und Kommunikationsdiensten betreffen.
- **Vorträge**
Regelmäßige Durchführung von Schulungsveranstaltungen zu aktuellen rechtlichen Fragestellungen, insbesondere im Rahmen der DFN- Mitgliederversammlungen und DFN-Betriebstagen.



ITM

Informations-, Telekommunikations- und Medienrecht

Prof. Dr. Thomas Hoeren



Sprache:



Werkzeuge

[Anmelden](#)

[Beitrags-Feed \(RSS\)](#)

Bildschirmfoto

Tübingen

Stellenausschreibung – SHK für den Bereich des Gewerblichen Rechtsschutzes gesucht

Veröffentlicht am 28. Januar 2020 von Michael Böckers & Kategorie Allgemein, Ankündigungen, Bekanntmachungen.

Stellenausschreibung

Am Institut für Informations-, Telekommunikations- und Medienrecht, zivilrechtliche Abteilung, ist **ab dem 1. April 2020** eine Stelle als

Studentische Hilfskraft (SHK)

(m/w/d)

mit 5 Std./Woche Arbeitszeit zu besetzen. Die Stelle ist bis zum 31. Dezember 2020 befristet. Eine längere Zusammenarbeit ist gewünscht.

Es handelt sich um eine **durch Drittmittel finanzierte Stelle im**

Bereich des Gewerblichen Rechtsschutzes.

Bewerberinnen/Bewerber sollen sich mindestens im zweiten Fachsemester befinden, insbesondere im Bürgerlichen Recht überdurchschnittliche Studienleistungen erbracht haben und ein ausgeprägtes Interesse an den Fragestel-

Wintersemester 2023/24





Virtuelles Datenschutzbüro

Ein Informationsangebot der öffentlichen Datenschutzinstanzen



Welche Rechte hat der Bürger?

Es gibt einige **grundlegende Rechte**, die praktisch immer gelten, unabhängig davon, welche Datenschutzgesetze konkret zur Anwendung kommen. Diese Rechte stehen den Betroffenen zu. Weitere Informationen [finden Sie hier](#). Da viele der Landesbeauftragten für Datenschutz sowie die Bundesbeauftragte für den Datenschutz zugleich auch Beauftragte für die Informationsfreiheit sind, kann der Bürger sich auch in diesen Belangen an die Beauftragten wenden. Weitere Informationen [finden Sie hier](#).

[RSS Feed abonnieren](#)

Neuste Nachrichten

[BayLDA stellt Tätigkeitsbericht für das Jahr 2019 vor](#)

[Sächsischer Datenschutzbeauftragter übernimmt Vorsitz in der deutschen Datenschutzkonferenz](#)

[Datenschutztag 2020 in der Schweiz: Zunehmende Vermischung der Privatsphäre bei der](#)

Bildschirmfoto

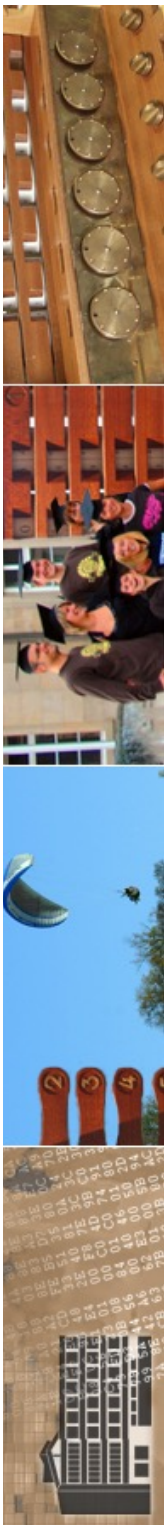




Tipp

- Script "Internetrecht" (Thomas Hoeren)

<https://www.itm.nrw/wp-content/uploads/skript-internetrecht-juli-2020.pdf>



Prof. Dr. Thomas Hoeren
Institut für Informations-, Telekommunikations- und Medienrecht
Universität Münster
Leonardo-Campus 9
D-48149 Münster
hoeren@uni-muenster.de



<https://www.itm.nrw/wp-content/uploads/skript-internetrecht-juli-2020.pdf>

Internetrecht

Stand: April 2020

Das folgende Skriptum steht zum kostenlosen Download zur Verfügung. Das Urheberrecht und sonstige Rechte an dem Text verbleiben beim Verfasser. Eine Verwendung des Textes, auch in Auszügen, bedarf der Genehmigung des Verfassers. Leider kann keine Gewähr für die Richtigkeit und Vollständigkeit der Inhalte übernommen werden. Das Skript kann und will die rechtliche Beratung im Einzelfall nicht ersetzen. Für den Download des Textes wird keine Gebühr verlangt. Es gilt insofern das Shareware-Prinzip. Wenn Ihnen der Text zusagt und Sie die Arbeit des Instituts unterstützen wollen, bitten wir um eine Spende für die „Kaffeekasse“ des Instituts auf folgendes Konto:

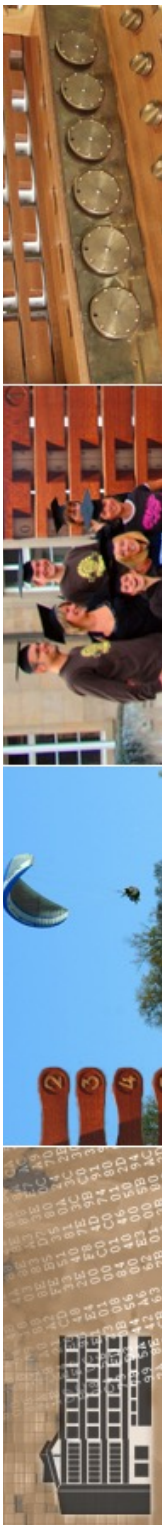




SPON, 01.01.2013

- **Privatsphäre**

Das mitteleuropäische, vernetzte Verständnis von Privatsphäre lässt sich weder technisch noch gesellschaftlich halten. Die kommende Diskussion sollte sich nicht darum drehen, wie sich diese Form der Privatsphäre noch ein paar Jahre verlängern lässt. Sondern wie sich eine dringend notwendige, zukünftige Form der Privatsphäre aus den Bedürfnissen der Gesellschaft heraus entwickeln lässt und nicht nur aus denen der Datenwirtschaft.



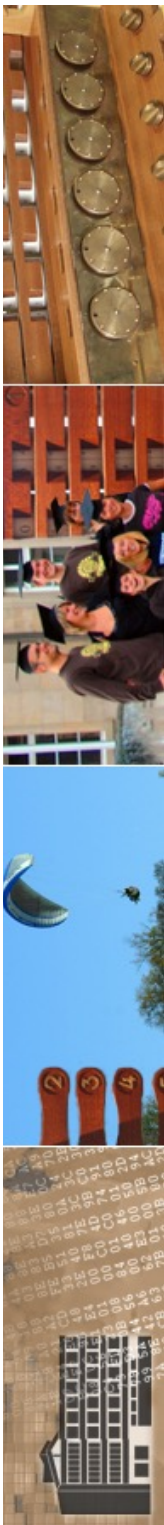


persönlich

- <nocite>
 - Spannungsfeld zwischen Theorie und Praxis ist unermesslich
 - juristische Lage stark gelöst von Technik
 - Datenschutz und Datensicherheit benötigen Ressourcen: nur Gesetze bewirken nichts
 - rein nationale Lösungen sinnlos
 - eine echte Herausforderung unserer Gesellschaft, die durch Corona nochmal deutlich verschärft wird.
- </nocite>



und noch mehr



Gesetz zur Steigerung der Energieeffizienz in Deutschland¹ (Energieeffizienzgesetz - EnEFG)

EnEFG

Ausfertigungsdatum: 13.11.2023

Vollzitat:

"Energieeffizienzgesetz vom 13. November 2023 (BGBl. 2023 I Nr. 309)"

¹ Dieses Gesetz dient der Umsetzung der Richtlinie 2012/27/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur Energieeffizienz, zur Änderung der Richtlinien 2009/125/EG und 2010/30/EU und zur Aufhebung der Richtlinien 2004/8/EG und 2006/32/EG in der Fassung der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU in der jeweils geltenden Fassung.

Fußnote

(+++ Textnachweis ab: 18.11.2023 +++)

(+++ Amtlicher Hinweis des Normgebers auf EG-Recht:

Umsetzung der

EURL 27/2012

(CELEX Nr: 32012L0027) +++)

Das G wurde als Artikel 1 des G v. 13.11.2023 I Nr. 309 vom Bundestag beschlossen. Es ist gem. Artikel 3 dieses G am 18.11.2023 in Kraft getreten.

Inhaltsübersicht

Abschnitt 1 Allgemeine Vorschriften

- § 1 Zweck des Gesetzes, Berichtspflicht
- § 2 Anwendungsbereich
- § 3 Begriffsbestimmungen
- § 4 Energieeffizienzziele

Abschnitt 2 Jährliche Endenergieeinsparverpflichtung des Bundes und der Länder sowie Verpflichtung öffentlicher Stellen

- § 5 Einsparung von Endenergie
- § 6 Einsparverpflichtung öffentlicher Stellen; Verordnungsermächtigungen
- § 7 Aufgaben der Bundesstelle für Energieeffizienz

Abschnitt 3 Energie- oder Umweltmanagementsysteme und Umsetzungspläne für Unternehmen

- § 8 Einrichtung von Energie- oder Umweltmanagementsystemen
- § 9 Umsetzungspläne von Endenergieeinsparmaßnahmen
- § 10 Stichprobenkontrolle hinsichtlich der Einrichtung von Energie- und Umweltmanagementsystemen und der Umsetzungspläne von Energieeinsparmaßnahmen

Abschnitt 4 Energieeffizienz in Rechenzentren

- § 11 Klimaneutrale Rechenzentren
- § 12 Energie- und Umweltmanagementsysteme in Rechenzentren



...und nun...

