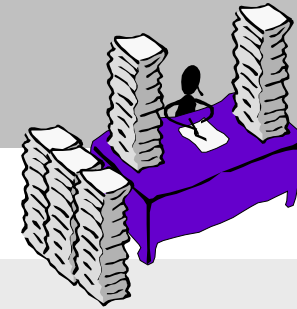


# Schön sicher!

Ein Plädoyer für schöne und sichere Webseiten J

14. Multimediatreff  
9.10.2004, Köln



- „ Diplom-Informatikerin
- „ Beratung, Sachverständigen- und Gutachtertätigkeit  
IT-Sicherheit und Datenschutz für
  - „ IT-Sicherheitsbeauftragte
  - „ Datenschutzbeauftragte
  - „ Betriebs- und Personalräte
  - „ EU-Kommissionsprojekte
- „ Vorstandsmitglied der  
Deutschen Vereinigung für Datenschutz (DVD e. V.)

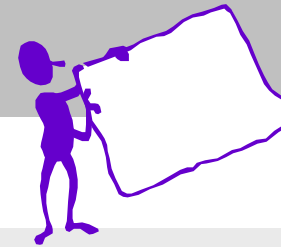
# Grundlagen Datenschutz und IT-Sicherheit

# Wie viel Selbstbestimmung ist erlaubt?

- „ Wer bestimmt im „richtigen Leben“ über das angemessene Maß an Sicherheit? Und wer tut das im Cyberspace?
  
- „ Was würdest du im „richtigen Leben“ akzeptieren und erlauben?
  - „ Dem Getränkeliieferanten ein Hausschlüssel?
  - „ Dem Ladeninhaber beim Betreten ein Meldeformular?
  - „ Ein Stempel auf die Hand beim Verlassen des Ladens?

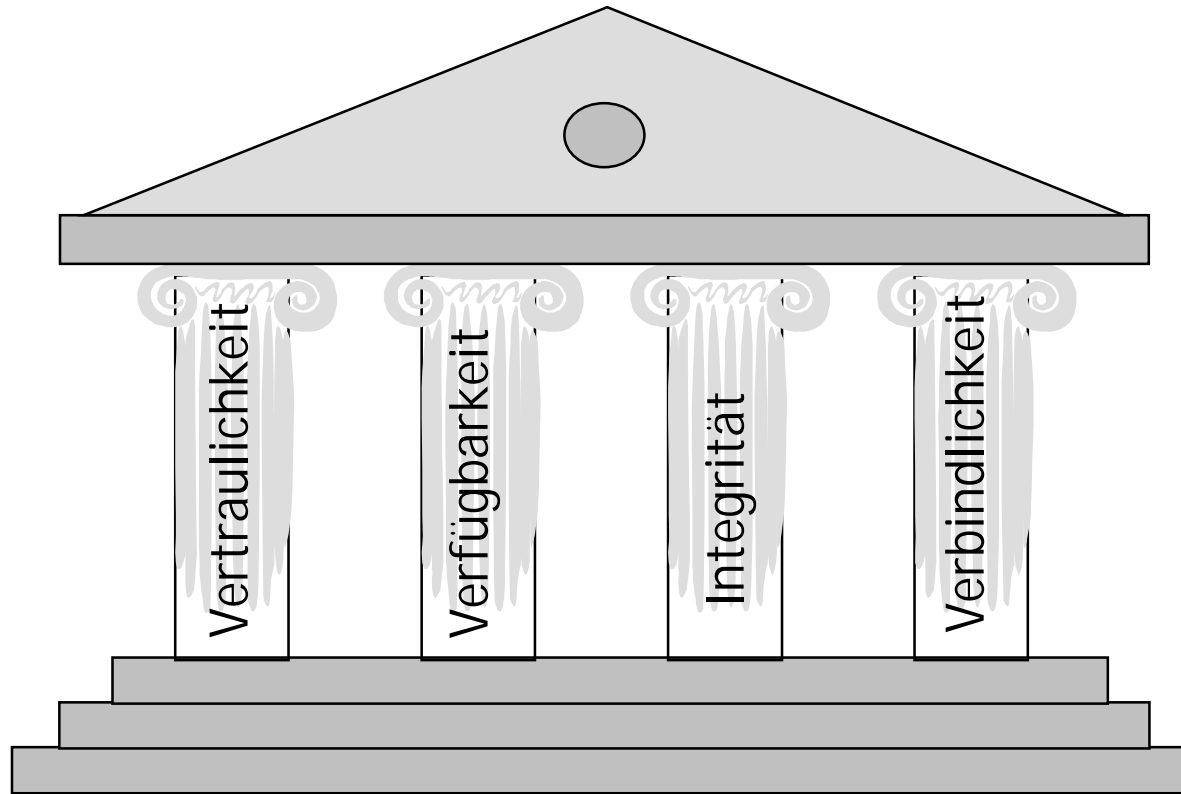
Dies und noch einiges andere  
ist im Cyberspace anscheinend selbstverständlich...

# Ablauf



- „ Datenschutz –  
Grundlagen und gesetzliche Rahmenbedingungen
- „ IT-Sicherheit –  
Verhältnis zum Datenschutz
- „ Privacy sells, Security aber auch:  
Kunden- und Verbraucherwünsche
- „ Die „dicksten Klopfer“ –  
Was zu vermeiden wäre...
- „ Der Webdesigner und die Internet-Programmiererin als Berater –  
mehr als Künstlerin und Codierknecht

# IT-Sicherheit



# Datenschutz schützt Menschen...

- „ ...und nicht die Daten
- „ Ausprägung des Persönlichkeitsrechts (Art. 2 GG)
- „ Bundesverfassungsgericht 1983 (Urteil zur Volkszählung)
  - „ „...Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß...“
- „ (Zu) viele Rechtsnormen:
  - „ BDSG als Auffanggesetz
  - „ Spezialgesetze (TKG, IUKDG, SGB,...)

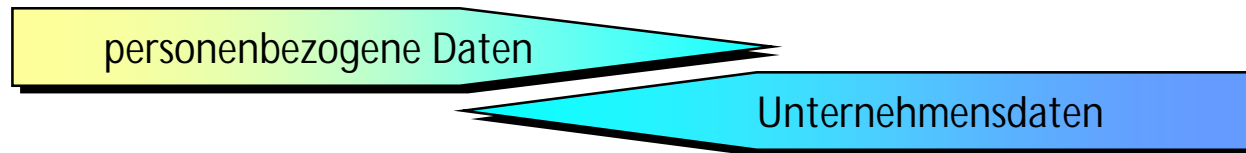
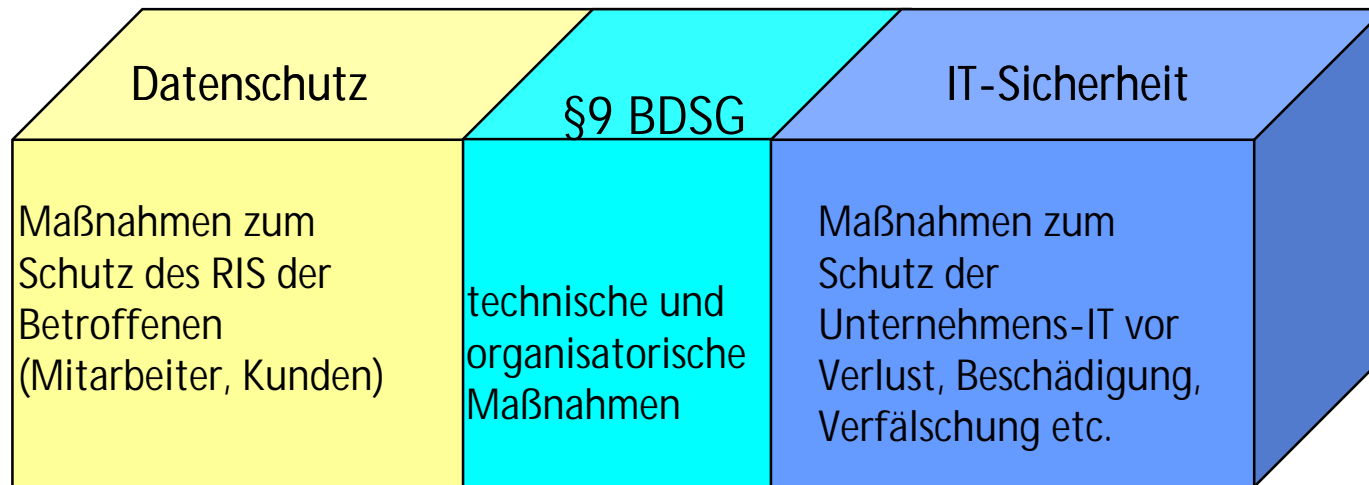
# Kontrollmaßnahmen nach § 9 BDSG

- „ Zutrittskontrolle
- „ Zugangskontrolle *f*
- „ Zugriffskontrolle *f*
- „ Weitergabekontrolle *f*
- „ Eingabekontrolle *f*
- „ Auftragskontrolle
- „ Verfügbarkeitskontrolle *f*
- „ Trennungsgebot *f*

## Beispiel „Zugriffskontrolle“

- „ Ziel: Berechtigte Systemnutzer sollen nur die für sie erforderlichen Berechtigungen und Zugriffsmöglichkeiten erhalten
  - „ Kein Gießkannenprinzip
  - „ „Prinzip der geringsten Berechtigung“
  
- „ Je nach System bzw. Anwendung denkbar:
  - „ Skalierbares Berechtigungssystem
  - „ Einsatz von Verschlüsselung
  - „ Vier-Augen-Prinzip
  - „ ...

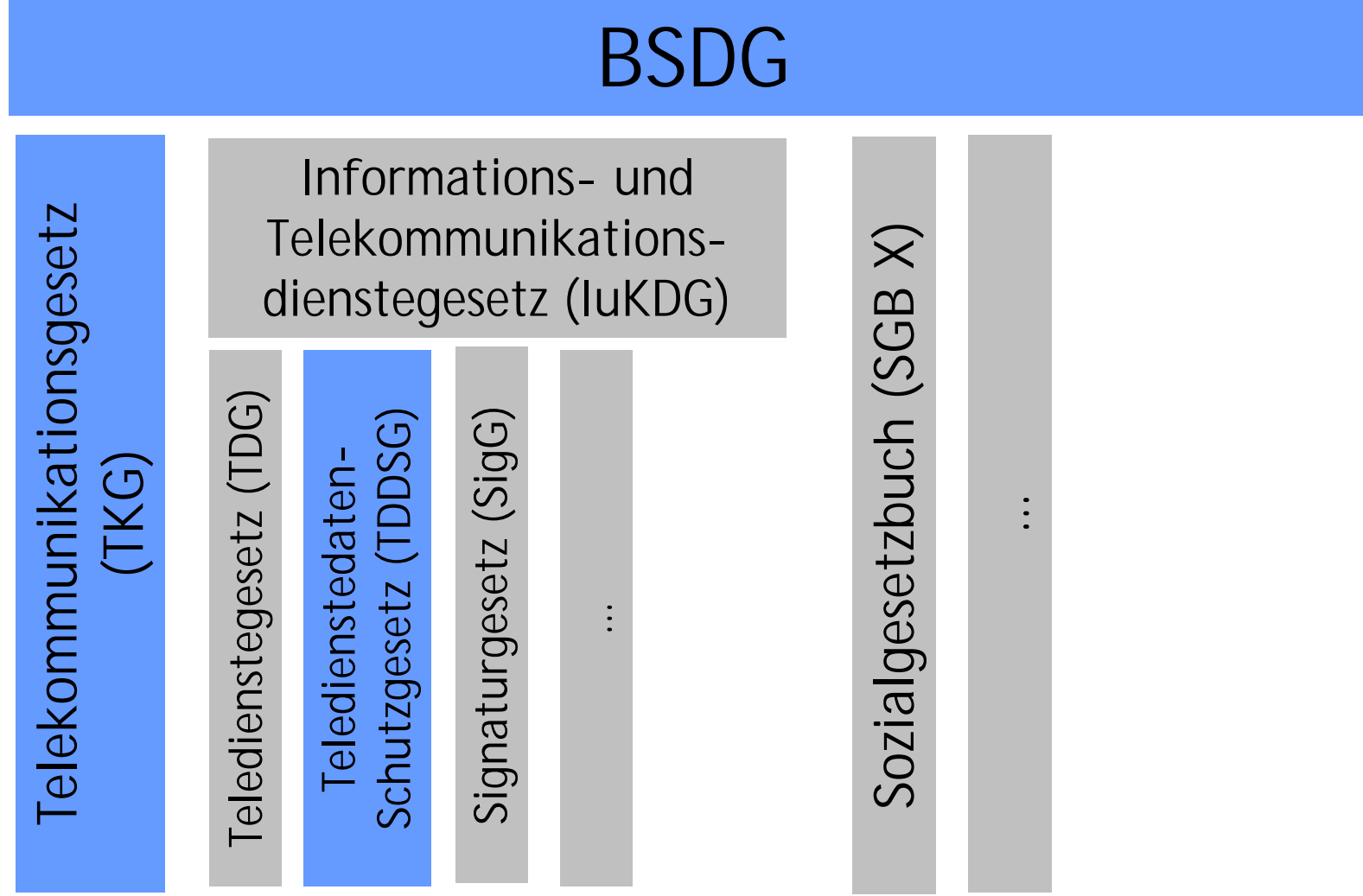
# Datenschutz und IT-Sicherheit



# Wie werden Schutzmaßnahmen bestimmt? Was ist angemessen?

- „ Anhaltspunkte sind:
  - „ Eigenes Wissen und eigene Erfahrung
  - „ Verhalten und Maßnahmen bei Mitbewerbern
  - „ Rechtlicher Rahmen (GG, BDSG, TK-Gesetze, BetrVG, EU-Recht,...)
  - „ Unternehmensstandards und –richtlinien
  - „ Risikoanalyse
  
- „ Daher: „Angemessen“ heißt nicht „Beliebig“

# Subsidiarität in der Datenschutzgesetzgebung



# Einwilligung in elektronischen Verfahren (TKG und TDG)

- „ Die Einwilligung muss bewusst und eindeutig erfolgen
  - „ Getrennt von anderen Vorgängen, wie z.B. einem Login
  - „ Textlich hervorgehoben und deutlich erkennbar
- „ Die Einwilligung muss protokolliert werden
  - „ Jederzeitige Nachweisbarkeit
- „ Der Nutzer muss den Inhalt der Einwilligung jederzeit abrufen können
  - „ Transparenz
  - „ Kein Verstecken in „Mikrofenstern“ auf der siebten logischen Hierarchieebene
- „ Der Nutzer muss die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen können

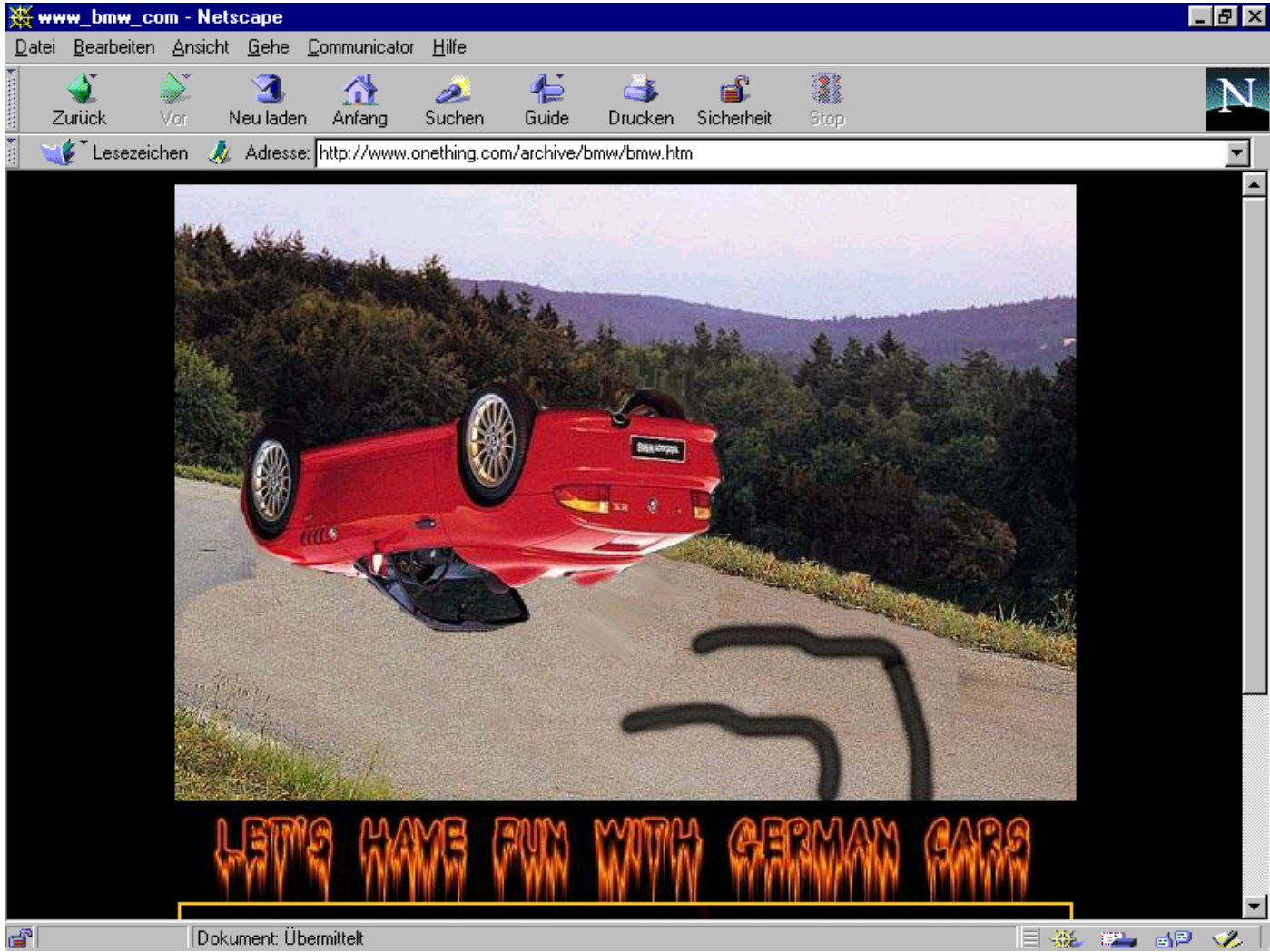
# Inhalt des Impressums (TDG)

- „ Name und Anschrift (bei juristischen Personen: Vertretungsberechtigter)
- „ E-Mail-Adresse
- „ Falls behördliche Zulassung nötig: Zuständige Aufsichtsbehörde
- „ Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister und entsprechende Registernummer
- „ Kammerzugehörigkeit für bestimmte Berufe
- „ UST-ID, sofern vorhanden

Und alles leicht erreichbar, erkennbar und ständig verfügbar!

# Die Wünsche der Kunden und der Nutzer

# Anti-Reklame I



# Anti-Reklame II

Themen  
 Pressemitteilungen  
 Termine  
 Kontakt  
 Datenschutzhinweis  
 Wir über uns  
 links  
 Schwarze liste  
 Impressum

Deutsche Vereinigung für Datenschutz e.V.  
 Bonner Talweg 33-35  
 53113 Bonn  
 Telefon: 0228/22 24 98  
 dvd@datenschutzverein.de

letzte Änderung: 19.9.2004

Kategorie: Finanzdienstleister	Betreiber	Aktive Inhalte	Cookies	Geprüft am	Reaktion auf Anschreiben
<a href="http://www.deutsche-boerse.com">www.deutsche-boerse.com</a>	Deutsche Börse	x		25.1.04	ablehnend
<a href="http://www.awd.de">www.awd.de</a>	AWD	x	x	18.3.03	keine
<a href="http://www.deutsche-bank-24.de">www.deutsche-bank-24.de</a>	Deutsche Bank 24	x	teils	11.8.02	automatisiert
Kategorie: Jobvermittler	Betreiber	Aktive Inhalte	Cookies	Geprüft am	Reaktion auf Anschreiben
<a href="http://www.stellenanzeigen.de">www.stellenanzeigen.de</a>	Stellenanzeigen.de GmbH	x		22.1.04	keine
<a href="http://www.stepstone.de">www.stepstone.de</a>	Stepstone	x		11.11.01	keine
Kategorie: KFZ	Betreiber	Aktive Inhalte	Cookies	Geprüft am	Reaktion auf Anschreiben

# Negativ: Keine Alternative ohne aktive Inhalte



Lieber Besucher!

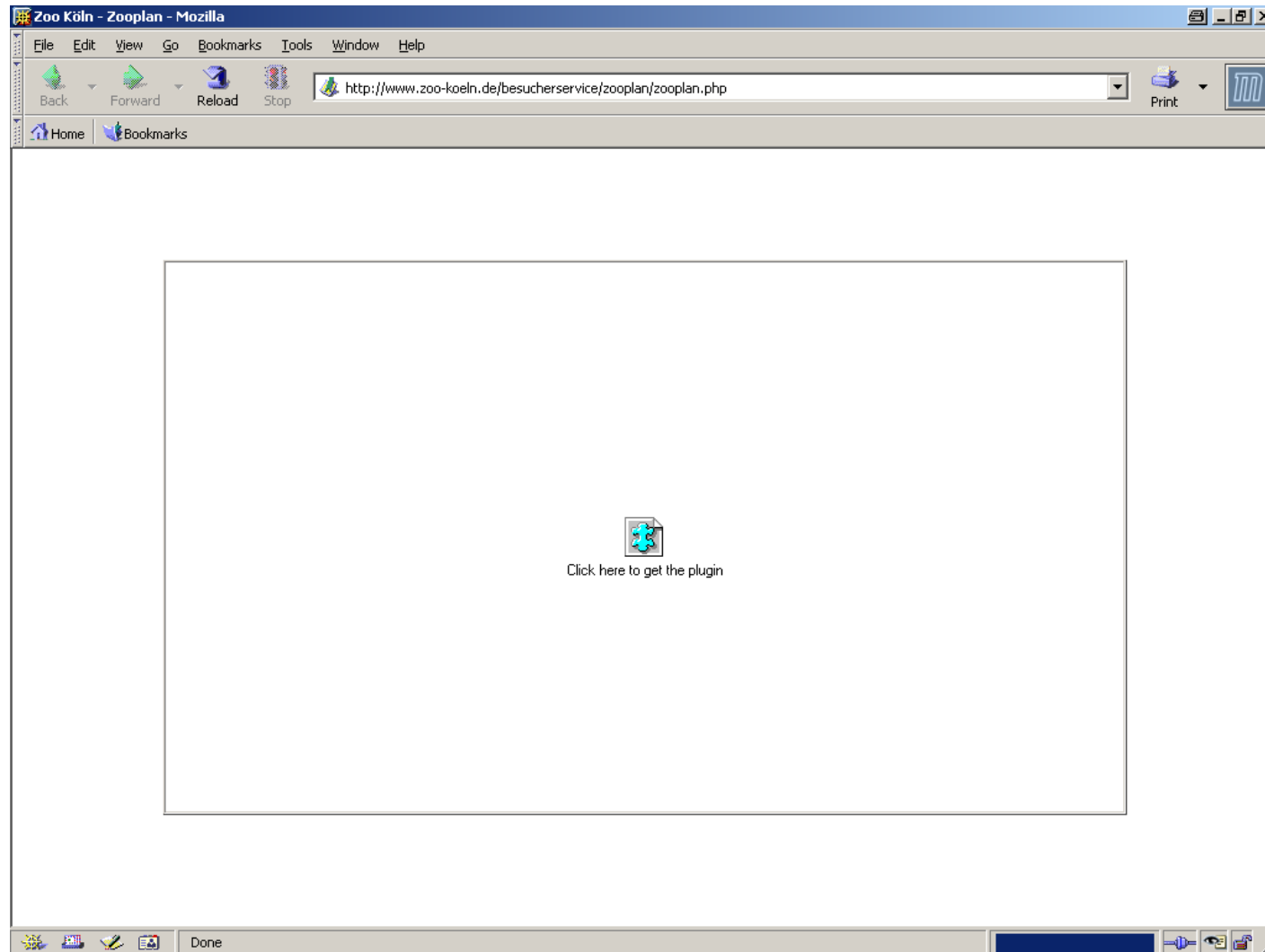
Für eine korrekte und optimale Darstellung benötigen Sie einen Browser mit aktiviertem Javascript und Cookies.

Vielen Dank!

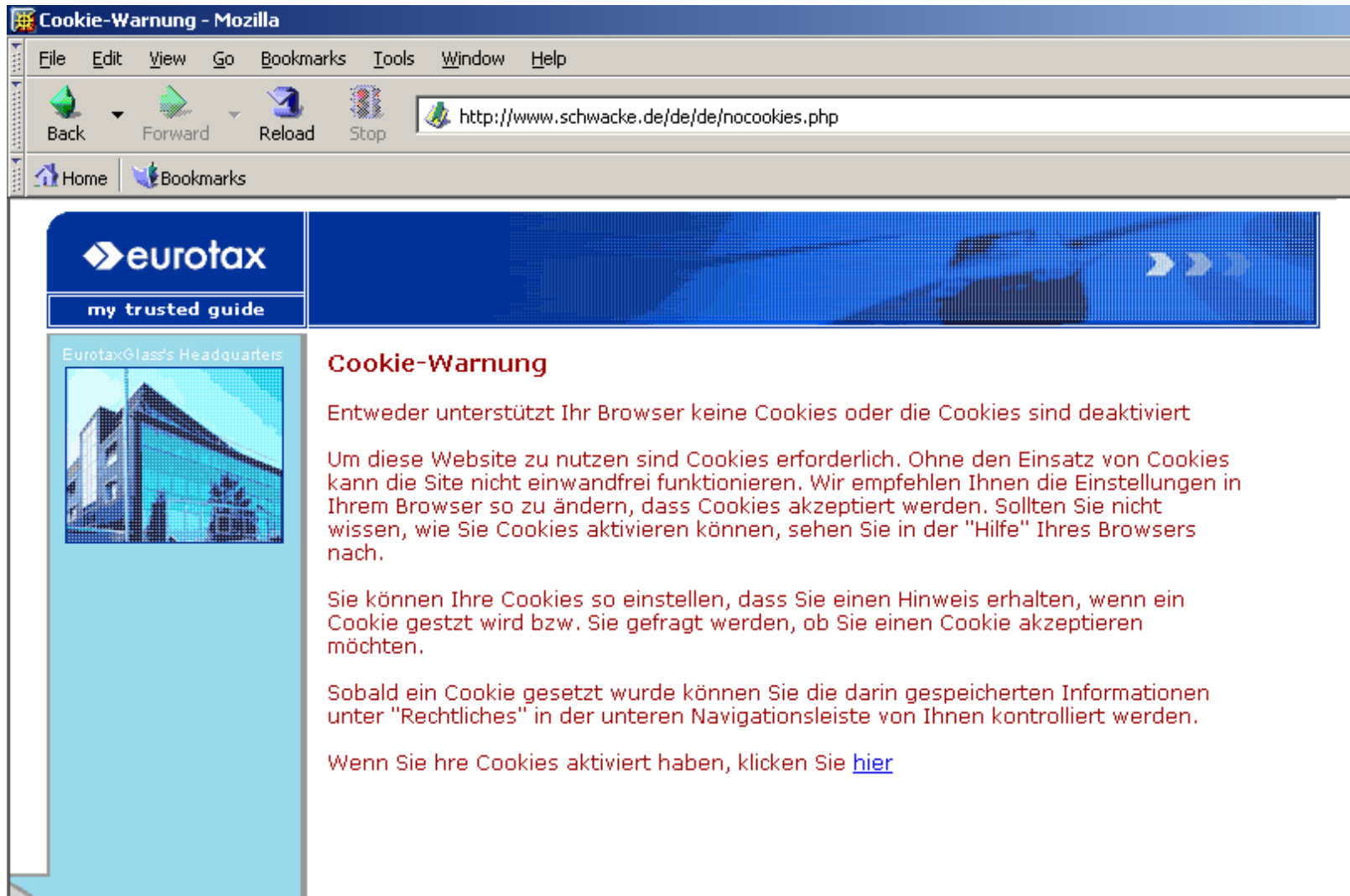
# Negativ: Keine Funktion ohne aktive Inhalte

The screenshot shows the homepage of 'DasTelefonbuch'. At the top left is the logo 'DasTelefonbuch. Alles in einem.' and at the top right is the 'info' logo. Below the logo is the text 'Für Deutschland.' and a search form with two tabs: 'Standard-Suche' (selected) and 'Detail-Suche'. The search form contains two input fields: 'Name\* / Suchwort' and 'Ort'. Below these is a 'Hilfe' button and a '\*Nachname / Firmenname' label. A 'Suchen!' button is at the bottom right of the form. To the right of the search form, there is a red box with white text that reads: 'Herzlich Willkommen - diese Website verwendet JavaScript! Sie benötigen einen Browser nach HTML 3.2 Standard, z. B. Netscape Navigator oder Microsoft Internet Explorer ab Version 4.0. Wenn Sie bereits einen dieser Browser verwenden, schalten Sie bitte JavaScript ein. Anschließend laden Sie diese Seite neu. Vielen Dank!' Below this message, there are three lines of text in German, French, and English, all providing the same information about the JavaScript requirement. At the bottom of the page, there are several links: 'Datenschutzhinweis', 'Häufig gestellte Fragen', 'Stellenmarkt', and 'Impressum'. The browser's taskbar is visible at the bottom of the screenshot.

# Negativ: Keine Funktion ohne Flash



# Negativ: Erzwungene Cookies



**Cookie-Warnung - Mozilla**

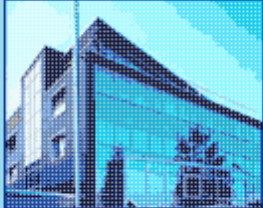
File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop <http://www.schwacke.de/de/de/nocookies.php>

Home Bookmarks

**eurotax**  
my trusted guide

EurotaxGlass's Headquarters



### Cookie-Warnung

Entweder unterstützt Ihr Browser keine Cookies oder die Cookies sind deaktiviert

Um diese Website zu nutzen sind Cookies erforderlich. Ohne den Einsatz von Cookies kann die Site nicht einwandfrei funktionieren. Wir empfehlen Ihnen die Einstellungen in Ihrem Browser so zu ändern, dass Cookies akzeptiert werden. Sollten Sie nicht wissen, wie Sie Cookies aktivieren können, sehen Sie in der "Hilfe" Ihres Browsers nach.

Sie können Ihre Cookies so einstellen, dass Sie einen Hinweis erhalten, wenn ein Cookie gesetzt wird bzw. Sie gefragt werden, ob Sie einen Cookie akzeptieren möchten.

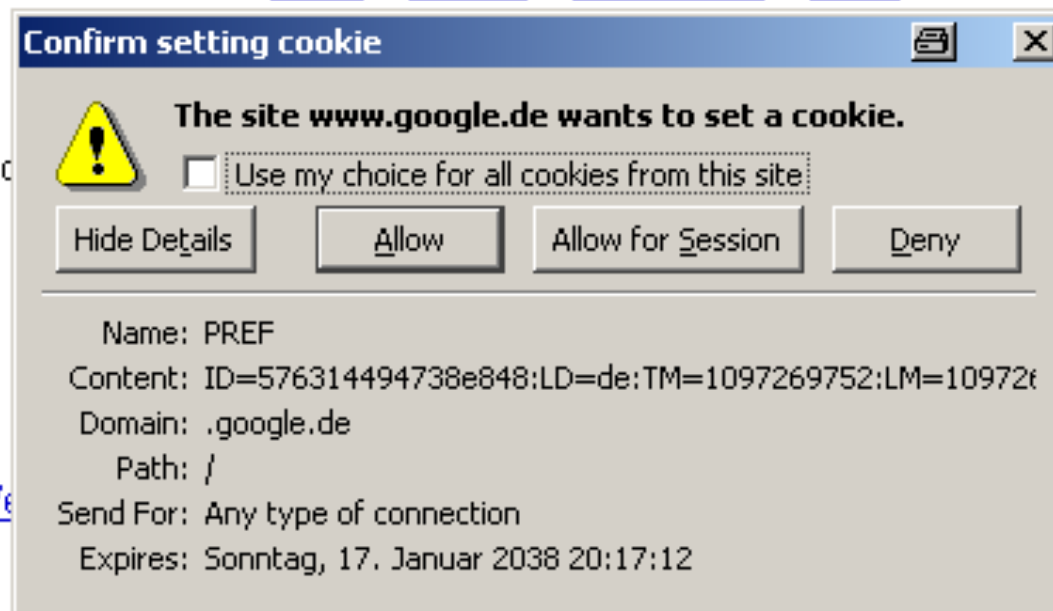
Sobald ein Cookie gesetzt wurde können Sie die darin gespeicherten Informationen unter "Rechtliches" in der unteren Navigationsleiste von Ihnen kontrolliert werden.

Wenn Sie Ihre Cookies aktiviert haben, klicken Sie [hier](#)

# Negativ: Cookies mit überlanger Lebensdauer



[Web](#) [Bilder](#) [Groups](#) [Verzeichnis](#) [News](#)



[Erweiterte Suche](#)  
[Einstellungen](#)  
[Sprachtools](#)

and

Suche

[Web](#)

[ish](#)

# Negativ: Formular ohne Quittung

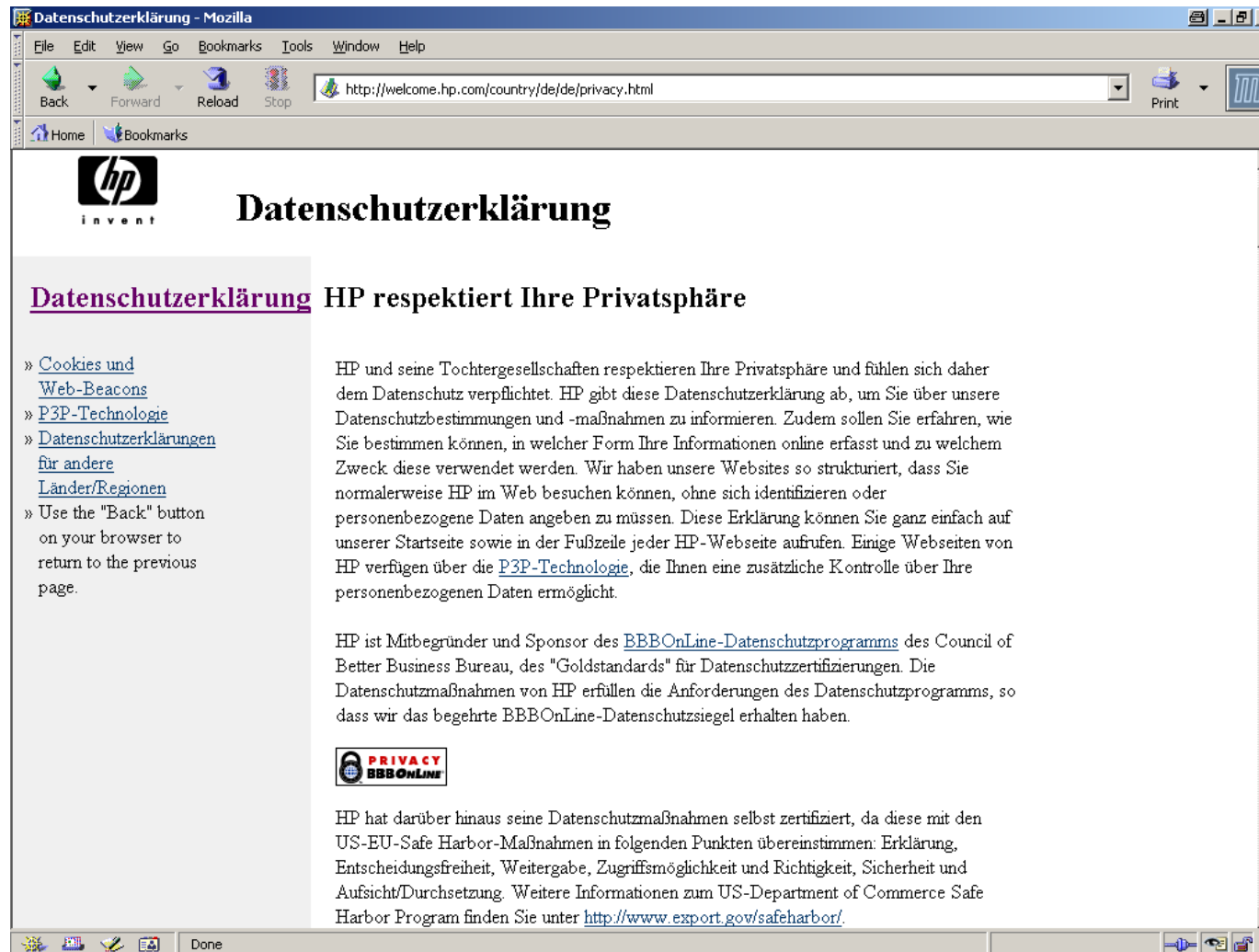
The screenshot shows a web browser window with the address bar containing the URL: `http://www.amazon.de/exec/obidos/handle-generic-form/028-6435075-6768509?action=next-page&target=stores/he`. The browser interface includes navigation buttons for Back, Forward, Reload, and Stop, as well as Home and Bookmarks buttons.

The main content area features a light green background with the heading "Schicken Sie uns Ihre Fragen oder Anmerkungen". Below the heading is the instruction: "Bitte füllen Sie das unten stehende Formular aus. Wenn Sie fertig sind, klicken Sie bitte auf 'Weiter'.".

The form itself is enclosed in a white box and contains the following fields:

- Ihr Name:** A text input field.
- Ihre E-Mail Adresse:** A text input field.
- Wichtig:** A note stating: "Bitte geben Sie die Ihrem Amazon.de-Konto zugehörige E-Mail-Adresse ein."
- Betreff:** A dropdown menu with the placeholder text "Bitte wählen Sie ein Thema aus."
- 17-stellige Bestellnummer:** A text input field with the label "(optional)" and an example: "(Beispiel: 028-1234567-1234567 oder 302-1234567-1234567)".
- Ihr Kommentar:** A large text area for providing feedback.

# Positiv: Aussagekräftige Datenschutzerklärung



The screenshot shows a Mozilla browser window titled "Datenschutzerklärung - Mozilla". The address bar contains the URL "http://welcome.hp.com/country/de/privacy.html". The page content includes the HP logo, the title "Datenschutzerklärung", and a sub-header "Datenschutzerklärung HP respektiert Ihre Privatsphäre". A sidebar on the left lists links: "Cookies und Web-Beacons", "P3P-Technologie", "Datenschutzerklärungen für andere Länder/Regionen", and "Use the 'Back' button on your browser to return to the previous page." The main text explains HP's commitment to privacy, mentioning their participation in the BBBOnLine-Datenschutzprogramm and their certification under the US-EU-Safe Harbor Program. A "PRIVACY BBBOnLINE" logo is displayed, and a link to "http://www.export.gov/safeharbor/" is provided for more information.

# Positiv: Datenbank alternativ ohne aktive Inhalte

Hotel Reservation Service (HRS) - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop http://www.hrs.de/

Home Bookmarks

**HOTEL RESERVATION SERVICE**  
seit 1972

AGB Über HRS Kooperationen Hilfe Jobs Impressum © HRS 1996 - 2004

**Hotel - Suche**  
**Einzelbuchung**

**Ändern**  
**Stornieren**

Gruppenbuchung  
Tagungs-Anfrage  
Tagung-Online24  
Messebuchung

Service für Firmen  
Service für Hotels

Werbung  
Presse  
Kontakt

Hotel-Profis unterstützen Sie:  
+49 (0)1805 - 477 000  
(0,12 € / Min. aus dem dt. Festnetz)  
Mo - Sa 7 - 24 Uhr  
So + Feiertage 8 - 22 Uhr

30 languages

**FINANCIAL TIMES**  
DEUTSCHLAND  
HRS mit 57,3% klarer Marktführer dt. Hotelportale  
( 7. Mai 2004 )

**HOTEL-SUCHE** →

**Online buchen - mit Sofortbestätigung...**

- ◆ in über 150.000 Hotels weltweit
- ◆ zu topaktuellen und garantiert besten HRS Preisen
- ◆ kostenlos buchen - auch ohne Kreditkarte
- ◆ Sie zahlen direkt im Hotel

# Positiv: Datenbank „ohne alles“ nutzbar

The screenshot shows the Deutsche Bahn website in a Mozilla browser window. The browser's address bar displays the URL `http://www.bahn.de/pv/view/index.shtml`. The website header features the Deutsche Bahn logo and a navigation menu with links for `Fahrpläne`, `Fahrkarten`, `Reisebüro`, `Angebote`, `Service`, `Int. Guests`, `Konzern`, and `Presse`. Below the header, there are links for `BahnShop 1435`, `Newsletter`, `Guided Tour`, `Sitemap`, `Kontakt`, and `FAQ`.

The main content area is divided into several sections:

- Reiseauskunft - Tickets:** A search form with fields for `von:`, `nach:`, `Datum:`, and `Uhrzeit:`. It includes radio buttons for `Abfahrt` and `Ankunft`, and a `Suchen` button.
- Knüllerpreise auf www.bahn.de:** A promotional banner for `Europa-Spezial-Preis` with a price of `39 EUR` for routes like `Amsterdam, Brüssel, Wien, Zürich`. It also features a `Surf&Rail` offer for `39 EUR` and a `Surf&Rail zum Festtagspreis` offer.
- Last Minute Tipps:** A list of offers including `Nordseeklima`, `Kultur & Shopping`, and `Sonne tanken`.
- Angebote, Fahrkarten, Reisebüro:** Three columns of links for various services like `BahnCard`, `Surf&Rail`, `Sparpreis 25 und 50`, `Schönes-Wochenende-Ticket`, `Länder-Tickets`, `Internationale Angebote`, `Hotels`, `Mietwagen`, `Urlaub mit eigener Anreise`, `Pauschalreisen`, `Last Minute`, and `Ferienhäuser`.
- Bahnurlaub:** A section for `Last Minute` offers, including `Attraktive Packages bis Mitte Dezember`.
- www.bahn.de präsentiert:** A promotional banner for `1200 FREI SMS` from `easy Credit`.

The footer of the browser window shows the `Done` status bar and various system icons.

# Webdesigner: Künstler oder Berater?

# Webdesigner: Künstler und Berater!

- „ Kunst, Ästhetik und Funktionalität brauchen keine unsicheren Techniken
- „ Kunden brauchen neben Funktionalität auch
  - „ Hohe Kundenakzeptanz
  - „ Legalität
  - „ Sichere Systeme
  - „ Vorsprung vor Mitbewerbern
  - „ Manche Kunden können (noch) nicht beurteilen, was das im einzelnen erfordert

Hier muss die Webdesignerin oder  
der Internetprogrammierer beraten

# Was sollte man tun und lassen? – Einige Highlights

## Auf jeden Fall

- „ Existierende Unternehmensrichtlinien ergründen
- „ Datenschutzbeauftragten ansprechen
- „ IT-Sicherheitsbeauftragten ansprechen
- „ Rechtsabteilung ansprechen
- „ Sich selbst über Datenschutz und IT-Sicherheit informieren
- „ Dem Kunden folgende Aspekte verdeutlichen und Entscheidungshilfen geben:
  - „ Datenschutz
  - „ Eigene IT-Sicherheit
  - „ IT-Sicherheit der Kunden

## Möglichst nie

- „ Aktive Inhalte ohne Alternativnutzungsmöglichkeit
- „ Cookies erzwingen
- „ Cookies mit langer Lebensdauer (vorzugsweise bis 2099;-))
- „ Impressum und Datenschutzerklärung verstecken
- „ Formulare mit unnötigen Pflichtfeldern („bevor wir nicht Ihre Hutgröße kennen, reden wir nicht mit Ihnen“)
- „ Nichtssagende „Datenschutzerklärung“ („Wir verarbeiten nur im Rahmen des BDSG“)
- „ Kontaktformulare ohne Quittung (Kopie an Absender)
- „ „Stöbern“ in Online-Shops unmöglich ohne sofortiges, personalisiertes Login

# Nützliche Links und Bücher

- „ Virtuelles Datenschutzbüro: [www.datenschutz.de](http://www.datenschutz.de)
- „ Deutsche Vereinigung für Datenschutz: [www.datenschutzverein.de](http://www.datenschutzverein.de) (für Neugestaltungsvorschläge dankbar!)
- „ Zeitschrift Datenschutz und Datensicherheit: [www.dud.de](http://www.dud.de)
  
- „ Bundesamt für die Sicherheit in der Informationstechnik: [www.bsi.de](http://www.bsi.de)
  
- „ Webimpressum-Assistent: [www.digi-info.de/de/netlaw/webimpressum/index.php](http://www.digi-info.de/de/netlaw/webimpressum/index.php)
- „ OECD-Generator für Datenschutzerklärungen: [www.oecd.org](http://www.oecd.org)
- „ B.A.T. Studien (Prof. Opaschowski): [www.bat.de](http://www.bat.de)
  
- „ Huseby, Innocent Code – a security wake-up call for web programmers, John Wiley & Sons, 2004 (sehr empfehlenswert!)
- „ Schaar, Datenschutz im Internet, C.H. Beck, 2002
- „ Consumers International, [Privacy@net](http://www.privacyatnet.org) - An international comparative study of consumer privacy on the internet, 2001, ISBN 19023 91 31 68
  
- „ ...

# Kontakt Daten

Karin Schuler  
Datenschutz und IT-Sicherheit  
Kronprinzenstr. 76  
53173 Bonn  
0228/24 20 733

[Schuler@datenschutzverein.de](mailto:Schuler@datenschutzverein.de)