Digitale Gegenwehr für Verbraucher – rechtliche und technische Hintergründe

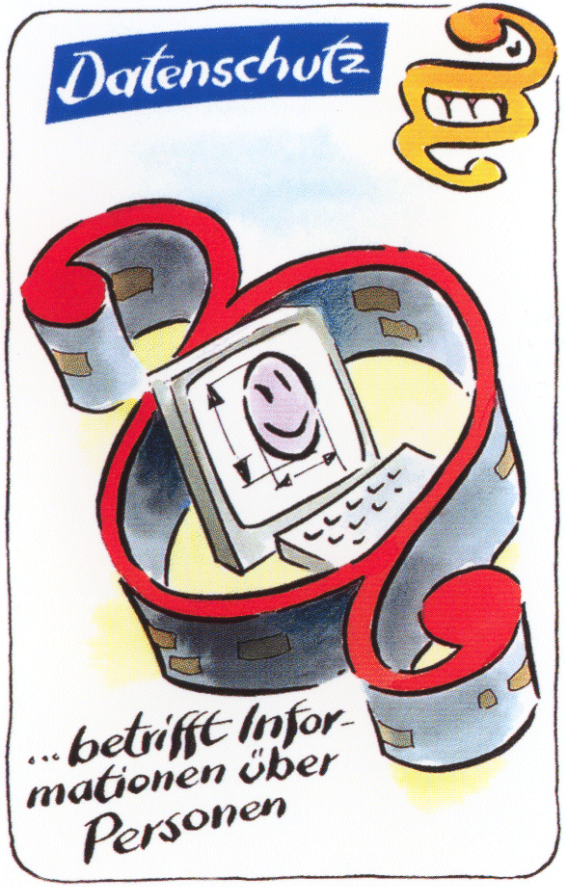
Sommerakademie 2019

Infobörse 5

Christian Krause, Henry Krasemann

Unabhängiges Landeszentrum für Datenschutz

Die Grundidee des Datenschutzrechts



ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Das Ideal

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****.*

Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

(Bundesverfassungsgericht 65,1 – Volkszählung)

Zweck der DSGVO

Zweck der DSGVO: Art. 1:

> Diese Verordnung enthält Vorschriften zum **Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten** und zum freien Verkehr solcher Daten.
>
> Diese Verordnung **schützt die Grundrechte und Grundfreiheiten natürlicher Personen** und insbesondere deren Recht auf Schutz personenbezogener Daten.

Sechs Goldene Regeln des Datenschutzes (vgl. Art. 5 DSGVO)

- Rechtmäßigkeit
  - Gesetz, Einwilligung, Vertrag, Dienst- oder Betriebsvereinbarung
- Zweckbindung
  - Verwendung nur für Erhebungszweck
- Datenminimierung und Speicherbegrenzung
  - Verarbeitung nur soweit für Erhebungszweck erforderlich
- Transparenz und Betroffenenrechte
  - Unterrichtung über Verwendung, Auskunfts-/Berichtigungs-/Löschrechte
- Datensicherheit und Richtigkeit
  - Technische und organisatorische Maßnahmen, Integrität und Vertraulichkeit
- Kontrolle
  - Interner / externer Datenschutzbeauftragter; Audit

Art. 6 DSGVO: Zentrale Befugnisnorm

- Datenverarbeitung ist nur (!) rechtmäßig, wenn:
  - **Einwilligung**
  - **Vertragserfüllung**
  - **Erfüllung rechtlicher Verpflichtung**
  - Lebenswichtige Interessen
  - Ausübung öffentliche Gewalt
  - **Wahrung berechtigter Interessen (sofern Interessen des Betroffenen nicht überwiegen)**

Selbsthilfe – Was ist zulässig?

- 8. Gebot: „Du sollst nicht falsch Zeugnis reden wider deinen Nächsten.“

- Wilhelm Busch: „Wer dir sagt, er hätte noch nie gelogen, dem traue nicht, mein Sohn!“

Früher war alles besser ™

- Ein Buch kaufen
- Ein Buch lesen
- Im Lexikon blättern
- Telefonieren
- Fernsehen
- Einkaufsbummel in der Stadt

Selbstschutz vor wem?

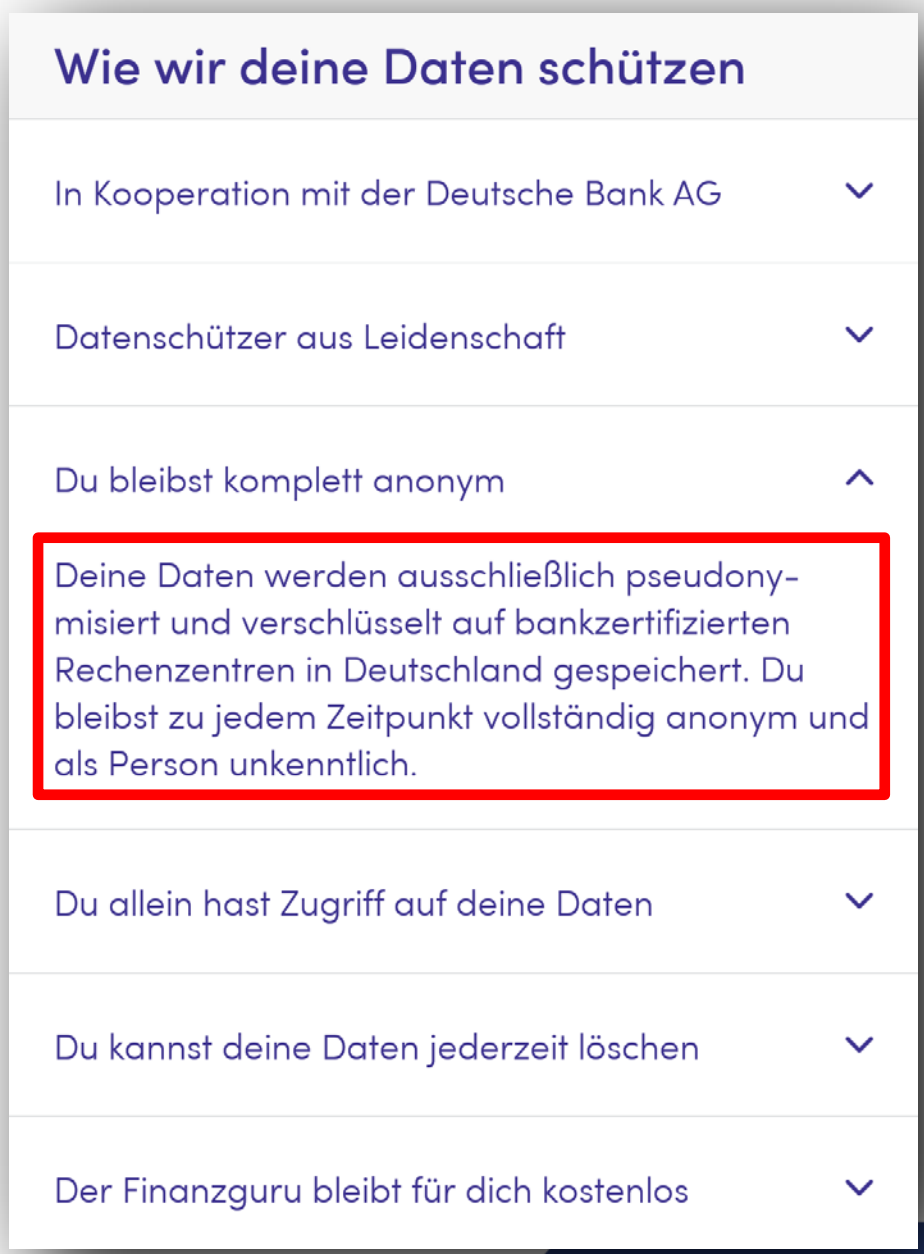
- Früher: Generelle, unspezifische Gefahrenlage
- Schutz vor dem Staat & „Hackern“ Lösung: z. B. Anonymisierungsdienste

- Heute: Individuelle Bedrohung
- Schutz vor Profiling / Scoring / Targeting des Diensteanbieters und eingebundener anderer Dienste (Soziale Netzwerke, Werbenetzwerke, Targetingdienste etc.)

Machtgefüge

- Organisation (privat und öffentlich) muss sich an das Datenschutzrecht halten (insbesondere DSGVO)
- Art. 25 Abs. 1 DSGVO: Technische und organisatorische Maßnahmen müssen zur Erfüllung der Datenschutzgrundsätze umgesetzt werden
  - Beispiel: Pseudonymisierung

Die App „Finanzguru“



- Pseudonym? Anonym? Was denn nun?

Nutzerseitige Pseudonyme

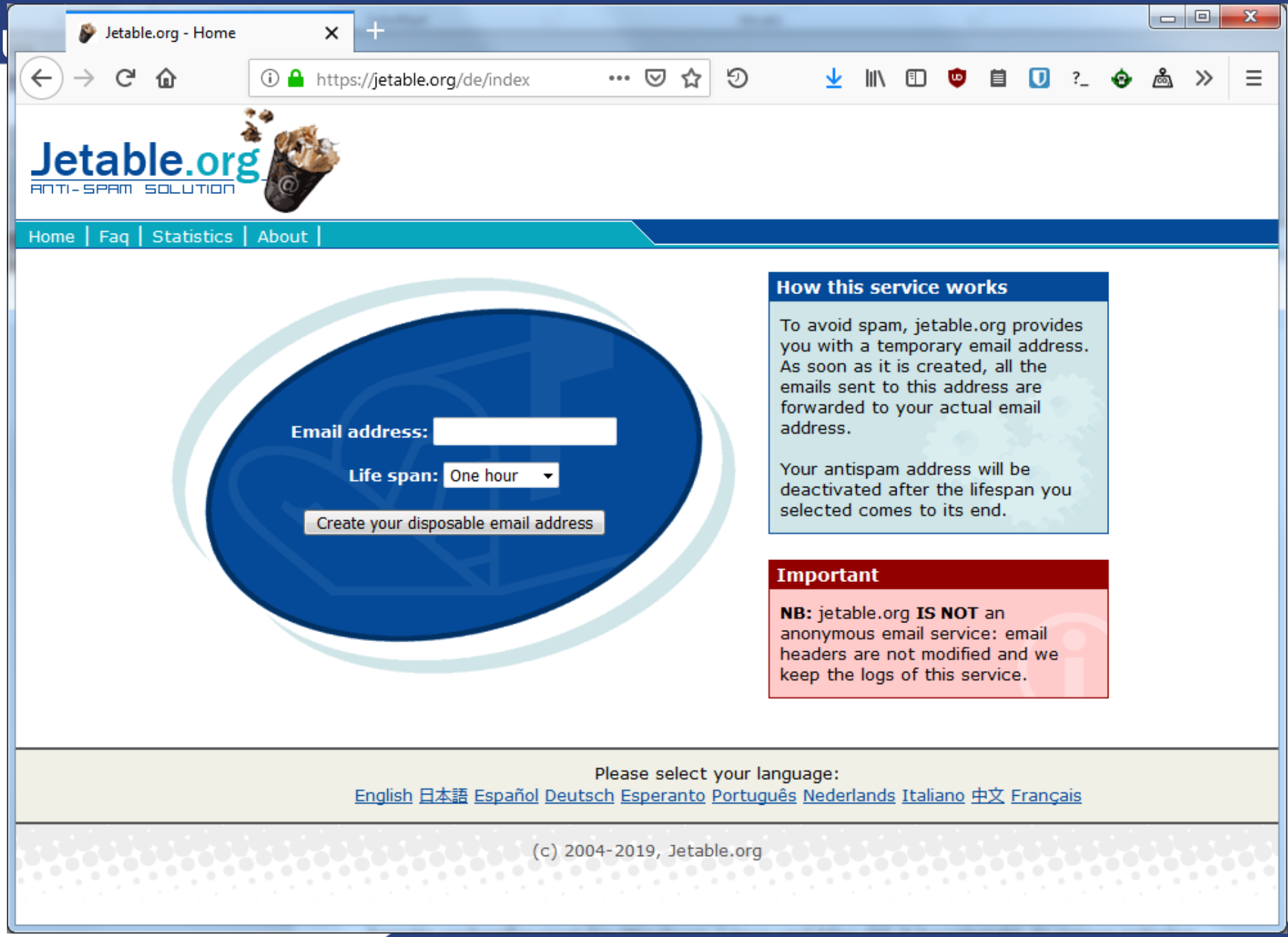
- Identität ist relativ:
  - Nutzungskontext erfordert stets ein Subset an Identitätsmerkmalen, nie alle auf einmal.
  - Synonyme Merkmale können alternativ verwendet werden.
  - E-Mail-Adressen sind dazu gut geeignet, mehrere zu haben ist nicht schwer.
  - Telefonnummern nicht so sehr
    (wenig überraschend geht der Trend bei Anbietern zu letzterem Identifier…)
  - Es ist eine gute Idee, verschiedene Identitäten zu pflegen — schließlich würde man dem Bäcker auch nicht seine Krankengeschichte mitteilen

Falsche Angaben machen

- Darf ich Selbsthilfe üben und selber pseudonymisieren?
- Zulässig:
  - Wenn keine Daten Dritter dadurch weiter gegeben werden
    - Phantasiedaten / Pseudonyme / Allerweltsdaten
  - Keine sonstigen Pflichten (Gesetze / Verträge etc.)

„echte“ Pseudonyme

- Verschiedene E-Mail-Adressen für verschiedene Zwecke
- Eine SIM-Karte und ein altes Handy in der Schublade sind etwas aufwändiger, erfüllen aber den gleichen Zweck:
  - Erstellung eines pseudonymen Identifikationsmerkmals, dass einerseits Verkettung erschwert, andererseits keine Flucht vor rechtlicher Zurechenbarkeit darstellt


Jetable.org - Home
https://jetable.org/de/index
Jetable.org
ANTI-SPAM SOLUTION
Home | Faq | Statistics | About |
Email address:
Life span: One hour
Create your disposable email address
How this service works
To avoid spam, jetable.org provides you with a temporary email address. As soon as it is created, all the emails sent to this address are forwarded to your actual email address.
Your antispam address will be deactivated after the lifespan you selected comes to its end.
Important
NB: jetable.org IS NOT an anonymous email service: email headers are not modified and we keep the logs of this service.
Please select your language:
English 日本語 Español Deutsch Esperanto Português Nederlands Italiano 中文 Français
(c) 2004-2019, Jetable.org

Falsche Angaben machen

- Unzulässig:
  - Verwendung von Daten eines existierenden Dritten (zumindest mittelbar zuordenbar)
  - Betrug (z. B. bei Zahlungsverpflichtungen)
  - § 269 StGB: Fälschung beweiserheblicher Daten
    - Beinhaltet eine unmittelbar rechtserhebliche Erklärung
  - Verstoß gegen Urheberrechtsvereinbarungen
  - Verstoß gegen vertragliche Regelungen

Beispiele

- Falsches Geburtsdatum i.d.R. zulässig
  - Ausnahme ggf.: Alter relevant (z. B. „ab 18“)
- Newsletter-Anmeldung: i.d.R. Fantasiedaten zulässig
- Probemonat Softwarenutzung: kommt darauf an
  - Ggf. Lizenzvertrag vereinbart, der auf eine Person beschränkt ist oder auf Privatpersonen
- Internetbestellung (kostenpflichtig): i.d.R. Echtdaten erforderlich
- Internetbestellung kostenlos: i.d.R. Fantasiedaten zulässig
  - Ggf. vertragliche Regelungen beachten

Beispiele

- Anmeldung Handelsplattformen (eBay etc.) mit falschen Personalien: i.d.R. unzulässig

- Falsche Angaben im Impressum / Datenschutzerklärung einer Webseite: unzulässig

Nutzungsdaten

- Auch pseudonym Nutzende erzeugen und hinterlassen Daten.

- IP-Adressen
- Cookies
- Link-IDs
- Im OS erzeugte Ids
- In Browser-AddOns, Programmen und Apps erzeugte IDs

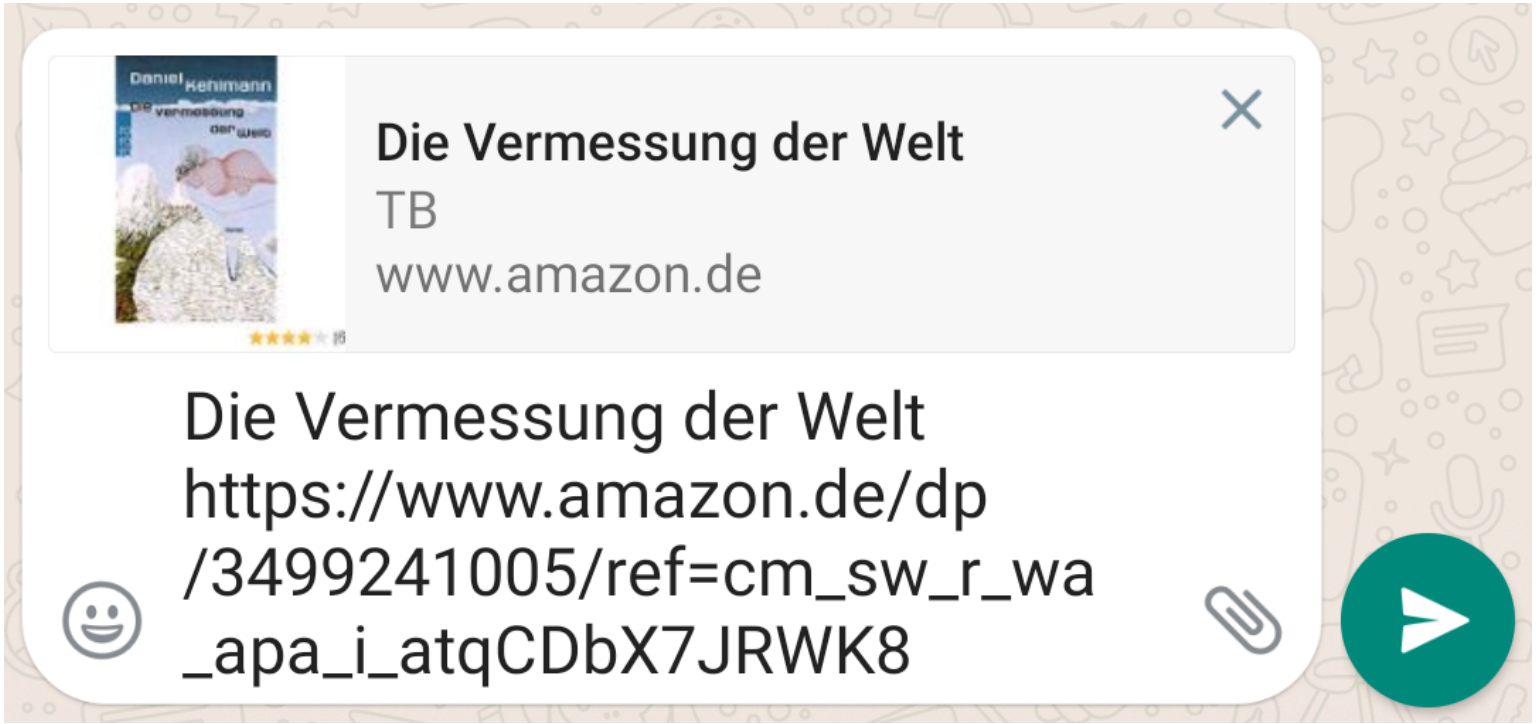
Trennung von identifizierenden Merkmalen

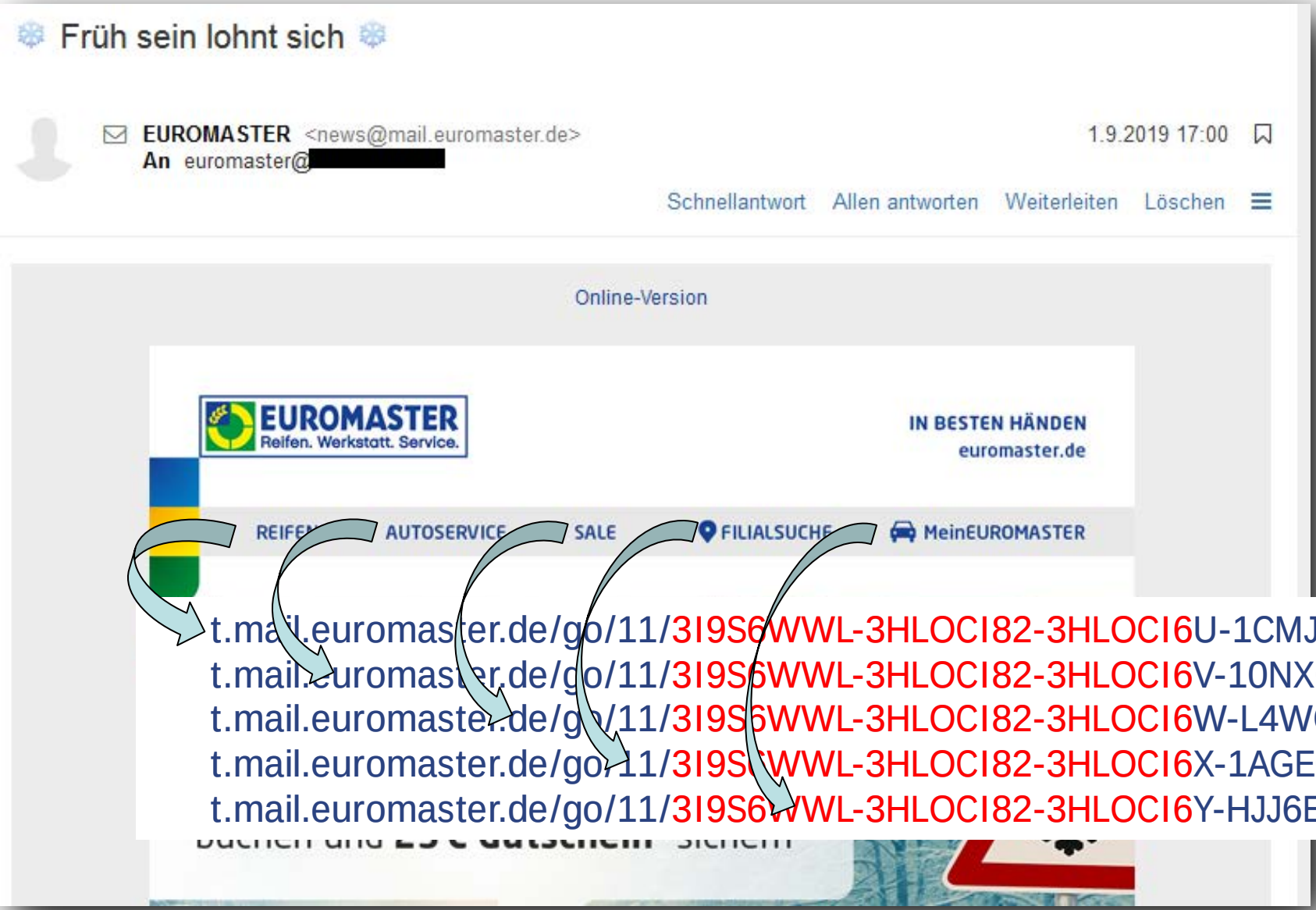
- **Verschiedene Browser**, je nach Kontext:
  Bspw. Firefox zum Surfen, Chrome für Soziale Netzwerke

- **Browser statt App**:
  Da Nutzende idR in der App angemeldet sind, kann dort jede Aktion protokolliert werden

Erzeugter Link in der Amazon-App – Ohne aktive Teilnahme am Referer-Programm

- Die Produkt-ID ist 3499241005. Alles danach ist „Referer“, der dem Empfehlenden eventuell Geld, Amazon aber auf jeden Fall Informationen liefert:




Früh sein lohnt sich
EUROMASTER <news@mail.euromaster.de>
An euromaster@[redacted]
1.9.2019 17:00
Schnellantwort Allen antworten Weiterleiten Löschen
Online-Version
EUROMASTER
Reifen. Werkstatt. Service.
IN BESTEN HÄNDEN
euromaster.de
REIFEN AUTOSERVICE SALE FILIALSUCHE MeinEUROMASTER
t.mail.euromaster.de/go/11/3I9S6WWL-3HLOCI82-3HLOCI6U-1CMJVJX.html
t.mail.euromaster.de/go/11/3I9S6WWL-3HLOCI82-3HLOCI6V-10NXOOJ.html
t.mail.euromaster.de/go/11/3I9S6WWL-3HLOCI82-3HLOCI6W-L4WCL0.html
t.mail.euromaster.de/go/11/3I9S6WWL-3HLOCI82-3HLOCI6X-1AGEQBY.html
t.mail.euromaster.de/go/11/3I9S6WWL-3HLOCI82-3HLOCI6Y-HJJ6EN.html

Lokale GUIDs

- GUIDs machen Nutzende für eine unbekannte Zahl dritter wiedererkennbar.
- IDs, die installierte Programme erzeugen

- IDs, die Betriebssysteme vergeben
  - Werbe-ID
  - Device-ID

Kaspersky Antivirus Software Exposed Millions to Web Tracking

By Paul Wagenseil 22 days ago Security

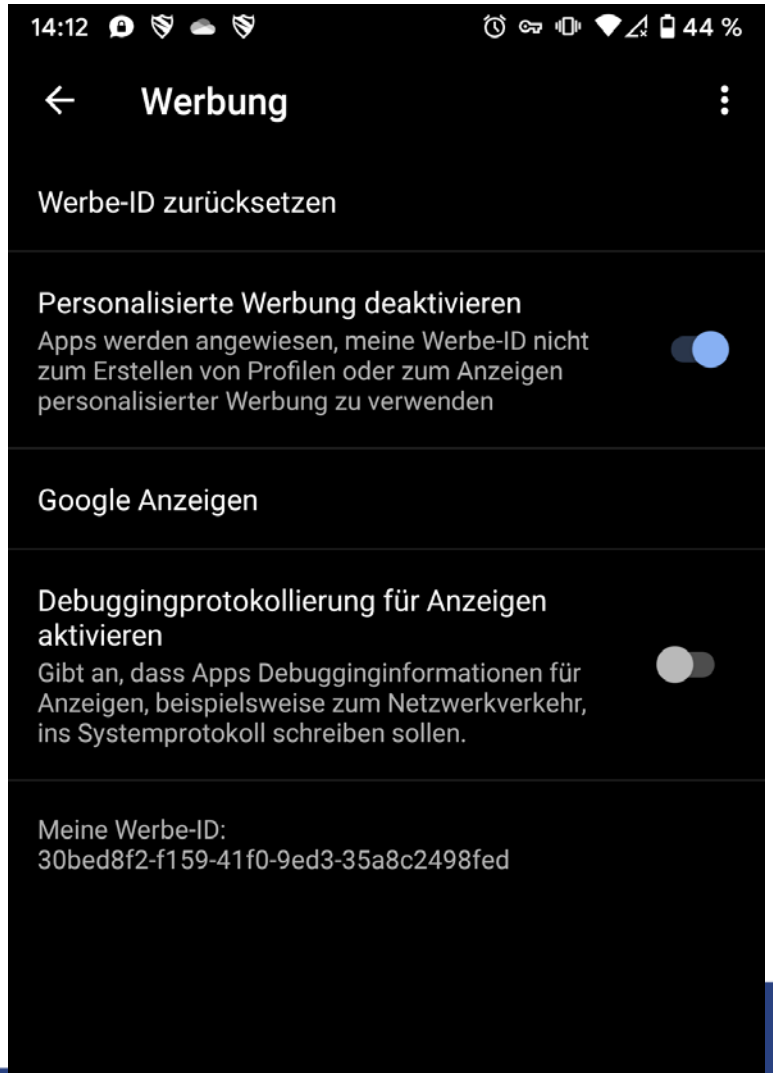
Program injected JavaScript, unique IDs into web pages

Eugene Kaspersky on stage at Mobile World Congress 2017, Barcelona.

(Image credit: catwalker/Shutterstock)

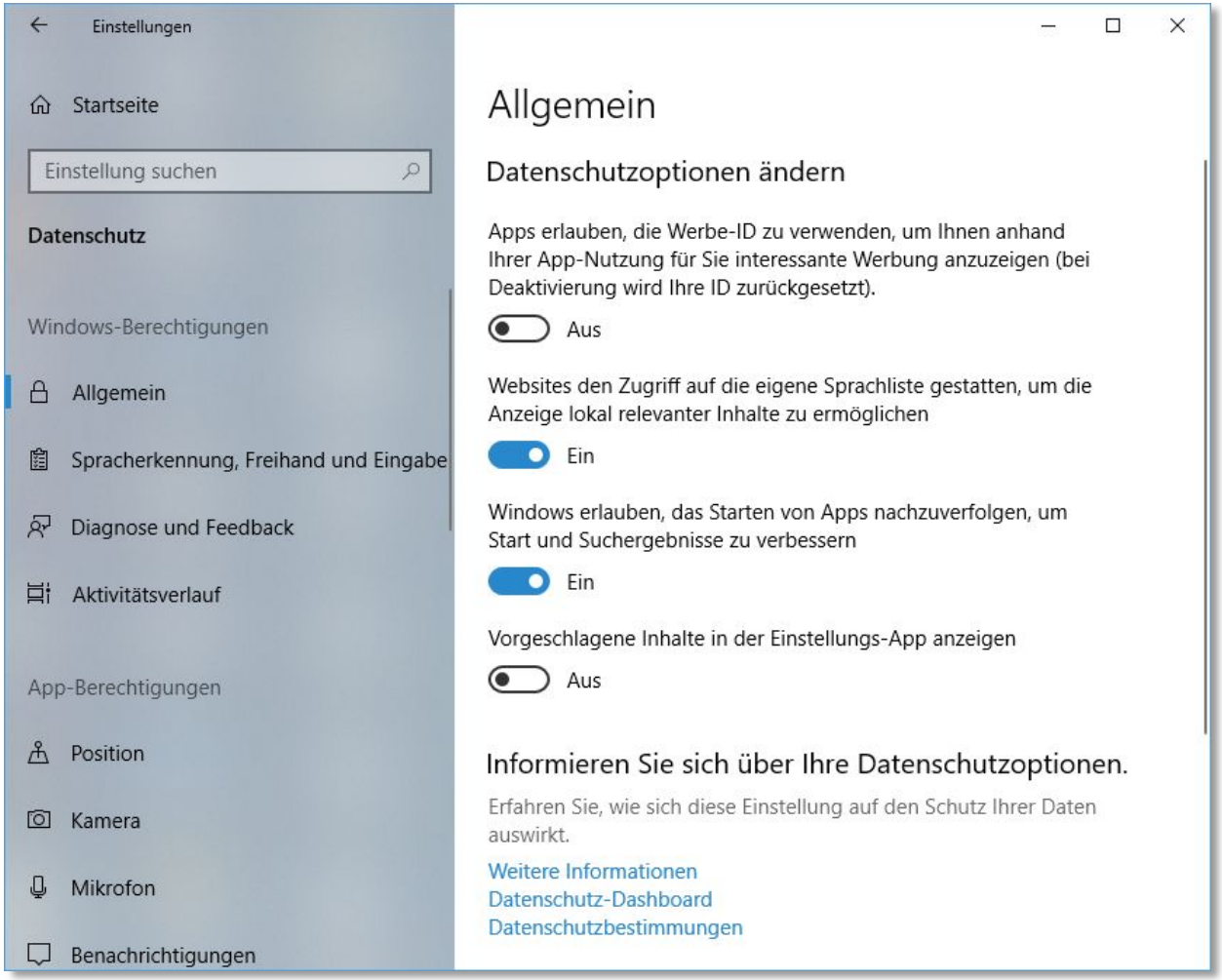
Werbe-ID

- Neu setzen bzw. Deaktivieren unter Android und iOS



Werbe-ID

- Deaktivieren unter Windows



Werbung und Datenschutz: Von der Freiwilligkeit der Einwilligung…

Thanks for downloading Paper.io 2

Voodoo attaches great importance to respect for privacy and the use of your personal data.

With your consent, we collect data via this application including your advertising identifiers and your IP address (usually provisional).

These data are collected via external tools (SDK) implemented by our partners, as detailed in our **Privacy Policy**, which are an integral part of the application.

I certify that I'm over the age of fifteen, have read, understood and accepted Voodoo's Privacy Policy.

I agree to play for free and that my personal data is collected via the SDK tools built into the application.

Start playing

Learn more

Are you sure?

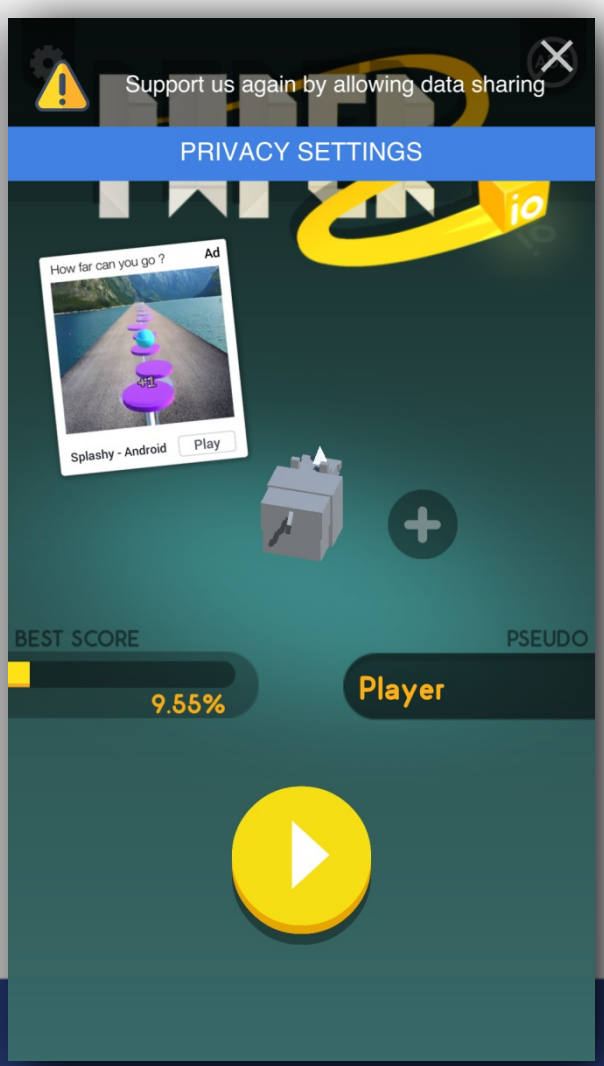
If you do not wish to share your data to be used as described in our Privacy Policy, you will continue to access an alternate version of the game including:

- Larger volume of non-targeted advertising
- An information banner informing you of your consent decision

You can change this setting via the application at any time.

Go back and fix my settings

I understand and confirm



Geteilte Daten sind doppelte Daten

- Unter Android existieren SDKs, die Daten in Bereichen speichern, auf die andere Apps Zugriff haben. Sie unterlaufen so jegliches Berechtigungskonzept.[1]
- Berechtigungen, die eine App legitimerweise hat, können so von einer anderen App zum Abfluss von Daten missbraucht werden.

[1] 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System
https://uldsh.de/xgsqj5

DNS Tracking

- Das Domain Name System dient der Auflösung von merkbaren Namen in IP-Adressen
- Mindestens der erste Aufruf einer Domain erzeugt eine Abfrage beim zuständigen DNS-Server

→ DNS-Server erhält umfangreiche Informationen über Nutzungsaktivität

→ DNS-Betreiber besitzt Kontrolle über Erreichbarkeit von Inhalten – nämlich ob und welche Inhalte angezeigt wird.

TRR: Trusted Recursive Resolver

- Applikationen wie Mozilla Firefox bringen eigene DNS-Einstellungen mit und überschreiben u.U. die DNS-Parameter des Betriebssystems.
- → Protest in GB wegen Unterlaufens staatlicher Zugriffsbeschränkungen

→ DNS bedeutet Kontrolle. Nutzende sollten zumindest WISSEN, wer diese Kontrolle gerade hat.

ZDNet / Workspace

Firefox: DNS-over-HTTPS (DoH) sorgt für Kritik in Großbritannien

Britische Internet Service Provider bezeichnen Mozilla wegen der Unterstützung von DNS-over-HTTPS (DoH) in Firefox als "Internet-Schurken". Zuvor hatten auch britische Behörden den Browserhersteller wegen der Einführung von DoH kritisiert.

von Kai Schmerer am 8. Juli 2019 , 09:12 Uhr

Werbeblocker

- Werbung wird online nahezu immer von Trackingmaßnahmen begleitet.
- Solange das so ist:
  Werbeblocker = Trackingblocker = datenschutzfreundlich
- Mögliche Probleme:
  - Nicht nutzbare Angebote
  - „Overblocking“
  - Filterlisten effektiv nicht von Nutzenden kontrollierbar

Filterlisten: Das Aber...

- Filterlisten (die bspw. in Werbeblockern eingesetzt werden) sind zumeist fremdbestimmt,
- DNS-Server sind idR fremdbetrieben.

- Eventuell treibt man hier
  den Teufel mit dem Beelzebub aus...

Vielen Dank!

Noch Fragen?

mail@datenschutzzentrum.de
Tel. 0431-988 1200

www.datenschutzzentrum.de