Privacy on the Web:
Hilft mehr Transparenz, den Datenschutz zu verbessern?

Prof. Dr. Dominik Herrmann · Otto-Friedrich Universität Bamberg
LSt Privatsphäre und Sicherheit in Informationssystemen
https://herdom.net · @herdom

Grundsatz der Transparenz

Erwägungsgrund 58 DSGVO

… dass eine … Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist.

Dies gilt insbesondere für Situationen, wo die große Zahl der Beteiligten und die Komplexität der … Technik es … schwer machen, … nachzuvollziehen, ob, von wem und zu welchem Zweck … personenbezogene Daten erfasst werden …

Transparenz i.S.d. DSGVO
ist auf vielen Webseiten … ausbaufähig.

Beispiel 1

„Mit der Teilnahme akzeptieren Sie die Datenschutzrichtlinien von WebEx.“

Benachrichtigen der Benutzer über Optionen bei der Konvertierung in Ihre Organisation

Wenn Sie einen Benutzer von einer Verbraucherorganisation in Ihre Unternehmensorganisation konvertieren, wird der Benutzer benachrichtigt und hat 14 Tage Zeit, um zu entscheiden, ob seine vorhandenen Inhalte privat bleiben oder er Ihrer Organisation beitritt.

- Wenn der Benutzer sich dafür entscheidet, seinen bestehenden Inhalt privat zu halten, ändert er die E-Mail-Adresse, die er mit der App verwendet, und es wird ein neues Konto für ihn in Ihrer Organisation erstellt.
- Wenn der Benutzer Ihrer Organisation beitritt, wird Ihre Organisation zum Eigentümer aller Teams, Bereiche oder Inhalte, die vom Benutzer in der App erstellt wurden. Die Aufbewahrungsrichtlinie Ihrer Organisation gilt für alle Inhalte, die sie erstellen. Wenn Sie die Active Directory verwenden, müssen Sie den Benutzer auch zu Ihrer Organisation Active Directory.

Wenn der Benutzer nach 14 Tagen keine Wahl getroffen hat, wird er automatisch in Ihre Organisation verschoben.

„Mit der Teilnahme akzeptieren Sie die Datenschutzrichtlinien von WebEx.“

Benachrichtigen der Benutzer über Optionen

Wenn Sie einen Benutzer von einer Verbraucherorganisa
Benutzer benachrichtigt und hat 14 Tage Zeit, um zu ent
Organisation beitritt.

- Wenn der Benutzer sich dafür entscheidet, seinen
  die er mit der App verwendet, und es wird ein neu
- Wenn der Benutzer Ihrer Organisation beitritt, wird
  Inhalte, die vom Benutzer in der App erstellt wurde
  die sie erstellen. Wenn Sie die Active Directory ver
  Active Directory.

Wenn der Benutzer nach 14 Tagen keine Wahl getroffen

War dieser Artikel hilfreich für Sie?

Ja, vielen Dank!

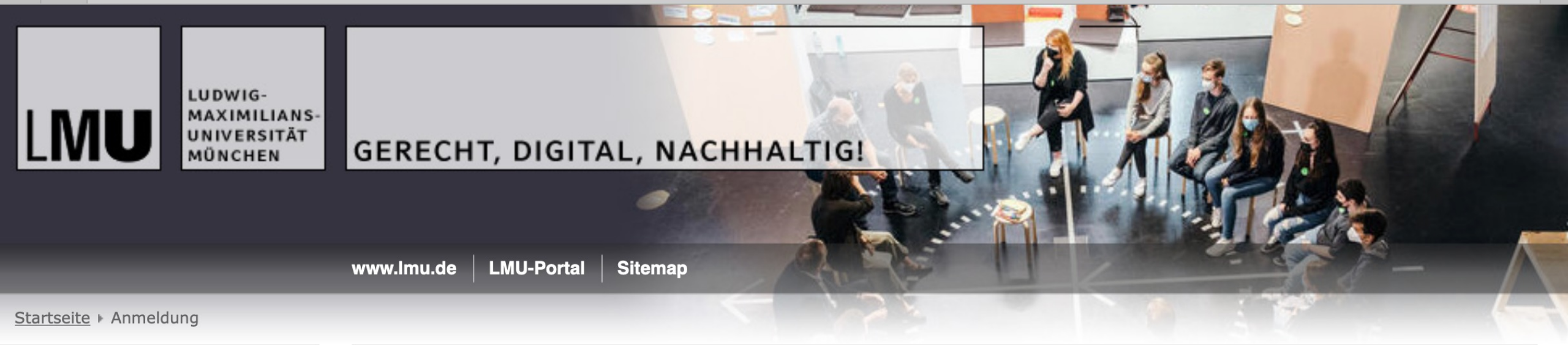
Eigentlich nicht

Was haben wir nicht so gut gemacht?

- ○ Mir gefällt nicht, wie das Produkt funktioniert.
- ○ Ich fand die Anweisungen oder Erläuterungen in dem Artikel verwirrend.
- ○ Dieser Artikel hat meine Fragen nicht beantwortet oder meine Probleme nicht gelöst.
- ◉ Sonstiges

Transparenz i.S.d. DSGVO
ist auf vielen Webseiten … ausbaufähig.

Beispiel 2



CALL FOR PAPERS
SPEAKER
PROGRAMM
ANMELDUNG
KONTAKT

drucken

Anmeldung

Kategorie	Anzahl
Vor-Ort Ticket	Nicht mehr verfügbar
Online-Ticket	1

* inkl. gesetzl. MwSt.

Weiter

2 Käufer- und Ticketdaten

3 Überprüfen und bestellen

Persönliche Daten

Vereinfachen Sie Ihre Bestellung: ⓘ

Mit XING einloggen

Vorname *

Nachname *

Firma

E-Mail *

Passwort ⓘ

☐ Ich akzeptiere die AGB und habe die Datenschutzerklärung der New Work SE zur Kenntnis genommen *

Weiter

Art. 12 (1) DSGVO

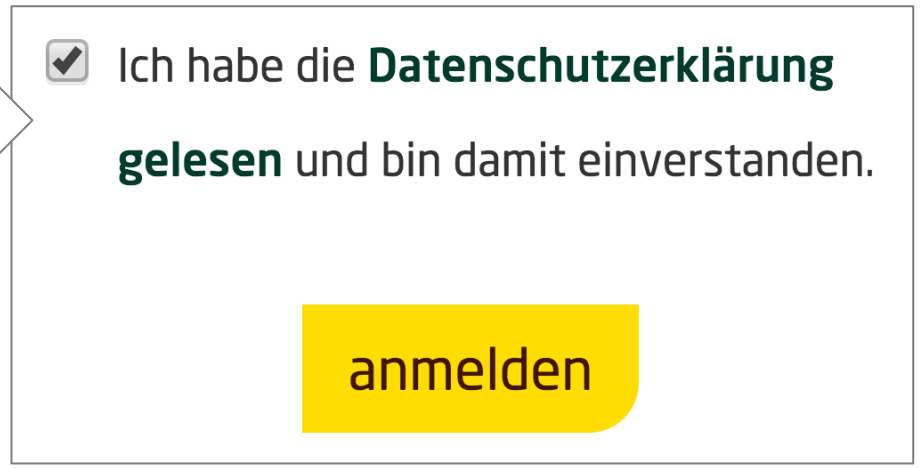
90% unverständlich

86% zu lang

[…] in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln

warum?

Hier wird oft gelogen…



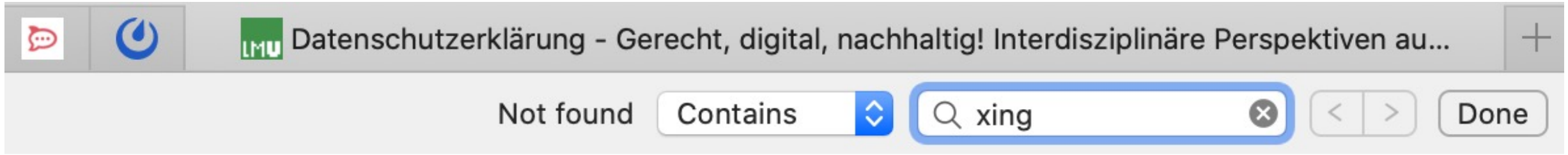
Bitkom Research (2015): https://www.bitkom.org/Presse/Presseinformation/Internetnutzer-gehen-pragmatisch-mit-Datenschutz-um.html

Mai 2017 Mai 2018

4360 Wörter

6358 wörter

Beispiel: **Facebook**



Datenschutzerklärung

Allgemeine Datenschutzerklärung für die Internetseiten der Ludwig-Maximilians-Universität München (im Folgenden „LMU“)

I. Kontaktinformationen im Zusammenhang mit dem Internetauftritt der LMU

mehr als 5200 Wörter

2. Informationen, die Du uns mitteilst.

Dies sind Daten, die wir direkt von Dir erhalten und Informationen, die Du auf XING Websites veröffentlichst oder versendest, beispielsweise:

- Zugangsdaten (z. B. Nutzername und Passwort)
- Profildaten (z. B. Jobtitel, Firmenname, Branche, Ausbildung, Kontaktmöglichkeiten, Foto)
- Nachrichten, Gruppenbeiträge, Eventteilnahmen, Zahlungsdaten

> Mehr erfahren

3. Automatisch auf Grund Deiner Nutzung von XING gesammelte Informationen

Während Du den Dienst XING nutzt oder besuchst, werden automatisch Daten von Dir mittels Tracking gesammelt. Hier erfährst Du,

- wie das Tracking geschieht,
- warum Tracking eingesetzt wird (Gewährleistung der Sicherheit, Bereitstellung unseres Dienstes, Erfolgsmessung und Optimierung von Werbung sowie Ermittlung statistischer Kennwerte).

> Mehr erfahren

Datenschutzerklärung (Druckversion)

Allgemeine Hinweise

Wie werden Deine personenbezogenen Daten verarbeitet?

1. Allgemeines zu den Zwecken der Datenverarbeitung.

2. Informationen, die Du uns mitteilst.

3. Automatisch auf Grund Deiner Nutzung von XING gesammelte Informationen

4. Informationen, die wir über Dich aus anderen Quellen erhalten.

5. Wer erhält Daten zu Deiner Person?

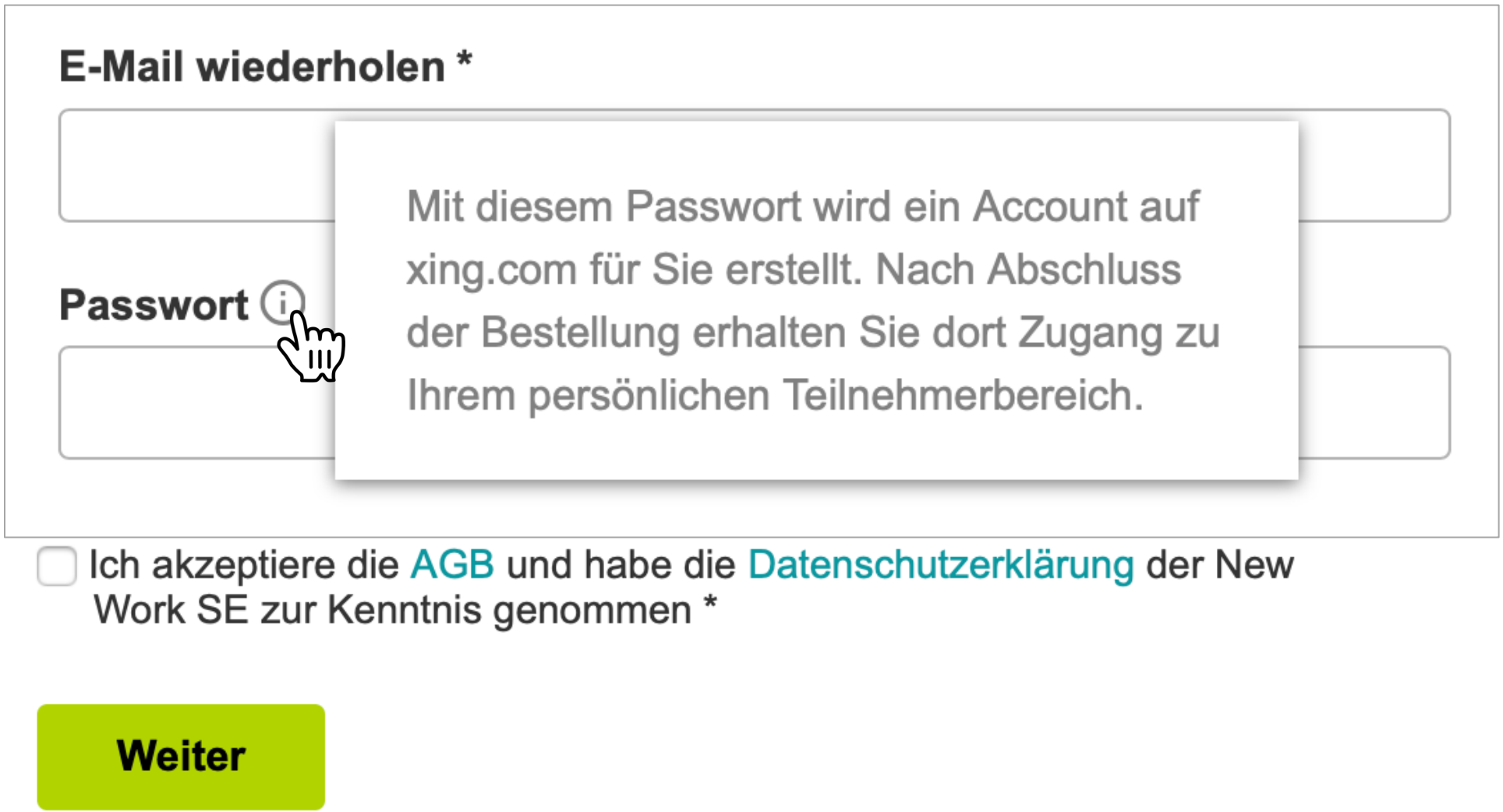
Allgemeine Hinweise

- Stand: 22. März 2022
- Hier informieren wir Dich über die Datenverarbeitung im Rahmen des gesamten Dienstes XING und seiner Anwendungen (kununu usw.).
- Verantwortlich für die Verarbeitung personenbezogener Daten ist die New Work SE.
- Unser Datenschutzbeauftragter ist Felix Lasse.

XING ist ein umfassender Dienst mit zahlreichen Anwendungen

XING ist ein Dienst, der den Zweck verfolgt, durch eine Vielfalt unterschiedlicher Anwendungen zur Verbesserung und Vereinfachung des Berufslebens des Nutzers beizutragen. Die Kombination dieser Anwendungen ermöglicht dem Nutzer das bestmögliche Nutzererlebnis und den größten Funktionsumfang. Angesichts des zunehmenden Verschwimmens der Grenzen zwischen Arbeits- und Privatleben und der Wechselwirkungen zwischen beiden, konzentriert sich XING dabei nicht ausschließlich auf den professionellen Kontext, sondern bezieht auch Anwendungen im privaten Kontext mit ein. Insbesondere möchte XING dem Nutzer neue Möglichkeiten eröffnen (vorwiegend im professionellen Kontext, aber auch im privaten Kontext), ihm erleichtern horizontale Netzwerke zu bilden, Informationen demokratisieren, den Informationsaustausch fördern und lebenslanges Lernen unterstützen. Um diese Zwecke zu erfüllen, stellt XING dem Nutzer unter anderem auf Basis erhobener Daten Informationen, Angebote, Empfehlungen sowie Dienstleistungen bereit und fördert die Interaktion – innerhalb und außerhalb des Netzwerks des Nutzers. Zu den Anwendungen des Dienstes XING gehören insbesondere das soziale Netzwerk, für das der Nutzer eine Mitgliedschaft erwerben kann, eine Veranstaltungsplattform, eine Arbeitgeberbewertungsplattform und eine Plattform zur Förderung des Mitarbeiterengagements. Einige der XING Anwendungen treten dabei gegebenenfalls unter anderen Markennamen oder unter Nutzung von anderen XING Websites in Erscheinung (z. B. kununu, HalloFreelancer).

mehr als 9000 Wörter


E-Mail wiederholen *
Passwort
Mit diesem Passwort wird ein Account auf xing.com für Sie erstellt. Nach Abschluss der Bestellung erhalten Sie dort Zugang zu Ihrem persönlichen Teilnehmerbereich.
Ich akzeptiere die AGB und habe die Datenschutzerklärung der New Work SE zur Kenntnis genommen *
Weiter

Art. 13 DSGVO

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

f) 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.

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

Informationspflichten: schon umfangreich, aber trotzdem sind wir oft schlecht informiert.

Art. 14 DSGVO

Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) zusätzlich die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) die Kategorien personenbezogener Daten, die verarbeitet werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

c) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

e) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

f) aus welcher Quelle die personenbezogenen Daten stammen und

g) 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.

(3) Der Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2

a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,

b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,

c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

(4) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(5) Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit

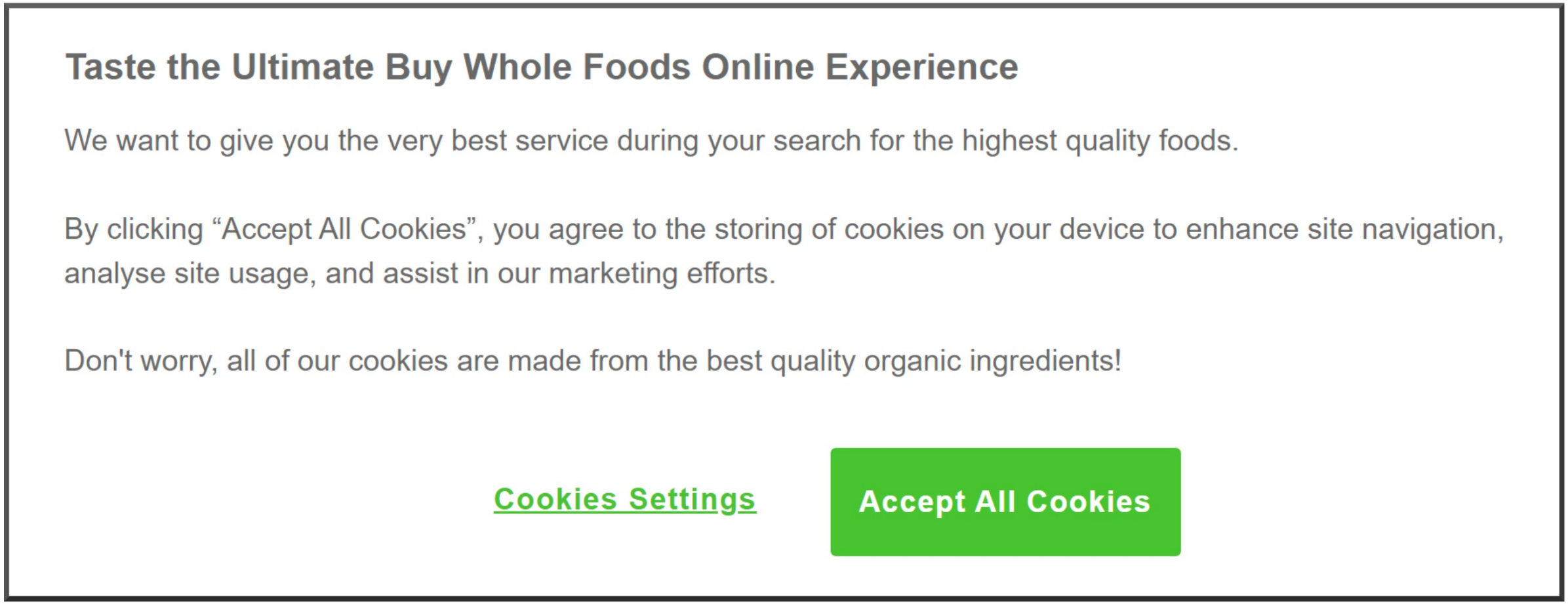
a) die betroffene Person bereits über die Informationen verfügt,

b) die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien oder soweit die in Absatz 1 des vorliegenden Artikels genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit,

c) die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder

d) die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

Wie verhalten sich hier die meisten?



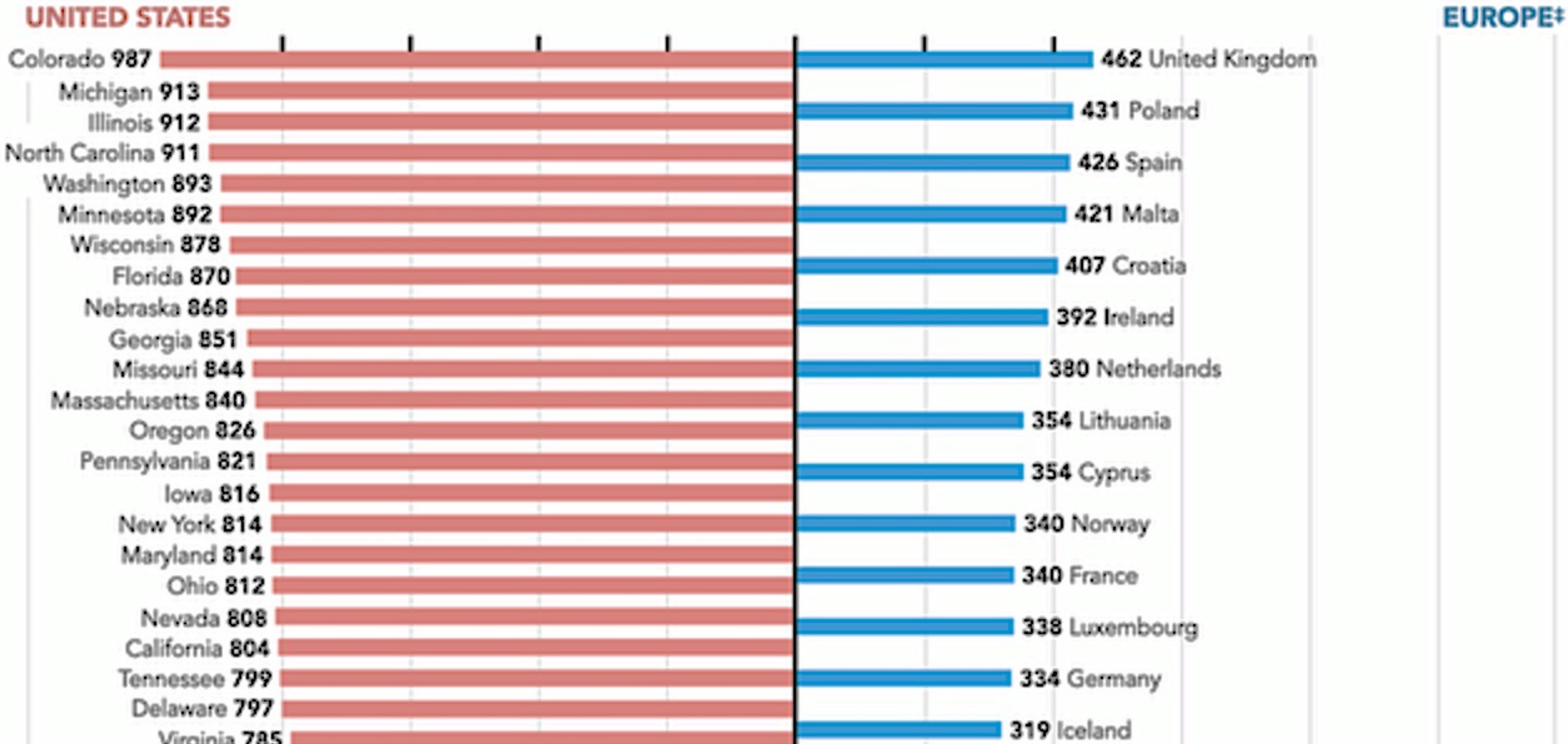
H. Habib et al. (2022) “Okay, whatever”: An Evaluation of Cookie Consent Interfaces. CHI 2022, ACM.

https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/

RTB broadcasts per person (daily)

Estimated RTB broadcasts per day[2]

„Accept All“? Wissen Sie denn was Real-Time Bidding ist?



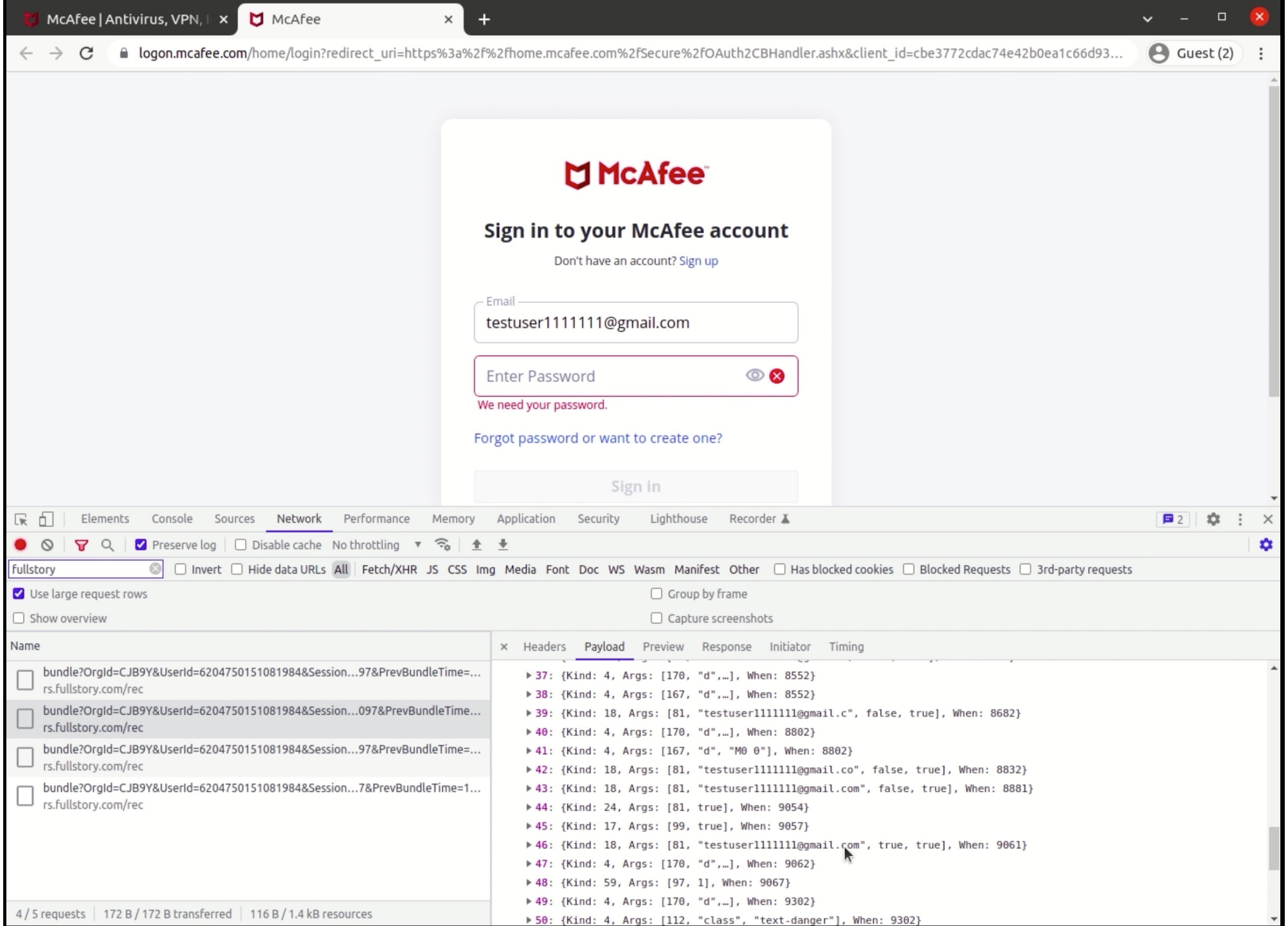
rechtskonform ≠ benutzbar

Viele Probleme unter der Oberfläche.

Technische Analysen notwendig.

Beispiel:

„Leaky Forms“



https://homes.esat.kuleuven.be/~asenol/leaky-forms/

Informationspflichten sind schön und gut,
aber wir sollten auch das **tatsächliche Verhalten**
prüfen und beschreiben.

Was könnten wir damit tun?

Öffentlichkeit herstellen

Seitenbetreiber ansprechen

Compare Websites with PrivacyScore

PrivacyScore allows you to test websites and rank them according to their security and privacy features.

Create new site list

— or scan a single site immediately —

URL, e.g. privacyscore.org SCAN

PrivacyScore is in public beta since 8 June 2017.

We post updates on Twitter.

Some parts of the site are also available in German. Please contact us if you want to contribute by translating the site.

Note that it is not possible to edit lists at the moment. Feel free to create a new list and inform us so that we can delete the previous version.

Tests von PrivacyScore

Privatsphäre und Tracking	**Verschlüsselung Webserver**	**Verschlüsselung Mailserver**	**andere Angriffe**
Third Parties Bekannte Tracker Server-Standorte	HTTPS/STARTTLS verfügbar? Zertifikat: gültig / Schlüssellänge Unsichere Protokolle: SSLv3, … Schwachstellen: Heartbleed, …		Referer-Policy Security-Header Problematische Inhalte
	HSTS Mixed Content Automatische Umleitung zu HTTPS		

server-status

phpinfo.php *server.key*

backup.sql *.git*

.svn

Alternativen z.B. webbkoll.dataskydd.net und urlscan.io

Webseiten deutscher Krankenkassen und -versicherungen

Ranking

#	URL	Name	Versicherte	Typ	Kategorie	NoTrack	EncWeb	Attacks	EncMail	Rating
1	http://www.ikkbb.de/ / 2019-12-08 @ 18:59:22	Innungskrankenkasse Brandenburg und Berlin	212.807	gesetzl	IKK	✓	✓	!	?	!
2	http://www.bkk-bpw.de/ / 2019-12-08 @ 19:02:21	Betriebskrankenkasse BPW Bergische Achsen KG – betriebsbezogen	6.550	gesetzl	BKK	✓	!	!	?	!
3	http://www.atlasbkkahlmann.de/ / 2019-12-08 @ 18:59:22	Atlas BKK ahlmann	55.000	gesetzl	BKK	✓	!	!	?	!
4	http://www.bkkgs.de/ / 2019-12-08 @ 19:01:25	BKK Gildemeister Seidensticker	183.297	gesetzl	BKK	✓	!	!	!	!
5	http://www.bkk-pfaff.de/ / 2019-12-08 @ 19:01:17	Betriebskrankenkasse der G. M. Pfaff AG Kaiserslautern	29.391	gesetzl	BKK	✓	!	!	!	!
5	http://www.bkk-linde.de/ / 2019-12-08 @ 19:02:59	BKK Linde	89.540	gesetzl	BKK	✓	!	!	!	!
6	http://www.bkk-da.de/ / 2019-12-08 @ 19:02:45	BKK Dürkopp Adler	23.622	gesetzl	BKK	✓	!	!	!	!
7	http://www.bkk-grillo.de/ / 2019-12-08 @ 19:01:25	BKK Grillo-Werke AG – betriebsbezogen	1.150	gesetzl	BKK	✓	✗	!	!	✗

NoTrack: No Tracking by Website and Third Parties

Check if 3rd party embeds are being used reliable
The site does not use any third parties.

Check if embedded 3rd parties are known trackers reliable
The site does not use known tracking or advertising services.

Determine how many cookies the website sets reliable
The site sets 1 short-term, 1 long-term, and 0 Flash cookies.

Determine how many cookies are set by third parties reliable
No one else is setting any cookies.

Check if Google Analytics is being used reliable
The site does not use Google Analytics.

Check if Google Analytics has privacy extension enabled reliable
Not checking as the site does not use Google Analytics.

Check whether web server is located ir
All web servers are located in Germany.

Check whether mail server is located ir
All mail servers are located in Germany.

Check whether web and mail servers in same country unreliable
The geo-location(s) of the web and mail server(s) are identical.

Attacks: Protection Against Various Attacks

Check for unintentional information leaks unreliable
The site does not disclose internal system information.

Check for presence of Content Security Policy shallow
The site does not set a Content-Security-Policy (CSP) header.

Check for presence of X-Frame-Options unreliable
The site does not set a X-Frame-Options (XFO) header.

Check for secure XSS Protection unreliable
The site does not set a X-XSS-Protection header.

Check for secure X-Content-Type-Options unreliable
The site does not set a X-Content-Type-Options header.

Check for privacy-friendly Referrer Policy unreliable
The site does not set a referrer-policy header.

...nts the browser from disclosing the URL of the ...Without a referrer policy most browsers send a ...tent is retrieved from third parties or when you ...ng on a link. This may disclose sensitive informa-

Conditions for passing: Referrer-Policy header is present. Referrer-Policy is set to "no-referrer" (which is the only recommended policy recommended by dataskydd.net in their Webbkoll scan service).

Reliability: unreliable. At the moment we only check for this header in the response that belongs to the first request for the final URL (after following potential redirects to other HTTP/HTTPS URLs).

Potential scan errors: We may miss security problems on sites that redirect multiple times. We may also miss security problems on sites that issue multi-

Detail-Ergebnisse

Wie reagieren Anbieter, wenn sie auf das Ranking hingewiesen werden?

M. Maass et al., **On the Difficulties of Incentivizing Online Privacy through Transparency: A Qualitative Survey of the German Health Insurance Market**, WI 2019, https://arxiv.org/abs/1811.12775 (2019).

Von weiteren Scans ausgenommen

Die Betreiber der hier aufgeführten Seiten haben uns gebeten, keine weiteren Scans durchzuführen. Aus Gründen der Transparenz archivieren wir das Ergebnis des letzten erfolgreichen Scans in der folgenden Tabelle. Beachten Sie, dass es möglich ist, dass Seitenbetreiber in der Zwischenzeit Änderungen an ihrer Website vorgenommen haben, die sich nicht in diesen veralteten Ergebnissen widerspiegeln.

#	Adresse (URL)	Name	Versicherte	Typ	Kategorie	NoTrack »	EncWeb « »	Attacks « »	EncMail «	Rating
1	http://www.meine-krankenkasse.de/ / 2018-01-12 @ 06:51:56	BKK Verkehrsbau Union	498.000	gesetzl	BKK	!	!	!	?	!
2	http://www.novitas-bkk.de/ (1 Fehler) / 2018-01-16 @ 13:18:50	Novitas BKK	410.216	gesetzl	BKK	!	!	!	?	!
3	http://www.bmwbkk.de/ / 2017-12-18 @ 13:53:50	Betriebskrankenkasse der BMW AG – betriebsbezogen	157.839	gesetzl	BKK	!	!	!	!	!
4	http://www.big-direkt.de/ / 2017-12-13 @ 14:46:08	Bundesinnungskrankenkasse Gesundheit	409.000	gesetzl	IKK	!	!	!	!	!
5	http://www.ikk-nord.de/ / 2017-12-14 @ 13:40:04	Innungskrankenkasse Nord	230.005	gesetzl	IKK	!	!	!	!	!
6	http://www.die-bergische-kk.de/ / 2017-12-18 @ 09:48:17	Die Bergische Krankenkasse	71.889	gesetzl	BKK	!	!	⚠	!	⚠
7	http://www.bkkdb.de/ / 2018-01-11 @ 06:27:53	BKK Deutsche Bank AG – betriebsbezogen	80.998	gesetzl	BKK	!	✖	!	?	✖
8	http://www.bkk-pwc.de/ / 2017-12-18 @ 10:08:47	Betriebskrankenkasse PricewaterhouseCoopers – betriebsbezogen	19.001	gesetzl	BKK	!	✖	!	!	✖

Betrieb in Deutschland rechtlich zulässig, siehe *arxiv.org/abs/1705.08889* (GI INFORMATIK 2017)

noch mehr

Öffentlichkeit herstellen

Seitenbetreiber ansprechen

Sicherheitslücke betraf mehr als 170 Online-Apotheken

Wer kauft gerade welche Medikamente ein? Dritte konnten solche sensiblen Informationen bei zahlreichen Internetapotheken einsehen. Die Panne betraf Dutzende Websites auf einmal.

Von Markus Böhm

Donnerstag, 24.05.2018 14:44 Uhr

Mehr als 170 Online-Apotheken, darunter etwa Apotal und Sanicare, hatten bis vor Kurzem ein Sicherheitsproblem. Dritte konnten, teils bis zum Dienstagmittag, auf einfachem Weg Einblick in die Daten gerade aktiver Kunden der Websites bekommen.

Sie konnten dabei Berichten zufolge unter anderem an die Namen, Adressen und die Kontodaten der Betroffenen kommen. Auch Informationen zu den Bestellungen sollen prinzipiell einsehbar gewesen sein. Entdeckt haben die Sicherheitslücke Forscher der Universität Bamberg; zuerst darüber berichtet haben am Donnerstagmorgen NDR und WDR.

https://www.apc[redacted].de/server-status

Szenario nachgestellt

Apache Server Status for [redacted]

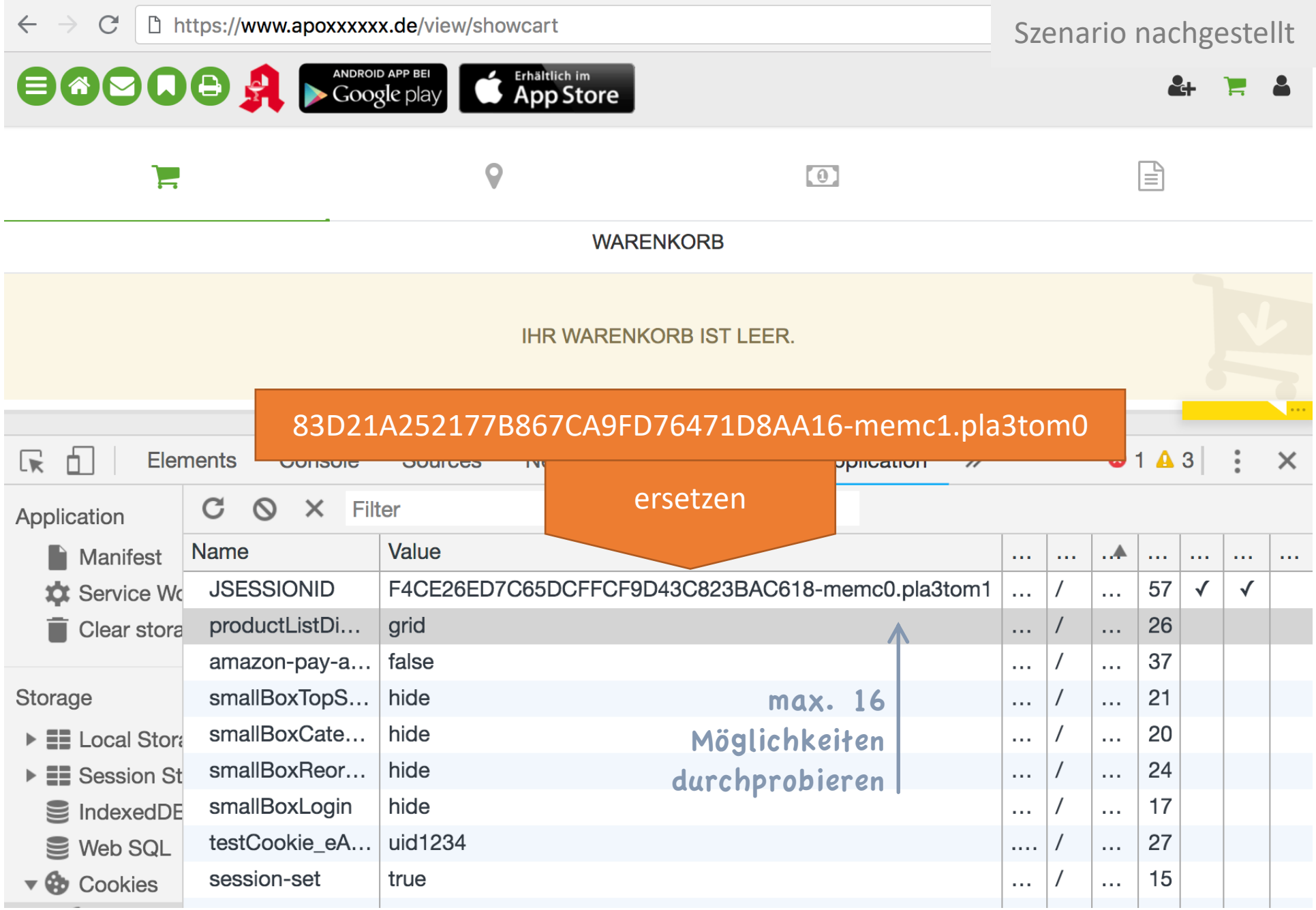
Server Version: Apache/2.2.8 (Ubuntu) mod_auth_pgsql/2.0.3 mod_python/3.3.1 Python/2.5.2 PHP/5.2.4-2ubuntu5.27 with Suhosin-Patch mod_ruby/1.2.6 Ruby/1.8.6(2007-09-24) mod_ssl/2.2.8 OpenSSL/0.9.8g mod_perl/2.0.3 Perl/v5.8.8
Server Built: Mar 8 2013 17:04:27

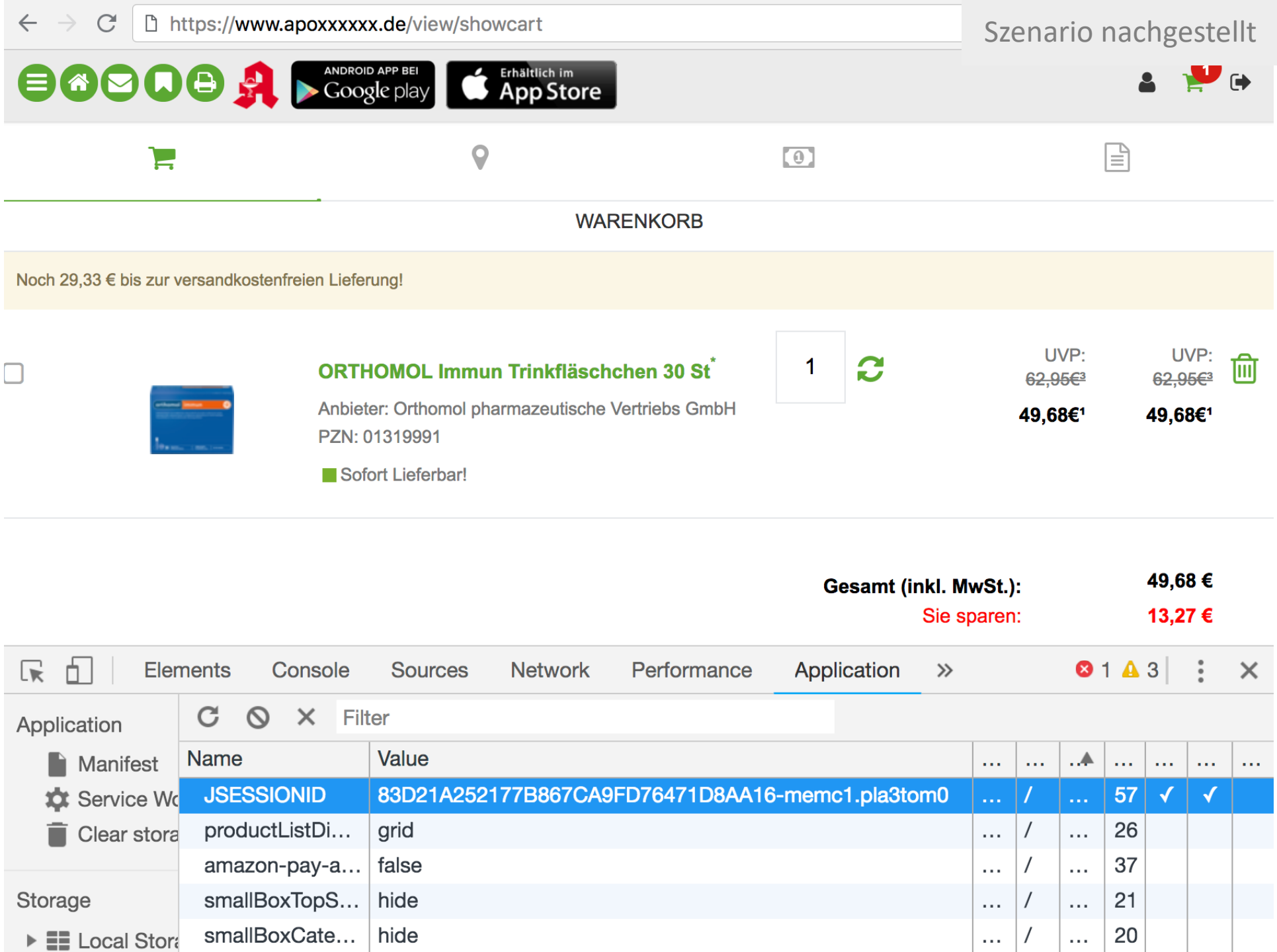
Current Time: Monday, 11-Jun-2018 11:07:53 NZST
Restart Time: Tuesday, 22-May-2018 15:24:04 NZST
Parent Server Generation: 13
Server uptime: 19 days 19 hours 43 minutes 48 seconds
Total accesses: 138469 - Total Traffic: 5.9 GB
CPU Usage: u20.71 s3.32 cu0 cs0 - .0014% CPU load
.0809 requests/sec - 3719 B/second - 44.9 kB/request
1 requests currently being processed, 9 idle workers

____._._W.___.................

Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-13	4978	0/8/11203	_	0.37	345	0	0.0	0.01	495.05	[redacted]	[redacted]	NULL
1-13	4501	0/26/10972	_	0.49	346	230	0.0	18.34	435.15	[redacted]	[redacted]	GET /keywordsearch;jsessionid=83D21A252177B8
2-13	5207	0/1/10580	_	0.01	138	8	0.0	0.00	364.21	[redacted]	[redacted]	[redacted]
3-13	3210	0/102/10603	_	2.68	344	0	0.0	18.22	534.61	[redacted]	[redacted]	[redacted]
4-13	-	0/0/10030	.	0.01	341	8	0.0	0.00	335.80	[redacted]	[redacted]	[redacted]
5-13	4437	0/35/10152	_	0.90	346	0	0.0	47.02	371.89	[redacted]	[redacted]	[redacted]
6-												


https://www.apoxxxxxx.de/view/showcart
Szenario nachgestellt
ANDROID APP BEI Google play
Erhältlich im App Store
WARENKORB
IHR WARENKORB IST LEER.
83D21A252177B867CA9FD76471D8AA16-memc1.pla3tom0
ersetzen
Elements
Application
Manifest
Service Wo
Clear stora
Storage
Local Stora
Session St
IndexedDE
Web SQL
Cookies
Filter
Name
Value
JSESSIONID
F4CE26ED7C65DCFFCF9D43C823BAC618-memc0.pla3tom1
productListDi…
grid
amazon-pay-a…
false
smallBoxTopS…
hide
smallBoxCate…
hide
smallBoxReor…
hide
smallBoxLogin
hide
testCookie_eA…
uid1234
session-set
true
max. 16 Möglichkeiten durchprobieren


https://www.apoxxxxxx.de/view/showcart
Szenario nachgestellt
ANDROID APP BEI Google play
Erhältlich im App Store
WARENKORB
Noch 29,33 € bis zur versandkostenfreien Lieferung!
ORTHOMOL Immun Trinkfläschchen 30 St*
Anbieter: Orthomol pharmazeutische Vertriebs GmbH
PZN: 01319991
Sofort Lieferbar!
1
UVP: 62,95€³ 49,68€¹
UVP: 62,95€³ 49,68€¹
Gesamt (inkl. MwSt.): 49,68 €
Sie sparen: 13,27 €
Elements Console Sources Network Performance Application
1 3
Application
Manifest
Service Wo
Clear stora
Storage
Local Stora
Filter
Name Value
JSESSIONID 83D21A252177B867CA9FD76471D8AA16-memc1.pla3tom0 / 57
productListDi… grid / 26
amazon-pay-a… false / 37
smallBoxTopS… hide / 21
smallBoxCate… hide / 20

https://www.apoxxxxxx.de/viewprofile

Szenario nachgestellt

ANDROID APP BEI Google play

Erhältlich im App Store

Persönliche Daten | Passwort ändern | Gespeicherte Adressen | Bestellhistorie | Einkaufslisten / Favoriten

Das Profil von Gregor Schmidbauer

Persönliche Daten

Anmelden:
gregorschmidbauer@gmail.com

Name:	Gregor Schmidbauer
Geburtstag:	02.03.1984
E-Mail:	gregorschmidbauer@gmail.com
Straße:	An Der Weberei
Hausnummer:	5
Postleitzahl:	96047
Ort:	Bamberg
Land:	Deutschland
Telefon:	0151-1234567890
Mobil:	
Fax:	

Bearbeiten

Ihr persönliches Passwort

Um Ihr Passwort zu ändern Hier klicken.

Gespeicherte Adressen

neue Adresse anlegen

Reaktion?

§202a StGB!

Also lieber doch keine öffentlichen Pranger?

noch mehr

Öffentlichkeit herstellen

Seitenbetreiber ansprechen

Rückblende: 2018

Vortrag auf einer Konferenz für Rechtsinformatik

Aus einer Datenschutzerklärung…

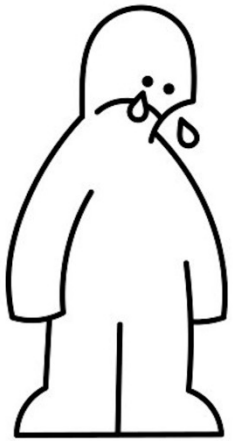
Adresse mit anderen Daten von Google
zusammengeführt. Die IP-Adressen wer
anonymisiert, so dass eine Zuordnung n
möglich ist (IP-Masking).
Um die Nutzung unserer Webseite statis
zu erfassen und zum Zwecke der
Optimierung
auszuwerten
Google Conv

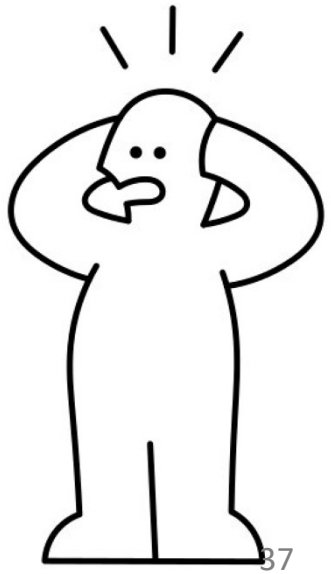
view-source:http://www 200%

```
<script>
(function(i,s,o,g,r,a,m){i['GoogleAnalytic
(i[r].q=i[r].q||[]).push(arguments)},i[r].
m=s.getElementsByTagName(o)[0];a.async=1;a
})(window,document,'script','//www.google-

ga('create', '[redacted]', '[redacted]');
ga('send', 'pageview');
```

view-source:https://www.tablette 133%

```
(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r
(i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Dat
m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.pa
})(window,document,'script','//www.google-analytics.c

ga('create', '[redacted]', 'auto');

ga('send', 'pageview');

ga('set', 'anonymizeIp', true);

</script>
```





kurz darauf …

Rechtsverletzung durch Betrieb von Google Analytics ohne "anonymizeIP"

Landgericht Dresden

Urteil v. 11.01.2019 - Az.: 1a O 1582/18

Leitsatz

Rechtsverletzung durch Betrieb von Google Analytics ohne "anonymizeIP"

Tenor

In dem Rechtsstreit (...)

wegen Unterlassung und Auskunft

hat die 1a. Zivilkammer des Landgerichts Dresden durch (...) als Einzelrichter auf Grund der mündlichen Verhandlung vom 20. November 2018 am 11. Januar 2019 für Recht erkannt:

I. Die Beklagte wird verurteilt,

1. Es bei Meidung eines für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes bis zu 250.000 €, ersatzweise Ordnungshaft oder Ordnungshaft bis zu 6 Monaten zu unterlassen, eine IP-Adresse des Klägers zu speichern und an die Google Inc. zu übermitteln, indem die Beklagte auf der vom Kläger besuchten Webseite den Tracking-Dienst Google Analytics nutzt, ohne dabei gleichzeitig die Code-Erweiterung „anonymisiert“ zu verwenden,

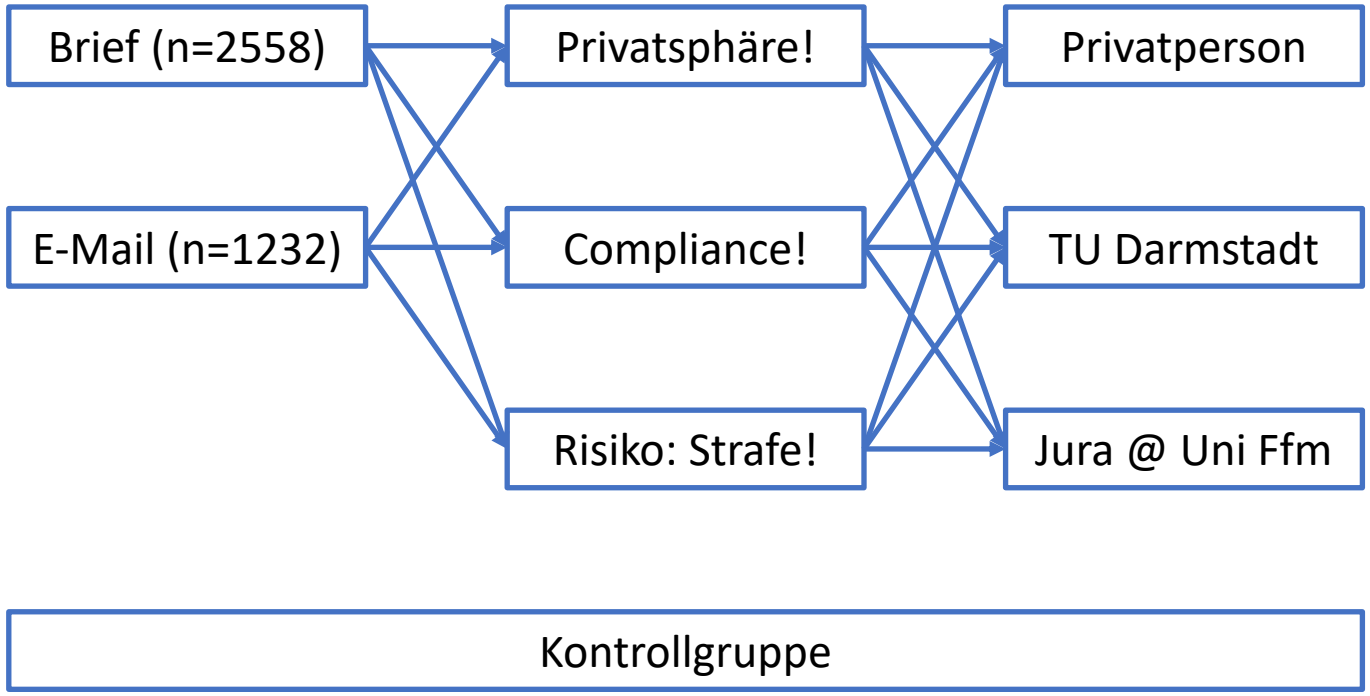
2. dem Kläger Auskunft zu erteilen, ob über den Kläger betreffende personenbezogene Daten verbreitet werden, sowie ggf. Auskunft zu erteilen, welche personenbezogenen Daten über den Kläger gespeichert werden und
3. dem Kläger von der Zahlung vorgerichtlicher Anwaltskosten in Höhe von 571,44 € zuzüglich Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 11. September 2018 feizustellen.

«Wir könnten die Seitenbetreiber persönlich anschreiben und sie über das Problem informieren!»

Crawl mit einem automatisierten Chromium-Browser

Ergebnis: 8000 nicht-konforme «de»-Webseiten.

Experiment



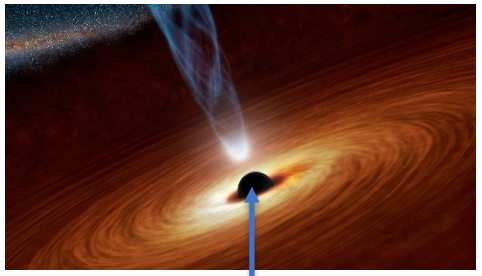
https://checkgoogleanalytics.psi.uni-bamberg.de/

7/2019: erste Benachrichtigung
8/2019: Erinnerung
9/2019: Debriefing/Umfrage

https://www.usenix.org/conference/usenixsecurity21/presentation/maass

Erwartung

Realität



Hey, du hast ein Problem!

Oh, danke!

Wie bitte?

“Vielen Dank für die Informationen. Können Sie mir auch mitteilen, an welcher Stelle wir bei Google Analytics die entsprechenden Einstellungen ändern können."

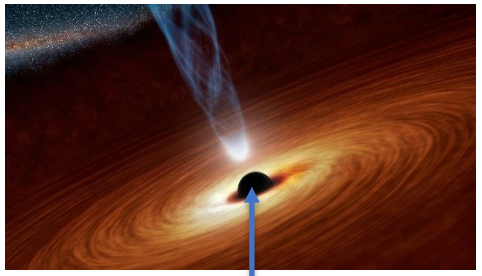
„[ist] dieses Schreiben echt oder, wie es schon häufig vorgekommen ist, eine unerlaubte Aufforderung um an gewisse Daten zu kommen.“

„Ich könnte dir Zugang zu unserem Account geben und dann kannst du das vielleicht selbst machen wenn das für dich wichtig ist?“

„Gerne würde ich die IP Anonymisierung aktivieren, aber ich weiß nicht wie. Könnten Sie mir da weiterhelfen.“

„Wo steckt der Bug? Im Test der Uni Bamberg? In unserem System?“

Realität

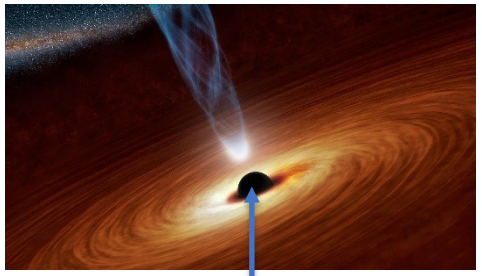


Hey, du hast ein Problem!

Ich hätte da noch ein paar Fragen!

Oh, danke!

Realität



Hey, du hast ein Problem!

Nein, bei uns ist alles in Ordnung – wirklich!

Ich hätte da noch ein paar Fragen!

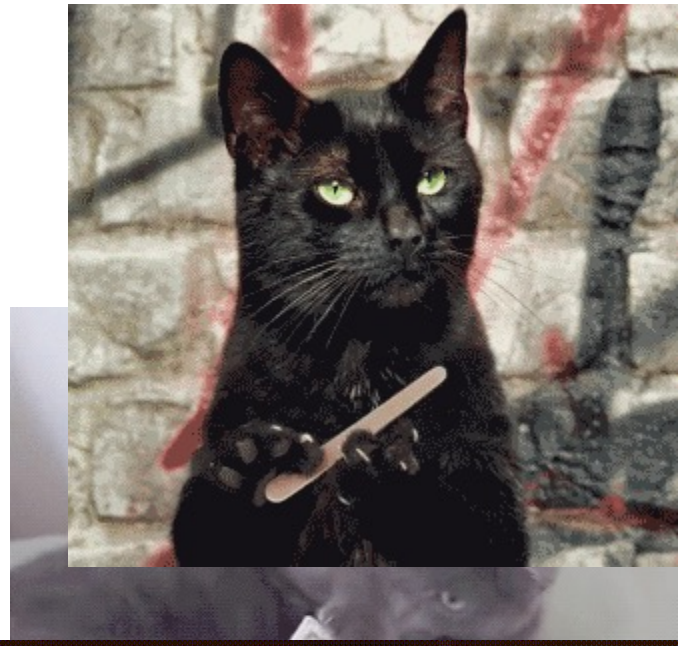
Oh, danke!

Nicht schon wieder …

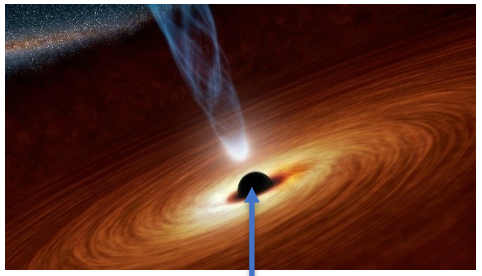
Ein Betreiber ruft den Kanzler an und droht, die TU Darmstadt zu verklagen, wenn sie nicht aufhöre, «falsche und diffamierende» Aussagen zu machen.

Ein externer Datenschutzbeauftragter stellt uns eine Rechnung für die Zeit, die er für die Überprüfung unserer Nachricht aufgewendet hat.

Ein Leiter einer Webdesign-Agentur beschwert sich und sagt, dass «Max Maass wie ein erfundener Name klingt».



Realität



Hey, du hast ein Problem!

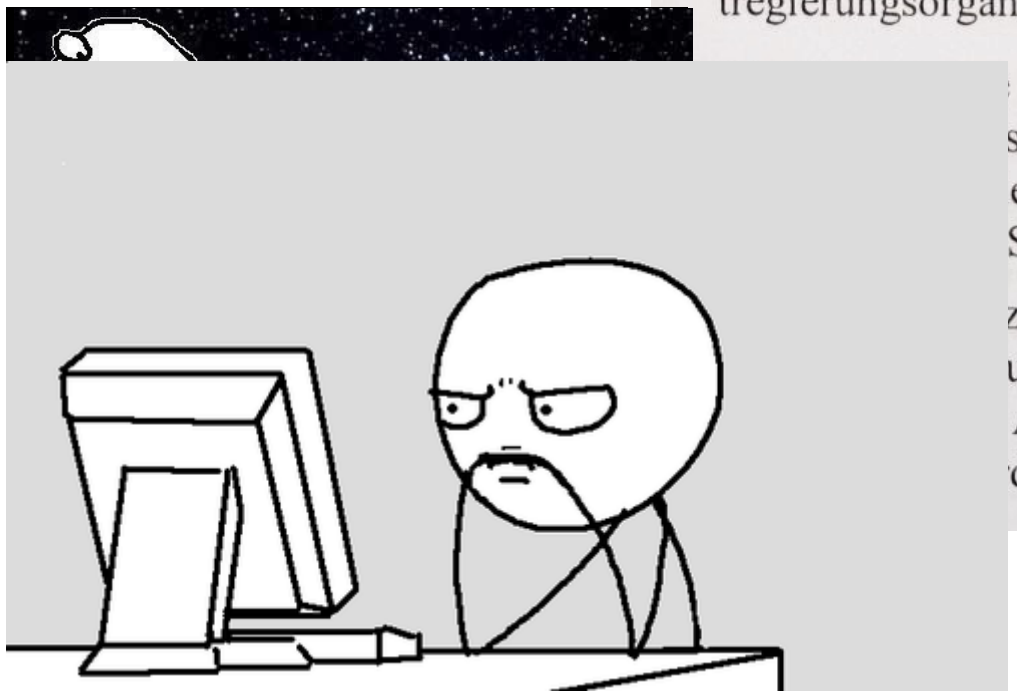
Nein, bei uns ist alles in Ordnung – wirklich!

Ich hätte da noch ein paar Fragen!

Oh, danke!

Lasst uns einfach in Ruhe damit!

Geht es noch schlimmer?

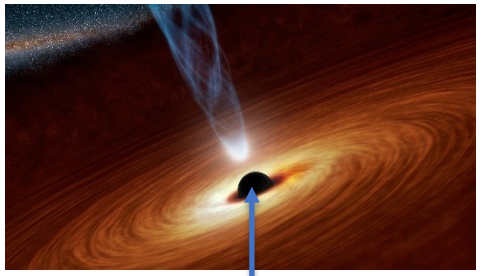


Im Entwurf ihrer Katalogkonservenwerbepost, -im Zusammenhang mit der Datenschutz-grundverordnung-, behauptet sie, daß sie Unsere Tätigkeit im weltweiten Internet untersucht haben. Wir haben ihnen weder einen Auftrag erteilt noch sie um ihre Meinung gefragt, da Wir vorstaatlich im originären Recht sind, denn das Zentrum ist eine nichtwirtschaftliche Nich-tregierungsorganisationen mit besonderen Vorrechten.

Spionage- und Sabotagefunktionen ausüben, und sie haben im Bereich Recht
sse. Das Internationale Zentrum für Menschenrecht ist keine Demokratieein-
e Seite wurde mit WebSite X5 erstellt. Wenden sie sich an diese Firma mit
Sie haben ein Problem.

zgrundverordnung ist für Unsere Einrichtungen im öffentlichen Recht nicht
unitäten sind vertraglich im Völkerrecht geregelt, so daß Wir ihren Angriff als
Aggression für Streit- und Feindhandlungen mit dem Ziel eines bewaffneten
dnen.

Realität



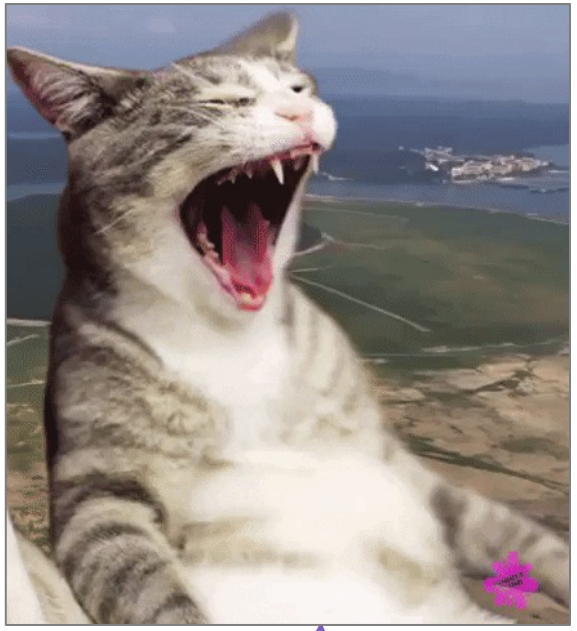
Hey, du hast ein Problem!

Nein, bei uns ist alles in Ordnung – wirklich!

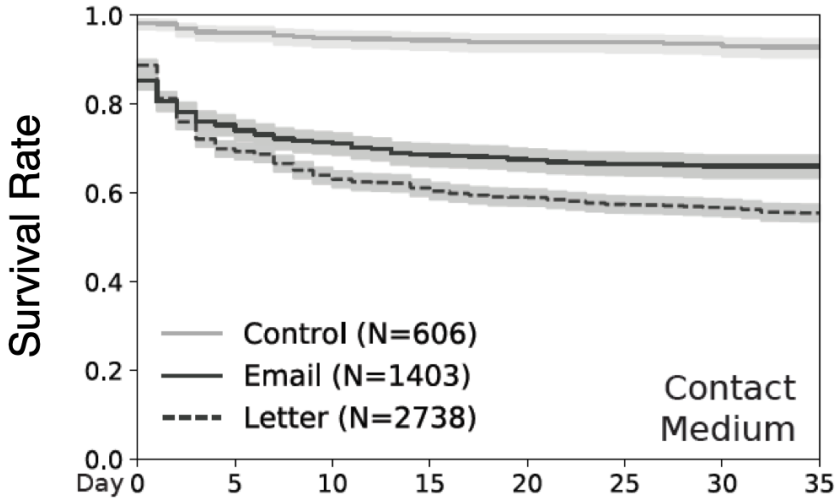
Ich hätte da noch ein paar Fragen!

Oh, danke!

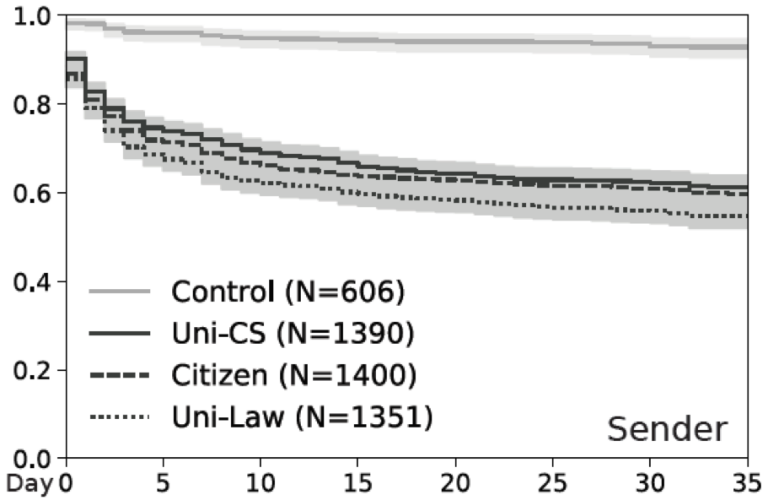
Lasst uns einfach in Ruhe damit!



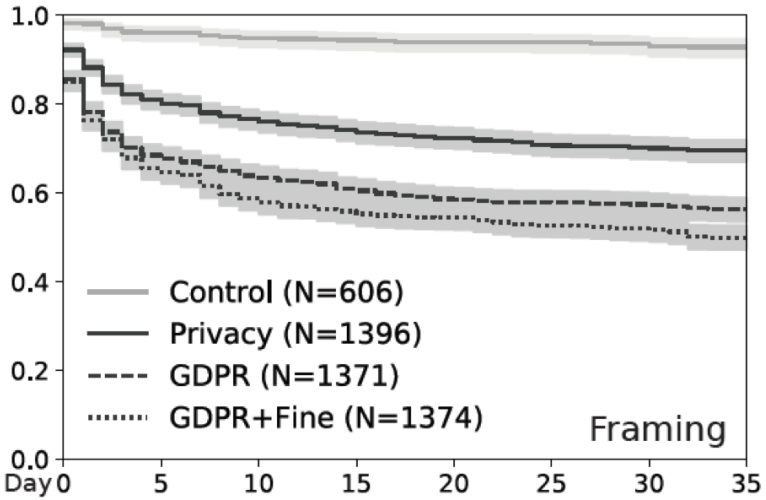
Ergebnisse



Briefe effektiver



Juristischer Absender effektiver



Erinnerung an Risiko von Strafen effektiver

Wie viele Seiten bleiben trotz Benachrichtigung *nicht-konform*?

E-Mail / Informatik / Privatsphäre: 82%

Brief / Jura / Strafe: **39%**

Überraschendes

36% der Seiten, die rechtskonform wurden,
haben Google Analytics einfach komplett deaktiviert.

Umfrage (N = 477) ergab: nur 80% der
Antwortenden wussten, dass sie GA einsetzten.

13% wussten bereits vor unserer Nachricht,
dass IP-Anonymisierung nicht aktiv war…

87% fanden unser CheckGA-Tool nützlich.

Privacy on the Web:
Hilft mehr Transparenz, den Datenschutz zu verbessern?

Automatisierte technische Analysen
schaffen mehr **Transparenz.**

Ermöglichen **Herstellen von Öffentlichkeit** und
direkte Ansprache zur Verbesserung des Datenschutzes.

Best Practices zur Benachrichtigung:
https://dl.acm.org/doi/10.1145/3465481.3470081

Prof. Dr. Dominik Herrmann · Universität Bamberg
LSt Privatsphäre und Sicherheit in Informationssystemen
https://www.uni-bamberg.de/psi/ · @herdom auf Twitter

Slides: https://dhgo.to/wlb22