

# **Internationale Bürgerrechtsorganisationen: Unternehmen gefährden unsere Grundrechte auf Privatsphäre und Datenschutz**



Dieser Bericht wurde durch Mitglieder von European Digital Rights, Bits of Freedom, Open Rights Group und Privacy International erstellt. An der Kampagne beteiligten sich weiterhin der Verein Digitale Gesellschaft, Access und La Quadrature du Net.

Die deutsche Übersetzung sowie die Postkarten-Kampagne erfolgte durch den Verein Digitale Gesellschaft.

**nakedcitizens.eu**  
**digitalegesellschaft.de**



# Inhalt

Zusammenfassung	3
2. Warum braucht die EU neue Regeln für den Datenschutz?	4
Warum die neue Datenschutzgrundverordnung helfen wird	5
Warum gibt es damit Probleme?	5
3. Die fünf Vorschläge, die die Privatsphäre am stärksten verletzen würden	6
1. Verwässerung der Definition von "Einwilligung"	6
2. Profilbildung ohne Zustimmung der Betroffenen	7
3. Die erlaubte Nutzung von persönlichen Daten für alle möglichen Zwecke	7
4. Geschäftsinteressen vs. Rechte der Bürgerinnen und Bürger	8
5. Die Einführung der sogenannten "pseudonymen Daten"	8
4. Empfehlungen und weiterführende Literatur	9
Weitere Informationen:	9
Anhang: Die Änderungsanträge, die den meisten Schaden anrichten würden	10
Impressum	13

## Zusammenfassung

Der vorliegende Bericht ist eine von Datenschutzerxperten formulierte Analyse der Änderungsanträgen des Entwurfs für eine europäische Datenschutzgrundverordnung. Er zeigt, wie viele dieser Vorschläge die Privatsphäre der Verbraucher und Bürger Europas auszuhöhlen drohen. Zusammen genommen sind die Änderungsanträge ein Versuch, die Bürgerinnen und Bürger Europas "nackt" dastehen zu lassen, indem es ihnen fast unmöglich wird, zu kontrollieren, wer ihre persönlichen Informationen sieht und wie diese genutzt werden.

Mehr als 3000 Änderungsanträge zur Verordnung werden zurzeit vom Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments verhandelt. Die 46 Schlimmsten haben wir herausgearbeitet. Die meisten davon wurden von Mitgliedern der konservativen Europäischen Volkspartei (EVP) sowie der liberalen Parteien (LIBE) eingebracht (15 von der EVP und 24 von ALDE). Da diese Parteien zusammengenommen über eine Mehrheit im Europaparlament und dem LIBE-Ausschuss verfügen, bedrohen sie gemeinsam die Datenschutzrechte derjenigen, die sie gewählt haben.

Wir haben die Änderungsanträge thematisch in fünf Kategorien gegliedert, anhand derer wir genau erklären, warum sie schädlich für die Privatsphäre aller EU-Bürgerinnen und Bürger sind. Die Vorschläge würden...

- die Definition von "Zustimmung" aufweichen und damit die unbeabsichtigte Einwilligung der Nutzerinnen und Nutzer in die Verwendung ihrer Daten wahrscheinlicher machen.
- es Firmen einfacher machen, ohne Einverständnis Nutzerprofile zu erstellen, was womöglich zu Diskriminierung vor allem sozial Schwächerer führt.
- es Unternehmen leichter machen, die eigenen Interessen höher zu gewichten und gegenüber den Datenschutzinteressen der Bürgerinnen und Bürger geltend zu machen.
- sogenannte "pseudonymisierte" Daten als effektiven Weg zur Vermeidung von Datenschutzrisiken anerkennen.

Dies sind jedoch keineswegs die einzigen schädlichen Änderungsanträge. Viele weitere der tausenden im LIBE-Ausschuss eingereichten Anträge würden weitere Bürgerrechte wie Widerspruchs- und Löschungsrechte unterminieren sowie Sanktionen abschwächen, die bei Verstößen gegen Datenschutzbestimmungen drohen.

Wir fordern die Mitglieder des Europäischen Parlaments auf, diese schädlichen Änderungsanträge abzulehnen und die Menschen dabei zu unterstützen, die Kontrolle über ihre Daten zu behalten. Anders als bisweilen behauptet, wäre eine starke und effektive Datenschutzverordnung keineswegs schädlich für Wirtschaft und Innovation. Ein hohes Datenschutzniveau würde eine globale Führungsrolle der EU in diesem Feld sicherstellen, indem mittels harmonisierter Bestimmungen ein Mehr an Vertrauen, Daten- und Rechtssicherheit für einen Wirtschaftsraum mit 400 Millionen Menschen geschaffen würde.

## 2. Warum braucht die EU neue Regeln für den Datenschutz?

Das Internet ist ein Überwachungsstaat. Ob wir es uns eingestehen oder nicht, ob wir es mögen oder nicht: Wir werden immer erfasst."  
*IT-Sicherheitsexperte Bruce Schneider, März 2013<sup>1</sup>*

Datenschutzregulierung mag technisch klingen – ein Nischenthema für Rechtsexperten. Aber es betrifft uns alle auf verschiedene Weisen.

Fast alles, was wir tun, hinterlässt Datenspuren. Informationen über die Webseiten, die wir besuchen, werden nachverfolgt und gespeichert. Über elektronische Tickets kann unser Reiseverhalten nachvollzogen werden. Mobile Apps, die wir verwenden, erfordern Zugriff auf Informationen über unseren Standort oder greifen auf Informationen in unseren Adressbüchern zu.

Wen wir kennen, welche Musik wir mögen, welche Nachrichten wir lesen und was wir ausgeben – all das kann heute nachverfolgt, gespeichert und ausgewertet werden.

Personenbezogene Daten, die wir hinterlassen, werden heute von Institutionen und Organisationen verwendet, um viele wichtige Entscheidungen über uns zu treffen. Persönlichkeitsprofile beeinflussen, welche Werbeangebote wir auf Grund unserer Kreditwürdigkeit erhalten oder welche Versicherungsangebote uns angeboten werden. Diese Informationen dienen jenen, die Einblicke in unser Reiseverhalten, unsere Persönlichkeit, Geschichte und zwischenmenschliche Beziehungen gewinnen möchten.<sup>2</sup>

Viel zu oft können wir nicht kontrollieren, wie und von wem persönliche Informationen verwendet werden. Und viel zu oft sind persönliche Daten nicht sicher genug, bleiben Missbrauch und Fehlverhalten praktisch ungeahndet. Aus diesem Grund speichern verschiedenste Unternehmen persönliche Daten für Zwecke, die wenig mit jenen Gründen zu tun haben, für die die Daten ursprünglich gesammelt wurden. Sie verwenden diese Daten auf Arten und Weisen, denen die "Datensubjekte" möglicherweise widersprechen würden.

Es ist nicht überraschend, dass die Mehrheit der Bevölkerung jenen misstraut, die ihre persönlichen Daten sammeln und verwenden. Einer Eurobarometer-Studie<sup>3</sup> zufolge sind 70% der Europäerinnen und Europäer besorgt, dass Unternehmen Daten für andere Zwecke verwenden als jene, für die diese gesammelt wurden. Und kürzlich hat eine Studie von Ovum ergeben, dass nur 14 Prozent der Befragten glauben, dass Internetunternehmen ehrlich in Bezug auf die Verwendung personenbezogener Konsumentendaten sind.<sup>4</sup>

---

<sup>1</sup> [http://www.schneier.com/blog/archives/2013/03/our\\_internet\\_su.html](http://www.schneier.com/blog/archives/2013/03/our_internet_su.html)

<sup>2</sup> See for example the study from Cambridge's Psychometrics Centre into Facebook 'Likes': <http://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions>

<sup>3</sup> [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_359\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf)

<sup>4</sup>

[http://ovum.com/press\\_releases/ovum-predicts-turbulence-for-the-internet-economy-as-more-than-two-thirds-of-consumers-say-no-to-internet-tracking/](http://ovum.com/press_releases/ovum-predicts-turbulence-for-the-internet-economy-as-more-than-two-thirds-of-consumers-say-no-to-internet-tracking/)

Ein Mangel an Privatsphäre sorgt nicht nur dafür, dass sich Menschen unsicher fühlen: Eine Studie von TRUSTe in Großbritannien ergab, dass 94% der Menschen sich um ihre Privatsphäre sorgen und dass Verbraucher sich weniger auf Unternehmen einlassen, denen sie nicht vertrauen - was zu weniger Einkäufen (29%), App Downloads (68%) und Teilen von Informationen (86%) führt. Eine Marktstudie der Exekutivagentur für Gesundheit und Verbraucher (Executive Agency for Health and Consumers) hat im Jahr 2011 herausgefunden, dass 29% der Menschen sagen, dass Sorgen um den Missbrauch persönlicher Informationen oder Zahlungsdetails ein wesentlicher Grund für sie sind, nicht online einzukaufen.<sup>56</sup>

### ***Warum die neue Datenschutzgrundverordnung helfen wird***

Die Europäische Kommission hat den Entwurf einer Datenschutzgrundverordnung am 25. Januar 2012 veröffentlicht. Es handelt sich dabei um die vorgeschlagene Aktualisierung der Datenschutzrichtlinie von 1995. Die Verordnung wurde entworfen, um die oben erwähnten Probleme anzugehen. Sie ist eine stärker und besser durchsetzbarere Erklärung aktueller Datenschutzprinzipien.

Die Verordnung beinhaltet eine Reihe von Maßnahmen, die Menschen mehr Kontrolle über ihre Daten geben, indem gewährleistet wird, dass Unternehmen, die sich an diese Regeln halten, ebenfalls für ihren Umgang mit Daten zur Verantwortung gezogen werden. Die Verordnung würde den Menschen eine echte Möglichkeit zur Einwilligung und stärkere Lösungsrechte geben. Sie kann es Menschen möglich machen überhaupt von Profilingmaßnahmen zu erfahren und gegebenenfalls Rechtsmittel gegen sie einzulegen. So wäre sichergestellt, dass Datenverarbeiter für Fehler und Datenmissbrauch verantwortlich gemacht werden können.

Eine starke Datenschutzverordnung würde Bürgerinnen und Bürger wieder ins Zentrum der Online-Wirtschaft rücken. Sie könnte für eine Harmonisierung der Regeln in der gesamten Europäischen Union sorgen und so einen vertrauenswürdigen, sicheren und berechenbaren Rechtsraum schaffen.

### ***Warum gibt es damit Probleme?***

Die Datenschutzverordnung wird derzeit im federführenden Ausschuss für Bürgerliche Freiheiten, Inneres und Justiz (LIBE) diskutiert.

Unter den tausenden Änderungsanträgen gibt es viele, die eine ernsthafte Bedrohung für unser deutsches Datenschutzrecht sind. Diese gefährlichen Änderungsanträge sind zum Großteil das Resultat einer nie da gewesenen Lobbywelle großer US-amerikanischer Technologieunternehmen, der US-Regierung und der Werbeindustrie.

Statt einer Verordnung, die es Nutzerinnen und Nutzern ermöglicht, zu erfahren, welche ihrer persönlichen Daten benutzt werden, zielen diese Änderungsanträge darauf ab, die Menschen datenschutzrechtlich zu entmündigen. Statt einer Stärkung der Nutzerrechte, würden diese Änderungs-

---

<sup>5</sup> [http://www.truste.com/about-TRUSTe/press-room/news\\_truste\\_transparency\\_choice\\_needed\\_to\\_address\\_uk\\_privacy](http://www.truste.com/about-TRUSTe/press-room/news_truste_transparency_choice_needed_to_address_uk_privacy)

<sup>6</sup> Consumer market study on the functioning of e-commerce and Internet marketing and selling techniques in the retail of goods, Executive Agency for Health and Consumers, 2011 [http://ec.europa.eu/consumers/consumer\\_research/market\\_studies/docs/study\\_ecommerce\\_goods\\_en.pdf](http://ec.europa.eu/consumers/consumer_research/market_studies/docs/study_ecommerce_goods_en.pdf) (Page 32)

vorschläge dafür sorgen, dass Unternehmen, Behörden und Organisationen personenbezogene Daten in undurchsichtiger und unverantwortlicher Art und Weise aneinander weitergeben können.

Die vorgeschlagenen Änderungen zur Datenschutzgrundverordnung, die in diesem Bericht analysiert werden, würden Bürgerinnen und Bürger die Kontrolle über ihre persönlichen Daten entziehen und sie nackt vor den neugierigen Augen großer Unternehmen zurücklassen. Wir appellieren an die Abgeordneten des Europäischen Parlaments gegen diese Änderungsvorschläge zu stimmen und den Bürgerinnen und Bürgern Kontrolle über ihre persönlichen Daten zu ermöglichen.

### **3. Die fünf Vorschläge, die die Privatsphäre am stärksten verletzen würden**

Unten stehend finden sich die fünf schlimmsten Änderungsvorschläge zur Datenschutzgrundverordnung, die von den Mitgliedern des LIBE-Ausschusses vorgeschlagen wurden. Jede Kategorie enthält eine kurze Analyse des Problemfeldes und eine Erklärung, warum die Änderungsvorschläge gefährliche Folgen für unsere Privatsphäre haben würden.

#### ***1. Verwässerung der Definition von "Einwilligung"***

Warum ist das ein Problem?

Einwilligung ist eine der rechtlichen Grundlagen für Datenverarbeitung. Sie wird regelmäßig missbraucht, vor allem online, wo Zustimmung oft auf vager oder verwirrender Sprache basiert. Manche Unternehmen sind der Meinung, dass bestimmte Verhaltensweisen, zum Beispiel die Anmeldung auf einer Webseite, bereits Einwilligung in die Nutzung von personenbezogenen Daten bedeuten.

Die Verordnung schreibt vor, dass die Einwilligung in die Datenverarbeitung in informierter, konkret fallbezogener und ausdrücklicher Art und Weise erfolgen muss. Das heißt, Nutzerinnen und Nutzer müssen eine echte Wahlmöglichkeit haben, die sicherstellt, dass sie wissen, welcher Art von Datenverarbeitung sie zustimmen.

Die Bürgerinnen und Bürger wollen jedoch mehr Kontrolle über die Nutzung ihrer Daten haben. In einer Befragung, die der englische Think Tank "Demos" im Jahr 2010 durchgeführt hat, wird eine Vielzahl von Forderungen hinsichtlich mehr Kontrolle laut. Das kann geschehen durch größere Transparenz und echte Einwilligung bei der Datenverarbeitung.<sup>7</sup>

Was würden die vorgeschlagenen Änderungsanträge bewirken?

Viele Änderungsvorschläge, die wir für diesen Bericht untersucht haben, würden die Definition von Einwilligung abschwächen, etwa indem sie das Wort "ausdrücklich" aus dem Text der Verordnung streichen oder durch vagere Formulierungen ersetzen. Das würde Unternehmen erlauben, die Einwilligung der Nutzerinnen und Nutzer in die Datenverarbeitung auf Grund einer Vermutung als ge-

---

<sup>7</sup> [http://www.demos.co.uk/files/Private\\_Lives\\_-\\_web.pdf](http://www.demos.co.uk/files/Private_Lives_-_web.pdf) (see for example page 94)

geben anzusehen oder die Einwilligungsbedingungen in schwer verständlichen Formulierungen zu verstecken.

## **2. Profilbildung ohne Zustimmung der Betroffenen**

Warum ist das ein Problem?

Die automatische Verarbeitung von personenbezogenen Daten, um daraus Schlüsse auf Gewohnheiten und Charaktereigenschaften zu ziehen, heißt "Profilbildung" (Profiling). Zu diesen Daten können zum Beispiel die Kreditwürdigkeit, der Aufenthaltsort oder sonstiges persönliches Verhalten zählen. Die so gewonnenen Informationen werden genutzt, um Entscheidungen zu treffen, die die Betroffenen in vielen Bereichen des Lebens beeinflussen - von Angeboten im Internet bis hin zum Kreditrating.

Die von der Europäischen Kommission vorgeschlagene Verordnung könnte erreichen, dass dieses Profiling nur stattfindet, wenn die Betroffenen klar zustimmen oder wenn es gilt einen Vertrag zu erfüllen (z.B. für einen Privatkredit). Für alle anderen Fälle sollte Profiling verboten werden. Es muss sichergestellt werden, dass jeder beeinflussen kann, was über ihn gesagt und wie er beurteilt wird.

Was würden die vorgeschlagenen Änderungsanträge bewirken?

Viele der von den Abgeordneten eingereichten Änderungsanträgen erkennen nicht die Gefahren von Profiling und gehen sogar so weit, Profiling ohne Zustimmung des Bürgers zu erlauben. Das hieße, dass jeder Bürger Gefahr läuft, ohne sein Wissen oder seine Zustimmung automatisch erfasst und bewertet zu werden - und das auch online.

## **3. Die erlaubte Nutzung von persönlichen Daten für alle möglichen Zwecke**

Warum ist das ein Problem?

Das Datenschutzrecht basiert auf dem Prinzip der "Zweckbindung". Die für einen Zweck gesammelten Daten können nicht für einen anderen wiederverwendet werden. Dies verhindert, dass ein Unternehmen durch eine Erhebung von Daten für einen scheinbar vernünftigen Zweck diese dann einfach weiterverwenden darf, ohne dass die Betroffenen widersprechen konnten.

Was würden die vorgeschlagenen Änderungsanträge bewirken?

Eine Reihe von Änderungsanträgen untergraben oder streichen sogar dieses Prinzip mit dem Vorschlag, dass die gesammelten Daten für den Zweck "A" ebenso für einen völlig anderen Zweck und ohne Bezug für das gleiche oder sogar in einigen Fällen für ein anderes Unternehmen wiederverwendet werden können. Dies würde den Bürgerinnen und Bürgern all ihre Kontrolle über ihre eigenen Daten entziehen – Unternehmen und Regierungen könnten diese Daten kostenlos nutzen. Dies würde Menschen zurücklassen, die fast kein Wissen von oder Kontrolle darüber haben, wie ihre Daten genutzt werden.

#### **4. Geschäftsinteressen vs. Rechte der Bürgerinnen und Bürger**

Warum ist das ein Problem?

Firmen rechtfertigen die Verarbeitung von Daten oft mit ihren "berechtigten Interessen", einer Formulierung, die auch im Kommissionsentwurf vorkommt und es ermöglicht, dass "berechtigte Geschäftsinteressen" den Vorrang bekommen vor den Rechten und Interessen der Bürgerinnen und Bürger.

Recherchen haben gezeigt, dass Unternehmen diese Begründung oft missbrauchen - zum Beispiel hat sie Google gestattet, die Datenschutzrichtlinien ihrer verschiedenen Dienste zusammenzufassen und hat Google damit erlaubt, die Daten von all ihren Diensten für jeglichen Zweck zu kombinieren<sup>8</sup>. Nutzer haben oft keinen Zugang zu Informationen darüber, wann diese Begründung genutzt wird und welche Interessen dadurch bedient werden.

Was würden die vorgeschlagenen Änderungsanträge bewirken?

Statt diese falsche Rechtfertigung abzuschaffen, schlagen die Mitglieder des Europäischen Parlaments vor, sie durch die Einbeziehung der Interessen Dritter zu erweitern. Dies wird es Unternehmen, von denen die jeweils betroffenen Bürgerinnen und Bürger noch nie gehört haben, ermöglichen, personenbezogene Daten dieser Menschen zu verarbeiten - auf Grundlage der Annahme, es sei im berechtigten Interesse der Firma. Dadurch würde ein bereits großes Schlupfloch noch größer gemacht werden und alle Arten von Verarbeitung ohne Zustimmung des Einzelnen ermöglicht.

#### **5. Die Einführung der sogenannten "pseudonymen Daten"**

Warum ist das ein Problem?

Es gibt Methoden, mit denen versucht wird, Datensätze zu "anonymisieren". Die Datensätze, auf die diese Methoden angewendet werden, erwecken den Anschein, als seien die Personen, deren Daten gespeichert wurden, nicht mehr identifizierbar. Mit dem Begriff "Pseudonymisierung" werden eine Vielzahl von Techniken bezeichnet, mit denen versucht wird, Daten nur in Kombination mit anderen Daten identifizierbar zu machen.

Das Gegenteil ist in der Tat wahr. Selbst wenn ein Unternehmen "pseudonymisierte" Informationen über eine bestimmte Person (im Sinne von "Hr. Müllers" Name wird getrennt von anderen Informationen gespeichert und diese Information wird in einem separaten Datensatz als Satznummer "ABC123" gespeichert) können die Informationen weiterhin verwendet werden, um gezielte Erkenntnisse über Hr. Müller zu erhalten.

Darüber hinaus können die Daten, die vermutlich für "anonym" oder "anonymisiert" gehalten werden, in Wirklichkeit reidentifiziert werden. Zum Beispiel war es möglich, dass Personen identifiziert werden konnten, die an einer großen genomischen Studie teilgenommen hatten. Basierend auf den Genomen der Teilnehmer und anderen öffentlich zugänglichen Informationen konnte dies gesche-

---

<sup>8</sup> [https://www.bof.nl/live/wp-content/uploads/20121211\\_onderzoek\\_legitimate-interests-def.pdf](https://www.bof.nl/live/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf)



hen. Da sich Technologie und Technik ständig weiterentwickeln, wird es immer einfacher Reidentifikation von angeblich anonymisierten Datensätzen herzustellen.<sup>910</sup>

Was würden die vorgeschlagenen Änderungsanträge bewirken?

Viele Änderungsanträge bringen eine Definition von "pseudonymen Daten" ein. Diese basieren auf der falschen Annahme, dass die Verarbeitung pseudonymer Daten die Privatsphäre der Bürgerinnen und Bürger nicht beeinträchtigt. Das schlichte Entfernen von Namen verhindert nicht, dass die Daten für Targeting benutzt werden können.

Parlamentarier müssen erkennen, dass pseudonyme Daten de facto persönliche Daten sind und den vollen Schutz des Gesetzes verdienen. Pseudonymisierung könnte als nützliche zusätzliche Sicherheitsmaßnahme dienen, sollte jedoch nicht als eigene Kategorie mit weniger Rechten angelegt sein.

## 4. Empfehlungen und weiterführende Literatur

Wir fordern die Abgeordneten dazu auf, die in diesem Bericht analysierten Änderungsanträge abzulehnen. Stattdessen fordern wir die Abgeordneten dazu auf, eine Verordnung zu unterstützen, die es den Menschen ermöglicht Kontrolle über ihre Daten mittels eines durchsetzbaren Datenschutzrechts zu haben, engere Befreiungen und Ausnahmen zu diesen Rechten und stärkere Sanktionen einzufordern.<sup>11</sup>

### **Weitere Informationen:**

1. EU-Datenschutz in 10 Punkten  
[https://digitalegesellschaft.de/wp-content/uploads/2013/01/DG\\_Brussel\\_entscheidet\\_ueber\\_dine\\_Daten.pdf](https://digitalegesellschaft.de/wp-content/uploads/2013/01/DG_Brussel_entscheidet_ueber_dine_Daten.pdf)
2. EDRI's online information centre for the Data Protection Regulation: <http://protectmydata.eu/>
3. EDRI's have two "myth busting" briefings on the Data Protection Regulation:  
<http://www.privacycampaign.eu/2013/01/matierial/>
4. Open Rights Group brief guide to the issues:  
<http://www.openrightsgroup.org/ourwork/reports/data-protection-regulation:-a-brief-guide-to-the-issues>

### **Kontaktinformationen:**

Markus Beckedahl

Digitale Gesellschaft e. V.

---

<sup>9</sup> [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1740383](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1740383)

<sup>10</sup> <http://www.wired.com/wiredscience/2013/01/your-genome-could-reveal-your-identity/>

<sup>11</sup> EDRI: Key issues and what we need in the Regulation <http://www.privacycampaign.eu/wp-content/uploads/2013/02/Keyissues-EUDatAP.pdf>

Schönhauser Allee 6/7  
10119 Berlin

***Anhang: Die Änderungsanträge, die den meisten Schaden anrichten würden***

**1. Weakening the definition of consent**

AM757 (Jens Rohde, Adina-Ioana Vălean, ALDE);

AM758 (Louis Michel, ALDE);

AM760 (Lidia Joanna Geringer de Oedenberg S&D);

AM762 (Sarah Ludford, Charles Tannock, ALDE);

AM764 (Timothy Kirkhope, ECR);

AM765 (Axel Voss, Seán Kelly, Wim van de Camp, Hubert Pirker, Monika Hohlmeier, Georgios Panikolaou, Véronique Mathieu Houillon, Anna Maria Corazza Bildt, EPP)

AM766 (Agustín Díaz de Mera García Consuegra, Teresa Jiménez-Becerril Barrio, EPP);

(7)

**2. "Profiling" citizens without their consent**

AM1545 ((Alexander Alvaro, ALDE)

AM1547 (Jens Rohde, Adina-Ioana Vălean, ALDE);

AM1549 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, EPP)

AM1551 (Lidia Joanna Geringer de Oedenberg S&D);

AM1553 (Timothy Kirkhope, ECR);

AM1554 (Ewald Stadler)

AM1555 (Louis Michel, ALDE)

AM1556 (Jens Rohde, Adina-Ioana Vălean, ALDE);

AM1557 (Jens Rohde, Adina-Ioana Vălean, ALDE);

AM1560 ((Alexander Alvaro, ALDE)

AM1568 (Jens Rohde, Adina-Ioana Vălean, ALDE);

AM1572 (Axel Voss, EPP);

(12)

**3. Using personal data of citizens for all kinds of purposes**

Worst amendments proposed with respect to the 'purpose limitation principle'

AM818 (Jens Rohde, Adina-Ioana Vălean, ALDE)

AM819 (Louis Michel, ALDE)

AM944 (Alexander Alvaro, Nadja Hirsch, ALDE)

AM945 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Monika Hohlmeier, Lara Comi, Renate Sommer, EPP)

AM947 (Ewald Stadler)

AM948 (Jens Rohde, Adina-Ioana Vălean, ALDE)

(6)

#### 4. Business interests vs the rights of citizens

AM880 (Louis Michel, ALDE);

AM882 (Agustín Díaz de Mera García Consuegra, Teresa Jiménez-Becerril Barrio, EPP);

AM883 (Salvatore Iacolino, EPP);

AM884 (Ewald Stadler)

(4)

#### 5. The introduction and use of pseudonymous data

Worst amendments proposed in relation to the concept of 'pseudonymous' data

AM726 (Alexander Alvaro, ALDE);

AM729 (Sarah Ludford, ALDE);

AM730 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Renate Sommer, Monika Hohlmeier, Georgios Papanikolaou, Anna Maria Corazza Bildt, EPP).

AM732 (Adina-Ioana Vălean, Jens Rohde, ALDE);

AM851 (Alexander Alvaro, ALDE);

AM887 (Adina-Ioana Vălean, Jens Rohde, ALDE);

AM897 (Adina-Ioana Vălean, Jens Rohde, ALDE);

AM898 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Renate Sommer, Monika Hohlmeier, EPP);

AM900 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Renate Sommer, Monika Hohlmeier, EPP);

AM904 (Alexander Alvaro, Nadja Hirsch, ALDE);

AM921 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Renate Sommer, Monika Hohlmeier, EPP);

AM922 (Sabine Verheyen, Axel Voss, Anna Maria Corazza Bildt, Monika Hohlmeier, EPP)

AM1542 (Jens Rohde, Adina-Ioana Vălean, ALDE);

AM1543 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Renate Sommer, Monika Hohlmeier, EPP);

AM1568 (Jens Rohde, Adina-Ioana Vălean, ALDE);

AM1585 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Renate Sommer, Monika Hohlmeier, EPP);

AM1630 (Monika Hohlmeier, Axel Voss, EPP).

By group:

15 proposed by members of the EPP group.

24 amendments proposed by members of the ALDE group.

2 amendments from a member of the ECR group.

2 amendments from a member of the S&D group.

3 from an unattached member (Ewald Stadler).



Der Digitale Gesellschaft e.V. setzt sich für Bürger- und Verbraucherrechte ein.

Er klärt Öffentlichkeit, Politik und Bürger, Wirtschaft und Verbraucher über die Herausforderungen der Netzpolitik auf.

Wir verzichten bewusst auf Spenden von Konzernen, um unsere Unabhängigkeit zu wahren. Dafür sind wir in unserer Arbeit auf Ihre Unterstützung angewiesen: Helfen Sie uns mit einer Spende, damit wir weiterhin unbestechlich für Grund- und Verbraucherrechte eintreten können.

Nutzen Sie hierfür das Spendenformular unter [digitalegesellschaft.de/spenden](https://digitalegesellschaft.de/spenden) oder überweisen Sie Ihre Spende an:

Digitale Gesellschaft e.V.  
Konto-Nr: 1125012800  
BLZ: 430 609 67

Spenden verwalten wir dabei transparent und offen. Wir veröffentlichen einen jährlichen Tätigkeits- und Finanzbericht darüber, wofür welche Gelder konkret verwendet werden. Gleichzeitig berichten wir regelmäßig über unsere Aktivitäten und arbeiten an Möglichkeiten, Spender in Entscheidungen einzubinden.

Entscheidend für unsere Arbeit ist zudem eine stabile Basisfinanzierung, weil sie uns Unabhängigkeit und einen längeren Atem verschafft. Mit einer Fördermitgliedschaft leistest Du dazu einen wesentlichen Beitrag, dass wir noch besser gegen Industrielobby-Interessen und für mehr Bürgerrechte eintreten können.

Werde Fördermitglied unter: <https://digitalegesellschaft.de/foerdermitglied>

## Impressum

V.i.S.d.P.  
Markus Bechedahl  
Digitale Gesellschaft e. V.  
Schönhauser Allee 6/7  
10119 Berlin

<http://digitalegesellschaft.de/presse/>  
[presse@digitalegesellschaft.de](mailto:presse@digitalegesellschaft.de)

Unser Vorsitzender Markus Bechedahl ist unter 0177 7503541 erreichbar.