



Universität St.Gallen

Informationsrecht

Datenschutzrecht

Prof. Dr. iur. Daniel Hürlimann, Ass.-Prof. für Informationsrecht

23. März 2017

Überblick Datenschutzrecht

- Gesetz
 - Begriffe
 - Grundsätze
 - Auskunftsrecht
- Realität
 - Big Data
 - Grenzüberschreitende Datenflüsse
 - Relativierung der Grundsätze mittels AGB
- Fälle
 - Logistep-Urteil des BGer
 - Google-Urteil des EuGH
 - Safe-Harbor-Urteil des EuGH

Aktuell: Datenpolitik

Auf dem Weg zu einer Datenpolitik des Bundes

Bern, 22.03.2017 - Die Schweiz soll über kohärente Rechtsgrundlagen zu Daten und den Umgang mit ihnen verfügen und sich als attraktiven Standort für eine Wertschöpfung durch Daten positionieren. Zu diesem Zweck hat der Bundesrat an seiner Sitzung vom 22. März 2017 übergeordnete Ziele definiert und die Bundesverwaltung beauftragt, erste Eckwerte einer Datenpolitik zu entwerfen. Er stellt auch fest, dass Daten der Rohstoff einer digitalen Wirtschaft und Gesellschaft sind. Geeignete Datenbestände sollen deshalb für eine Wiederverwendung zur Verfügung stehen. Die Entwicklung einer Datenpolitik ist integraler Bestandteil der Strategie "Digitale Schweiz", die der Bundesrat im April 2016 verabschiedet hat.

- EJPD soll bis Ende 2017 die Rechtslage für eine Weiterverwendung von Personendaten, Sachdaten und anonymisierten Daten analysieren.
- EDI inventarisiert die Datenbestände des Bundes, um für die Publikation auf opendata.swiss geeignete Daten zu identifizieren

tinyurl.com/datenpolitik

Überblick Datenschutzgesetz

1. Abschnitt: Zweck, Geltungsbereich und Begriffe
2. Abschnitt: Allgemeine Datenschutzbestimmungen
3. Abschnitt: Bearbeiten von Personendaten durch private Personen
4. Abschnitt: Bearbeiten von Personendaten durch Bundesorgane
5. Abschnitt: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
6. Abschnitt: Rechtsschutz
7. Abschnitt: Strafbestimmungen

Begriffsdefinitionen des DSGVO (Art. 3)

- Personendaten (Daten): alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen;
- Bearbeiten: jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten;
- Bekanntgeben: das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen;

Fall: Logistep

- Logistep AG sucht in P2P-Netzen nach urheberrechtlich geschützten Werken
- Strafanzeige gegen Unbekannt durch Rechtsinhaber
- Identitätsdaten im Rahmen des Akteneinsichtsrechts
- Schadenersatzforderungen
- EDÖB: Vorgehen der Logistep AG ist geeignet, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen
- Bundesverwaltungsgericht: nein ([Urteil A-3144/2008](#) vom 27. Mai 2009)
- Bundesgericht: doch ([BGE 136 II 508](#))

Fall: Logistep

- Sind dynamische IP-Adressen Personendaten?
- [BGE 136 II 508 E. 3.5.:](#)

”Für den vorliegenden Fall ist die Bestimmbarkeit der betroffenen Personen grundsätzlich zu bejahen. Auf ihr beruht ganz eigentlich das Geschäftsmodell der Beschwerdegegnerin. Diese zeichnet nach eigenen Angaben dynamische IP-Adressen möglicher Urheberrechtsverletzer sowie weitere Daten auf, welche sie den Rechteinhabern weitergibt. Die Rechteinhaber ihrerseits können durch Strafanzeige auf die Einleitung eines Strafverfahrens hinwirken, um in dessen Rahmen Akteneinsicht zu nehmen und so den P2P-Teilnehmer ausfindig zu machen, welcher das urheberrechtlich geschützte Werk unrechtmässig angeboten hat.”

Grundsätze des DSG (Art. 4)

¹ Personendaten dürfen nur rechtmässig bearbeitet werden.

² Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.

³ Personendaten dürfen **nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.**

⁴ Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung **müssen für die betroffene Person erkennbar sein.**

⁵ Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen.

Grundsätze des DSGVO (Art. 4)

¹ Personendaten dürfen nur rechtmässig bearbeitet werden.

² Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.

³ Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

⁴ Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein.

⁵ Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt.

Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen.

Aufhebung der DSGVO-Grundsätze mittels AGB

Art. 4 Abs. 5 DSGVO: “Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen.”

David Vasella, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, in: Jusletter 16. November 2015 ([tinyurl.com/vasella-dsg](https://www.tinyurl.com/vasella-dsg))

c. Ausdrücklich können z.B. folgende Einwilligungserklärungen sein:

- Gesten, z.B. Kopfnicken oder eindeutige Handzeichen;
- schriftliche Einwilligungserklärung;
- mündliche Einwilligungserklärung;⁹⁴
- **Anklicken einer Checkbox auf einer Internetseite;**⁹⁵
- **Anklicken einer Schaltfläche wie etwa «weiter» bei einem Internetformular;**⁹⁶

Grenzüberschreitende Bekanntgabe (Art. 6 DSGVO)

¹ Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.

² Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn:

- a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten;
- b. die betroffene Person im Einzelfall eingewilligt hat;
- c. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt;
- d. die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist;
- e. die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen;
- f. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat;
- g. die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten.

Safe Harbor

- Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes
- Wird *Safe-Harbor-Abkommen* genannt, weil das Vorgehen mit den USA abgesprochen war
- US-Unternehmen konnten dem Safe Harbor beitreten und sich auf der entsprechenden Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichten, die Safe Harbor Principles zu befolgen.

Safe Harbor

- bis September 2015 ca. 5500 US-Unternehmen dem Safe-Harbor-Abkommen beigetreten, darunter IBM, Microsoft, Amazon, Google, Dropbox, Facebook
- Max Schrems, europe-v-facebook.org
- 16 Anzeigen beim irischen Data Protection Commissioner
- Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom High Court (Irland)
- Urteil des EuGH vom 6. Oktober 2015: Safe-Harbor-Entscheidung der EU-Kommission ungültig

Urteil des EuGH vom 6. Oktober 2015

- Rn. 94: Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens.
- Rn. 97: Die Kommission hat jedoch in der Entscheidung 2000/520 nicht festgestellt, dass die Vereinigten Staaten von Amerika aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein angemessenes Schutzniveau „gewährleisten“.
- Rn. 98: Daher ist, ohne dass es einer Prüfung des Inhalts der Grundsätze des „sicheren Hafens“ bedarf, der Schluss zu ziehen, dass Art. 1 der Entscheidung 2000/520 gegen die in Art. 25 Abs. 6 der Richtlinie 95/46 im Licht der Charta festgelegten Anforderungen [“angemessenes Schutzniveau”] verstößt und aus diesem Grund ungültig ist.

Situation in der Schweiz

- Urteil des EuGH gilt nur für EU-Mitgliedstaaten
- EDÖB: Safe Harbor CH ist aus vom EuGH angeführten Gründen ungenügend
- Safe-Harbor-Abkommen vom Bundesrat im Januar 2017 formell aufgehoben
- Swiss-US Privacy Shield: neuer Rahmen für die Übermittlung von Personendaten aus der Schweiz an Firmen mit Sitz in den USA
- USA auf Liste der Staaten mit angemessener Datenschutzgesetzgebung ([Art. 7 VDSG](#))
- US-Unternehmen können sich ab dem 12. April 2017 nach dem Swiss-US Privacy Shield zertifizieren und sich somit dessen Prinzipien unterwerfen

Übergangslösung bis 12. April 2017

- Bis die Möglichkeit zur Zertifizierung besteht, empfiehlt der EDÖB, beim Datenaustausch mit US-Unternehmen vertragliche Garantien im Sinne von [Art. 6 Abs. 2 lit. a DSGVO](#) zu vereinbaren. Folgendes muss dabei geregelt werden:
 - Personen, deren Daten in die USA übermittelt werden, müssen klar und umfassend über die möglichen Behördenzugriffe informiert werden, damit sie ihre Rechte wahrnehmen können. Der Vertrag zum Austausch von Personendaten sollte die beteiligten Parteien dahingehend verpflichten.
 - Die Parteien müssen sich verpflichten, betroffenen Personen die für einen wirksamen Rechtsschutz notwendigen Behelfe zur Verfügung zu stellen, entsprechende Verfahren tatsächlich durchzuführen und darauf ergehende Urteile zu akzeptieren.

Verbesserungen Privacy Shield ggü. Safe Harbor

- Verstärkung der Anwendung der Datenschutzprinzipien
- Überwachung des Rahmens durch die US-Behörden
- Schlichtungsorgan zur Behandlung von Streitigkeiten, die über die anderen verfügbaren Beschwerdewege nicht gelöst werden
- In der Schweiz ansässige Personen können Anfragen bezüglich der Bearbeitung ihrer Daten durch US-Nachrichtendienste an eine Ombudsperson im amerikanischen Aussenministerium richten
- Regelung entspricht der Lösung zwischen den USA und EU/EWR

Auskunftsrecht (Art. 8 DSGVO)

¹ Jede Person kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden.

² Der Inhaber der Datensammlung muss der betroffenen Person mitteilen:

- a. alle über sie in der Datensammlung vorhandenen Daten einschliesslich der verfügbaren Angaben über die Herkunft der Daten;
- b. den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens sowie die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger.

Exkurs: Recht auf Kopie

15.4045 POSTULAT

Recht auf Nutzung der persönlichen Daten. Recht auf Kopie

Eingereicht von:



DERDER FATHI
FDP-Liberale Fraktion
FDP.Die Liberalen

Einreichungsdatum: 25.09.2015

Eingereicht im: Nationalrat

Stand der Beratungen: Angenommen

☰ ALLES ZUKLAPPEN

☶ EINGEREICHTER TEXT

Der Bundesrat wird beauftragt, zu prüfen und Bericht zu erstatten, inwiefern der Einzelne und die Volkswirtschaft von der Weiterverwendung von personenbezogenen Daten profitieren könnten. Insbesondere soll er dabei ein "Recht auf Kopie" für den Einzelnen prüfen.

tinyurl.com/rechtaufkopie

Stellungnahme des BR vom
11. November 2015: Prüfung
wird im Rahmen der
DSG-Revision vorgenommen

Bearbeiten v. Personendaten durch private Personen

- Art. 12 Abs. 1 DSG: “Wer Personendaten bearbeitet, darf dabei die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen.”
- Insbesondere-Auflistung in [Art. 12 Abs. 2 DSG](#)
- Art. 13 Abs. 1 DSG: “Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.”
- Insbesondere-Auflistung in [Art. 13 Abs. 2 DSG](#)
- Rechtsansprüche in [Art. 15 DSG](#)

Fall: Logistep

- Verstoss gegen die Grundsätze der Zweckbindung und der Erkennbarkeit?
- [Art. 4 DSGVO](#): Grundsätze
- Verstoss bejaht von BVGer und BGer
- Rechtfertigung wegen überwiegendem Privatinteresse?
 - Bundesverwaltungsgericht: ja
 - Bundesgericht: nein

Fall: Logistep

BGE 136 II 508 E. 6.3.3:

“Mithin vermag auch das Interesse an der wirksamen Bekämpfung von Urheberrechtsverletzungen die Tragweite der Persönlichkeitsverletzung und der mit der umstrittenen Vorgehensweise einhergehenden Unsicherheiten über die Datenbearbeitung im Internet nicht aufzuwiegen. Ein überwiegendes privates oder öffentliches Interesse ist umso mehr zu verneinen, als dieses nur zurückhaltend bejaht werden darf. Die Rüge des Beschwerdeführers erweist sich somit als begründet, was zur Gutheissung der Beschwerde führt.”

Bearbeiten v. Personendaten durch Bundesorgane

- Art. 17 Abs. 1 DSG: “Organe des Bundes dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht.”
- Art. 17 Abs. 2 DSG: Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen sie nur bearbeiten, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht oder wenn ausnahmsweise: [\[Aufzählung\]](#).
- Art. 19 Abs. 1 DSG: Bundesorgane dürfen Personendaten nur bekannt geben, wenn dafür eine Rechtsgrundlage im Sinne von Artikel 17 besteht oder wenn: [\[Aufzählung\]](#).

Bearbeiten v. Personendaten durch Bundesorgane

Art. 25 DSG: Ansprüche und Verfahren

¹ Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, dass es:

- a. das widerrechtliche Bearbeiten von Personendaten unterlässt;
- b. die Folgen eines widerrechtlichen Bearbeitens beseitigt;
- c. die Widerrechtlichkeit des Bearbeitens feststellt.

² Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten bewiesen werden, so muss das Bundesorgan bei den Daten einen entsprechenden Vermerk anbringen.

Eidg. Datenschutz- und Öffentlichkeitsbeauftragter

- [Art. 27 DSG](#): Aufsicht über Bundesorgane (Beispiel: Swiss Pass)
- Art. 28 DSG: Beratung Privater
- Art. 29 DSG: Abklärungen und Empfehlungen im Privatrechtsbereich (Beispiel: Logistep)
- Art. 33 Abs. 1 DSG: “Der Rechtsschutz richtet sich nach den allgemeinen Bestimmungen über die Bundesrechtspflege.”
- [Art. 35 VGG](#): “Das Bundesverwaltungsgericht beurteilt auf Klage als erste Instanz: ...” (Beispiel: Dignitas vs. SNF)

Datenschutz beim «Swiss Pass»

Im Rahmen des «Swiss Pass» müssen der Verband öffentlicher Verkehr (VöV) und die Schweizerischen Bundesbahnen (SBB) die bereits erhobenen Kontrolldaten der Passagiere löschen und den Betrieb der Kontrolldatenbank einstellen. Dies fordert der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) in seiner Empfehlung zuhanden der beiden Akteure. Zudem rät er ihnen, in den AGB zum Halbtax- und zum Generalabonnement transparenter über die Verwendung der Kundendaten zu informieren.

(Medienmitteilung des EDÖB vom 17. Februar 2016, [tinyurl.com/edoeb-sbb](https://www.tinyurl.com/edoeb-sbb))

Datenschutz beim «Swiss Pass»

Medienmitteilung, 29. Februar 2016



Datenschutzbeauftragter überprüft den SwissPass: VöV und SBB sind sich mit dem Datenschutzbeauftragten einig.

Der Verband öffentlicher Verkehr (VöV) und die SBB haben in ihrer Stellungnahme dem eidgenössischen Datenschutzbeauftragten (EDÖB) mitgeteilt, dass sie den Vorschlägen und Empfehlungen aus dem Schlussbericht zum SwissPass folgen werden. Der Betrieb der Kontrolldatenbank wird per Ende März 2016 eingestellt. Die öV-Branche strebt klare Rechtsgrundlagen an, die eine Weiterentwicklung von kundenfreundlichen Tarifsystemen ermöglichen.

tinyurl.com/sbb-edoeb

Reform des europäischen Datenschutzrechts

- Einigung über die EU-Datenschutzreform am 15. Dezember 2015
 - einfacherer Zugang zu den eigenen Daten
 - Recht auf Datenübertragbarkeit
 - Klärung des „Rechts auf Vergessenwerden“
 - Recht zu erfahren, ob Daten gehackt wurden
- **Art. 18 Datenschutz-Grundverordnung: Recht auf Datenübertragbarkeit**

Abs. 1: “Werden personenbezogene Daten elektronisch in einem strukturierten gängigen elektronischen Format verarbeitet, hat die betroffene Person das Recht, von dem für die Verarbeitung Verantwortlichen eine Kopie der verarbeiteten Daten in einem von ihr weiter verwendbaren strukturierten gängigen elektronischen Format zu verlangen.”

Reform des schweizerischen Datenschutzrechts

- Vorentwurf vom 21. Dezember 2016 für totalrevidiertes Datenschutzgesetz
- Vernehmlassung läuft bis 4. April 2017
- Neuerungen:
 - Informationspflichten der Datenverarbeiter
 - Präzisierung des Auskunftsrechts
 - Selbstregulierung durch Empfehlungen des EDÖB
 - Stärkung der Aufsichtskompetenzen des EDÖB
 - Erleichterung der Bekanntgabe von Daten ins Ausland
 - Abschaffung des Datenschutzes für juristische Personen
 - Verschärfung der Strafbestimmungen
 - kein Recht auf Datenportabilität, kein Recht auf Vergessenwerden

Urteil des EuGH: Google gegen Mario Costeja

- Beschwerde gegen Tageszeitung und gegen Google
- Antrag: Seiten löschen oder nicht mehr anzeigen/verlinken
- Seiten enthielten eine Anzeige, in der unter Nennung des Namens des Betroffenen auf die Versteigerung eines Grundstücks hingewiesen wurde
- Veröffentlichung erfolgte auf Anordnung einer staatlichen Behörde
- Entscheid der spanischen Datenschutzbehörde: Tageszeitung muss die Seite nicht löschen, aber Google muss Links entfernen
- Weiterzug an Audiencia Nacional, Vorlagefrage an EuGH

Urteil des EuGH: Google gegen Mario Costeja

Von Suchmaschinenbetreiber ausgeführte Verarbeitung kann die Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten erheblich beeinträchtigen, wenn die Suche mit dieser Suchmaschine anhand des Namens einer natürlichen Person durchgeführt wird, da diese Verarbeitung es jedem Internetnutzer ermöglicht, mit der Ergebnisliste einen strukturierten Überblick über die zu der betreffenden Person im Internet zu findenden Informationen zu erhalten, die potenziell zahlreiche Aspekte von deren Privatleben betreffen und ohne die betreffende Suchmaschine nicht oder nur sehr schwer hätten miteinander verknüpft werden können, und somit ein mehr oder weniger detailliertes Profil der Person zu erstellen. (Randnummer 80 des [Urteils](#))

Urteil des EuGH: Google gegen Mario Costeja

Wegen seiner potenziellen Schwere kann ein solcher Eingriff nicht allein mit dem wirtschaftlichen Interesse des Suchmaschinenbetreibers an der Verarbeitung der Daten gerechtfertigt werden. Da sich die Entfernung von Links aus der Ergebnisliste aber je nach der Information, um die es sich handelt, auf das berechnete Interesse von potenziell am Zugang zu der Information interessierten Internetnutzern auswirken kann, ist ein angemessener Ausgleich u. a. zwischen diesem Interesse und den Grundrechten der betroffenen Person zu finden. Zwar **überwiegen die durch diese Artikel geschützten Rechte der betroffenen Person im Allgemeinen gegenüber dem Interesse der Internetnutzer; ...** (Randnummer 81 des [Urteils](#))

Schlussanträge des Generalanwalts

- Ausführliche Überlegungen zur grundrechtlichen Dimension des Falles (fehlen im Urteil des EuGH)
- “Angesichts der besonders komplexen und schwierigen Grundrechtskonstellation im vorliegenden Fall **lässt es sich nicht rechtfertigen**, die nach Maßgabe der Richtlinie bestehende Rechtsstellung der betroffenen Personen zu verstärken und um **ein Recht auf Vergessenwerden zu ergänzen**. Andernfalls würden entscheidende Rechte wie die Freiheit der Meinungsäußerung und die Informationsfreiheit geopfert.” (Randnummer 133 der [Schlussanträge](#))

Schlussanträge des Generalanwalts

“Ich möchte dem Gerichtshof auch abraten, in seinem Urteil zu dem Ergebnis zu gelangen, dass diese einander widerstreitenden Interessen im jeweiligen Einzelfall auf zufriedenstellende Weise in ein Gleichgewicht gebracht werden können und dass die Entscheidung dem Internetsuchmaschinen-Diensteanbieter überlassen bleibt. Derartige Verfahren zur Meldung und Entfernung, sollte der Gerichtshof sie vorschreiben, werden wahrscheinlich entweder zu einer automatischen Löschung von Links zu beanstandeten Inhalten oder zu einer von den beliebtesten und wichtigsten Internetsuchmaschinen-Diensteanbietern nicht zu bewältigenden Anzahl von entsprechenden Anträgen führen.”

(Randnummer 133 der [Schlussanträge](#))

Schlussanträge des Generalanwalts

“Vor allem sollten die Internetsuchmaschinen-Diensteanbieter nicht mit einer solchen Pflicht belastet werden. Es käme zu einem Eingriff in die Freiheit der Meinungsäußerung des Webseitenurhebers, der in einem solchen Fall ohne angemessenen Rechtsschutz bliebe, da ein unregelmäßiges Verfahren zur Meldung und Entfernung eine privatrechtliche Angelegenheit zwischen der betroffenen Person und dem Suchmaschinen-Diensteanbieter wäre. Dies liefe auf eine **Zensur** der vom Urheber veröffentlichten Inhalte durch einen Privaten hinaus. Auf einem ganz anderen Blatt steht hingegen, dass den Staaten die Handlungspflicht obliegt, gegen einen das Recht auf Privatleben verletzenden Verleger einen wirksamen Rechtsbehelf vorzusehen, der im Kontext des Internets gegen den Webseitenurheber gerichtet wäre.”
(Randnummer 134 der [Schlussanträge](#))

Beurteilung des Google-Falls nach Schweizer Recht

- DSG entspricht weitestgehend der EU-Datenschutzverordnung
- Grundrechtliche Ausgangslage nahezu identisch
- Rechtfertigungsgründe nach [Art. 13 Abs. 1 DSG](#)
- m.E. können Suchmaschinenbetreiber nicht dazu verpflichtet werden, rechtmässige Informationen aus den Ergebnislisten zu entfernen



Jimmy Wales ✓

@jimmy_wales



 Folgen

When will a European Court demand that Wikipedia censor an article with truthful information because an individual doesn't like it?