zeppelin universität

zwischen
Wirtschaft Kultur Politik

# Zukunftsforum Open Government

## #ZOG 13

Dokumentation der Veranstaltung
am 08. November 2013
an der Zeppelin Universität in Friedrichshafen

Prof. Dr. Jörn von Lucke
Deutsche Telekom Institute for Connected Cities
Zeppelin Universität Friedrichshafen

**Jörn von Lucke**

Prof Dr

Lehrstuhl für Verwaltungs-
und Wirtschaftsinformatik

Deutsche Telekom Institute
for Connected Cities (TICC)

Fon +49 7541 6009-1471
Fax +49 7541 6009-1499

http://ticc.zu.de

Zeppelin Universität gemeinnützige GmbH
Am Seemooser Horn 20 88045 Friedrichshafen | Bodensee

## Vorwort

Am 08.11.2013 fand an der Zeppelin Universität in Friedrichshafen das Zukunftsforum Open Government statt. Nach einer Eröffnungsrede von Herrn Staatssekretär Dr. Wilfried Bernhardt und einer anschließenden Podiumsdiskussion diskutierten rund 50 Teilnehmer in vier Panels über den Stand und die Zukunft von Open Government in Deutschland, die Möglichkeiten für Cloud Computing in der Verwaltung und über IT-Sicherheit und Vertrauen in Zeiten Von PRISM, Tempora & Co. Im Folgenden fassen wir die zentralen Diskussionspunkte für Sie zusammen.

Das vollständige Protokoll finden Sie unter:
http://www.zu.de/deutsch/lehrstuehle/ticc/TICC-131108-Protokoll_ZOG13_Zeppelin_Universitaet.pdf

Niederschrift der Eröffnungsrede von Staatssekretär Dr. Wilfried Bernhardt:
http://www.zu.de/deutsch/lehrstuehle/ticc/TICC-131108-Keynote_Bernhardt-ZOG-Friedrichshafen-V2.pdf

Fotos der Veranstaltung von Tom Schlansky, Verwendung unter CC BY:
https://drive.google.com/folderview?id=0B731z9dFnyHPZFlnZzFuUjYwd2c&usp=sharing

Wir möchten uns noch einmal bei allen Gästen und Teilnehmern für die interessanten Impulse, Gespräche und Diskussionen bedanken. Gemeinsam können wir Open Government in Deutschland gestalten und voranbringen.

Jörn von Lucke, Dirk Heckmann und Katharina Große

# Inhalt

## Eröffnungsrede: Das Internet nach der Wahl: Alles offen?

Das Zukunftsforum Open Government wurde von Staatssekretär Dr. Wilfried Bernhardt eröffnet, der sich mit den aktuellen deutschen Geschehnissen Rund um Open Government beschäftigte, offene Fragen aufwarf und Anforderungen aufzeigte, um offenes Regieren und Verwalten voranzubringen.

Eine Konsequenz der NSA-Affäre ist, dass bei der Diskussion um „Offenheit" momentan primär der Gedanke an unsere Offenheit gegenüber fremden Geheimdiensten im Vordergrund steht. Zwar war dies nicht unbedingt relevant für die Wahl, aber die Ausspähung von Angela Merkels Handy bekommt weiterhin große Aufmerksamkeit. Die Diskussion sollte sich aber eigentlich nicht nur um die Bundeskanzlerin drehen, sondern auch um Lieschen Müller. Die Privatsphäre jedes einzelnen ist ebenso wichtig. Es gilt daraus die Lehre zu ziehen, dass Transparenz und Offenheit nie isoliert zu betrachten sind, sondern immer auch in Verbdingung mit Datenschutz und –sicherheit gesehen werden müssen. Es muss die Frage gestellt werden: Was darf und soll transparent sein?

Abbildung 1: Staatssekretär Dr. Wilfried Bernhardt

In der Vergangenheit gab es viele Initiativen für transparenteres Regierungs- und Verwaltungshandeln. Sie äußerten sich z.B. Informationsfreiheitsgesetzen oder der PSI-Richtlinie. Bisher aber ist die Informationsfreiheit gekennzeichnet von einer Vielfalt an Ausnahmen, ein großer Teil der Informationen war nicht erhältlich. Das muss diskutiert werden. Wir brauchen ein Neu-Austarieren des Verhältnisses von Regierung und Bürger. Bernhardt wünscht sich einen Staat, der offen ist für Zusammenarbeit und transparenter und mündige Bürger, die sich einbringen. Dies wird unterstützt durch IT. Offene Daten, Informationsfreiheits-, Transparenz- und E-Government-Gesetze bilden den Rahmen.

Um dorthin zu gelangen müssen wir aber das „Tal der Enttäuschungen" durchschreiten, in dem sich Open Government laut Gartner momentan befindet. Es scheint, dass Open Government nicht gut genug in der Lebenswelt der Menschen verankert ist. Damit dies geändert werden kann und Open Government auf den „Pfad der Erleuchtung" gelangen kann, müssen einige strukturelle Herausforderung überwunden werden.

Wir müssen klare Vorgaben entwickeln, welche Daten wie zu veröffentlichen sind. Wir brauchen Prozessmanagement für die dazugehörigen Anläufe und elektronische Vorgangsbearbeitung. Verschiedene Open-Data-Portale müssen in ein übergreifendes Portal wie GovData integriert werden. Der IT-Planungsrat sollte als zentrales Steuerungsgremium fungieren. Es wird ein Gesamtansatz für die Nutzung von Open und Big Data benötigt und auch für die Eingabe und Pflege der Daten. Eine flächendeckende Breitbandversorgung ist essentiell. Beteiligungsangebote dürfen keine einseitigen Informationskanäle sein sondern

müssen dem Dialog dienen. Dabei ist es aber wichtig, die Verwaltung nicht zu überfordern und einige geschlossene Rückzugsräume aufrecht zu erhalten. Insgesamt muss eine Fehler- und Diskussionskultur gefördert werden.

Abschließend griff Dr. Bernhardt einige Fragen auf, die es zu diskutieren gilt. Darunter fällt zum Beispiel das Verhältnis zwischen großen Datenmengen und Transparenz. Wird diese durch Daten geschaffen oder durch die große Menge eher verhindert? Der Staatsekretär weist darauf hin, dass überlegt werden muss, wie multikanalfähige Angebote implementiert werden können und wie eine soziale Digital Divide vermieden wird. Mobiler Zugang wird an Relevanz gewinnen. Es muss diskutiert werden, welche Balance zwischen notwendiger Netzneutralität und durchaus üblichen Managed Services geschaffen werden kann. Auch ist fraglich, inwieweit Online-Beteiligung, die die repräsentative Demokratie nicht ersetzt sondern ergänzt, zu Verzögerungen bei der Gesetzgebung führt. Muss sich eventuell das Gesetzgebungsverfahren ändern? Brauchen wir überhaupt für alles Gesetze oder kann es eine neue Form der Verhaltensregel geben?

Staatssekretär Dr. Bernhardt macht deutlich, dass Verwaltung, Unternehmen und Bürger sich als Partner verstehen müssen, was aber Vertrauen und Freiheiten voraussetzt. Diese wird nicht nur durch Überwachung von außen gefährdet, sondern auch über Überlegungen zur Vorratsdatenspeicherung oder Mautüberwachungsstrukturen. Umso wichtiger ist es, dass ein offener Dialog geführt wird, der auch Skeptiker mitnimmt, denn Deutschland ist eine Demokratie, keine Expertokratie.

Insgesamt ergibt sich daraus der dringende Bedarf zum Ausbau der E-Kompetenz auf Seiten der Verwaltung. Dazu gehört nicht nur der Umgang mit Instrumente, sondern auch die Fähigkeit, Rahmenbedingungen und Schnittstellen zu schaffen. Bürger müssen an digitaler Souveränität dazugewinnen und an Medienkompetenz. Hier sind auch Schulen und Hochschulen in der Pflicht.

Werden all diese Anregungen in einem Nationalen Open Government Handlungsplan zusammengefasst, kann Open Government in Deutschland zu einer Erfolgsgeschichte werden.

## Podiumsdiskussion

*Podiumsgäste: Wilfried Bernhardt, Dirk Heckmann, Thomas Langkabel, Jörn von Lucke*
*Moderation: Wolfram Högel, Uwe Proll*

Die in der Eröffnungsrede wurden auch während der anschließenden Podiumsdiskussion kontrovers diskutiert. In den Mittelpunkt rückte erneut die Frage, warum Bürger erst nach Bekanntwerden der Ausspähung des Kanzlerinnenhandys ein Bewusstsein für Privatsphäre entwickelt haben. Es bestätigt sich hier, dass die Gefahren durch mangelnde IT-Sicherheit zu abstrakt für den Durschnitznutzer sind und erst anhand solcher Extrembeispiele an Substanz gewinnen.

Als weiter wichtiger Punkt drehte sich die Diskussion um den „politischen Willen", der als zentraler Erfolgsfaktor für Open Government dargestellt wurde. Dabei geht es nicht nur um

z.B. die Finanzierung von Open-Data-Projekten, sondern auch die stärkere Fokussierung auf Breitbandausbau oder die Erweiterung des Open Government Verständnisses auf mehr als offene Daten. Es wird dabei betont, dass es wichtig ist „machbare Themen" in den Blick zu nehmen, die die von Bernhardt in der Eröffnung angesprochene Bürgernähe herstellen können.

Für den weiteren Weg von Open Government wird es notwendig sein, unterschiedlichste Gruppen in die Neugestaltung einzubinden. Dazu gehören neben Bürgergruppen und zivilgesellschaftlichen Organisation auch Verwaltungen, die oft wegen großer Ressourcenknappheit derartigen Projekten skeptisch gegenüberstehen. Durch eine Kultur des Ausprobierens, speziell geförderte Pilotprojekte und dem Wissenstransfer aus diesen Experimenten können Bedenken abgebaut und gemeinsam an der Lösung von Umsetzungsproblemen gearbeitet werden. Die Prinzipien von Open Government bereits in der Gestaltung von Open Government anwenden – hier liegt der Schlüssel zum Erfolg.

## Panel 1: Gelebtes offenes Regierungs- und Verwaltungshandeln in Deutschland

*Panelisten: Jan-Ole Beyer, Christian Geiger, Beatrice Lederer*
*Moderation: Jörn von Lucke*

Die Panelisten eröffneten die Diskussion mit Impulsen zum GovData-Portal, zum Projekt ulm 2.0 und mit einer rechtlichen Einordnung von Open Government. Dabei wurde deutlich, dass die Bestreben nach mehr Offenheit auf Bundes-, Länder- und kommunaler Ebene durchaus auch aus der rechtlichen Grundlage als notwendig abgeleitet werden können.


Abbildung 2: Diskutieren und Arbeiten in den Panels

Weder diese Interpretation, noch das Bewusstsein für die Mehrwerte von Open Government sind aber bisher weit verbreitet. In der Diskussion wurde deutlich, dass mehr „Überzeugungsarbeit" notwendig, um die Öffnung von Regierung und Verwaltung in Deutschland voranzubringen, auch anhand von Positivbeispielen. Es wird eine „Marketing-Strategie" benötigt, der die Mehrwerte von zum Beispiel offenen Daten vermittelt. Dabei bietet es sich an, auf die kommunale Ebene zu fokussieren und Themen anzusprechen, die „nah am Bürger" sind. Bürger müssen Beteiligung „erleben" können und Spaß an der Mitarbeit haben.

Generell waren sich die Teilnehmer einig, dass Open Date noch ein neues Thema ist für Politik und Verwaltung, und sich Deutschland noch in der Lernphase ist. Es ist daher wichtig, Impulse aus verschiedenen Bereichen einzufangen, um potentielle Nutzen zu identifizieren und die Ansprüche, die Bürger und Wirtschaft an Open Data haben, besser abzubilden. Den

eigenen Lebensraum modellieren mit offenen Daten, Accountability fördern – noch nicht alle Potentiale der Nutzung von offenen Daten sind identifiziert.

Hieraus entwickelte sich die Diskussion um Big Data. Die Teilnehmer bezifferten bei diesem Thema den Bedarf, zum einen die Erforschung konkreter Auswertungsmöglichkeiten – auch in Zusammenarbeit mit der Wirtschaft – weiter voranzubringen. Dabei dürfen Einschränkungen zum Schutz der Privatsphäre aber nicht außer Acht gelassen werden. Besonders vor dem Hintergrund, dass die Bemühen von Unternehmen um Datenschutz noch häufig als unzureichend aufgefasst werden.

Als konkrete Impulse wurde der Bedarf nach mehr Unterstützung für die Kommunen formuliert. Dafür bieten sich zum Beispiel Rechenzentren an oder Wettbewerbe wie „Internetdorf des Jahres". Weiterhin wurde deutlich, dass eine klare Zielformulierung und Priorisierung notwendig sind, um Open Government in Deutschland voranzubringen.

## Panel 2: Gelebtes Regierungs- und Verwaltungshandeln in der Cloud

*Panelisten: Peter Bräutigam, Thorsten Hennrich, Matthias Kammer*
*Moderation: Dirk Heckmann*

Panel 2 widmete sich den Fragen, ob Cloud Computing (CC) im öffentlichen Sektor rechtlich zulässig ist und wie die sich daraus ergebenden Potentiale am besten genutzt werden können.

Abbildung 3: Engagierte Diskussion zu Cloud Computing

Während 2010 CC In Deutschland noch größtenteils auf Ablehnung stieß, wandelte sich in den letzten Jahren das Bild und CC wurde zur allgemein akzeptierten Lösung. Unter bestimmten Voraussetzung ist dies auch rechtlich zulässig, z.B. wenn es sich um Auftragsdatenverarbeitung handelt und die nötige Transparenz, Sicherheit und Zertifizierung gewährleistet ist. Daraus entstanden verschiedene Rahmenabkommen hervor. Das Safe-Harbor-Abkommen ermöglicht die Nutzung von Clouds in den USA. Für Unternehmen wurden EU Model Clauses gestaltet. Am Beispiel von CC in bayerischen Kommunen wird deutlich, dass CC durchaus eine bedeutende Rolle spielt und große Möglichkeiten zur Kostenersparnis und Standardisierung bietet. Dabei ist immer zu beachten, dass sensible, personenbezogene Daten nicht für CC geeignet sind. Es hat sich gezeigt, dass in der Zusammenarbeit mit Dienstleistern Vertrauen und ein Sicherheitsgefühl essentiell sind.

Es ist daher nicht verwunderlich, dass durch die Enthüllungen von Edward Snowden das Vertrauen in Cloud Computing einen herben Rückschlag erlitt. Von vielen Seiten wird als Konsequenz vorgeschlagen, zukünftig auf Europäische Dienste und „Cloud Services made in Germany" zurückzugreifen. Es muss aber dringend festgestellt werden, dass die keine

Lösung darstellt, weil nicht festgelegt ist, welchen Weg die Datenpakete nehmen und daher noch immer auf dem Radar ausländischer Geheimdienste sein können.

Dieser Aspekt wurde allerdings kontrovers diskutiert. Es gab auch Stimmen, die für ein funktionierendes regionales Internet argumentierten. Innerhalb von Behörden scheint es einen „Trend zur Regionalität" zu geben. Verschiedene Bundesländer haben bereits einen gemeinsamen IT-Dienstleister – ein erster Schritt zur Regionalisierung. Es gibt allerdings noch keine Cloud auf Bundesebene.

Es ist daher eine Grundsatzdiskussion, wie IT in der Verwaltung länderübergreifend organisiert werden kann. Der aktuelle Status muss erhoben werden. Vermutlich ist es nicht unbedingt nötig, auf externe Dienstleister im CC zurückzugreifen, sondern der bestehende öffentliche Anbieter ist effektiver und effizienter. Dazu braucht es aber ein Umdenken und den Willen zur Zusammenarbeit.

Daraus ergeben sich aber weitere Herausforderungen. Angreifer hätten in einer zentralen Bundes-Cloud einen einzigen Angriffspunkt, was großes Gefahrenpotential darstellt. Außerdem ist ein stabiler Betrieb essentiell. An dieser Stelle wird deutlich, dass eine Klassifizierung von Diensten erfolgen muss und dass das Design der Clouds daran angepasst werden muss: „Cloud ist nicht gleich Cloud." Abschließend ist es ebenfalls relevant zu erkennen, dass CC auf unterschiedlichen Ebenen Anwendung finden kann: bei Netzwerken, bei Hardware und bei Software. Diese Ebenen müssen differenziert betrachtet werden.

## Panel 3: Online-Brainstorming „Das Open Government der Zukunft"

*Panelisten: Katharin Große, Stephan Jaud, Celina Raffl*
*Moderation: Jörn von Lucke, Wolfram Högel*

In Panel 3 erarbeiteten die Teilnehmer gemeinsam mit Hilfe des Brainstorming-Tools MeetingSphere eine Ideensammlung zum Open Government der Zukunft. Angestoßen wurde die Diskussion von Katharina Große und Celina Raffl. Zunächst wurden Teilbereiche des Open Government aufgezeigt, die in Deutschland bisher weniger Beachtung finden. „Open Government ist bunter als gedacht". Vertiefend wurden die Konzepte „offene gesellschaftliche Innovation" und „eSociety" als neue Perspektiven vorgestellt.

Für die Wissenschaft wurden klare Arbeitsaufträge entwickelt, darunter zum Beispiel die Erforschung der tatsächlichen Bedürfnisse der Bürger und die Entwicklung einer gemeinsamen Strategie. Im Bereich der Dialog- und Partizipationsangebote wurde klar, dass es ständig offene Kanäle geben muss und verstärkt Wert darauf gelegt, dass zur Beteiligung notwendige Informationen gut aufbereitet und visualisiert werden. Open Data wird weiterhin als wichtiges Thema gesehen, dass durch eine Task-Force vorangebracht werden und verstärkt auch im schulischen Bereich Anwendung finden sollte. Dafür sind Vertrauen und Transparenz notwendig. Ein Kulturwandel zur mehr Offenheit kann aber nur mit einer Diskussion der Grenzen von Transparenz einhergehen und einer Debatte über Datenschutz.

Durch Open Government sind sowohl für die gemeinsame Erfüllung von Aufgaben große Schritte nach vorne als auch für die Demokratie an sich möglich. Dafür müssen aber Finanzierung und Infrastruktur verbessert werden. Breitbandausbau ist dabei ebenso relevant wie die Ermöglichung der Zusammenarbeit zwischen Bund, Länder und Kommunen. Um langfristige Finanzierung zu gewährleisten, wurde das Konzept der „Change Funds" als Lösung angeboten.

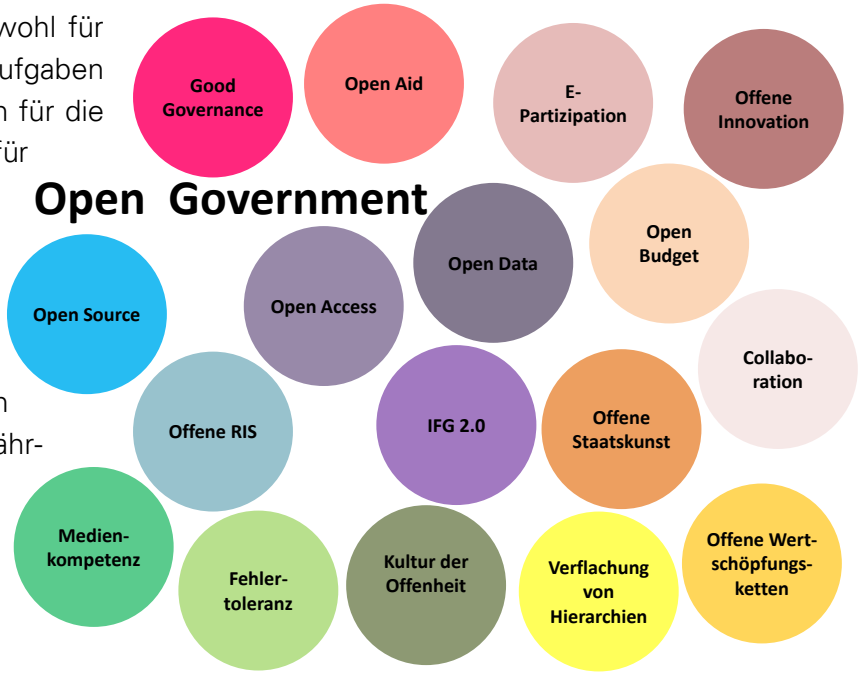


Abbildung 4: Open Government - bunter als gedacht

## Panel 4: Gewährleistung von IT-Sicherheit und Vertrauen trotz PRISM, Tempora & CO

*Panelisten: fukami, Till Kreutzer, Horst Samsel*
*Moderation: Dirk Heckmann*

Die Teilnehmer in Panel 4 stellten zunächst klar, dass IT-Sicherheit grundsätzlich nie hundertprozentig gewährleistet werden kann, sondern dass es sich immer um eine Risikoabwägung handelt. Das heißt, die Gewährleistung von IT-Sicherheit ist zwar das Ziel, was verfolgt wird, es kann aber nie erreicht werden.

Abbildung 5: Diskutanten und Moderator im Panel 4

Die Problematik, der sich IT-Sicherheitsexperten dabei gegenübersehen ist, dass die Erhöhung der Sicherheit Kosten verursacht und oft unbequem erscheint. Zusätzlich sind viele Risiken für Normalnutzer nicht wahrnehmbar. Deswegen werden geäußerte Bedenken oft nicht gehört. Das Bundesamt für Sicherheit in der Informationstechnik warnt beispielsweise seit 2000 der möglichen Spionage durch die NSA. Erst jetzt, nach den Enthüllungen durch Edward Snowden, stellt sich die Frage der IT-Sicherheit für den Bürger.

Die zentrale Frage bezüglich IT-Sicherheit ist inwieweit Bürger eigenverantwortlich für ihre Sicherheit sind oder in welchem Maße der Staat seinem Schutzauftrag nachkommen muss.

Dabei ist wichtig zu beachten, dass Schutz vor Überwachung nur eingeschränkt durch individuelle Abwehr des Bürgers gewährleistet werden kann. Dazu kommt noch, dass sich Nutzer zwar in der Verwendung bestimmter Dienste einschränken könnten. Das dies aber im Fall von sozialen Netzwerken zum Beispiel für Jugendliche keine einfache Entscheidung beziehungsweise faktisch unmöglich ist für. Ergänzt wird die Problematik für ein fehlendes Bewusstsein für die Notwendigkeit sich zu schützen. In Bezug auf technische Schutzmaßnahmen kommt hinzu, dass das Wissen fehlt und Kosten entstehen.

Als Konsequenz fordert das Panel deshalb a) drastischere politische Reaktionen, die in Abkommen und negative Regulierungen münden, b) ausreichende Default-Einstellungen zum Schutz der Nutzer und c) die Weiterentwicklung von Instrumenten und Software zum Schutze, die auch für Gelegenheitsnutzer anwendbar sind. Möglich wäre zum Beispiel eine Bestrafung von Software, die nicht regelmäßig verbessert und aktualisiert wird. Allerdings steht die Industrie höheren Standards und verstärkter Regulierung naturgemäß kritisch gegenüber.

Es wird weiter darauf hingewiesen, dass auch ein Kulturwandel unter Informatikern notwendig ist, die bisher eher provisorische und teilweise unsichere Lösungen entwickeln. Dieser würde allerdings Standardisierungen in der Software-Entwicklung voraussetzen, die nur schwer zu realisieren sind.

Abschließend bleibt festzustellen, dass es ein schwieriges Unterfangen wird, alle Schwachstellen zu schließen, durch die unter anderem die NSA Zugriff auf Daten und Systeme hat. Auch eine verstärkte Aufsicht von Geheimdiensten, wie von einigen Seiten gefordert, scheint nicht realistisch. Deshalb wird dafür argumentiert, verstärkt in Bildung und Aufklärung zur IT-Sicherheit zu investieren. Dies sollte auch in der Schulbildung ein zentraler Aspekt sein.