



Anforderungen an die Technik? Zur Regulierung des technischen Datenschutzes

Marit Hansen

Landesbeauftragte für Datenschutz Schleswig-Holstein

CAST-Forum „Recht und IT-Sicherheit“
Darmstadt, 23.03.2017



www.datenschutzzentrum.de

Überblick

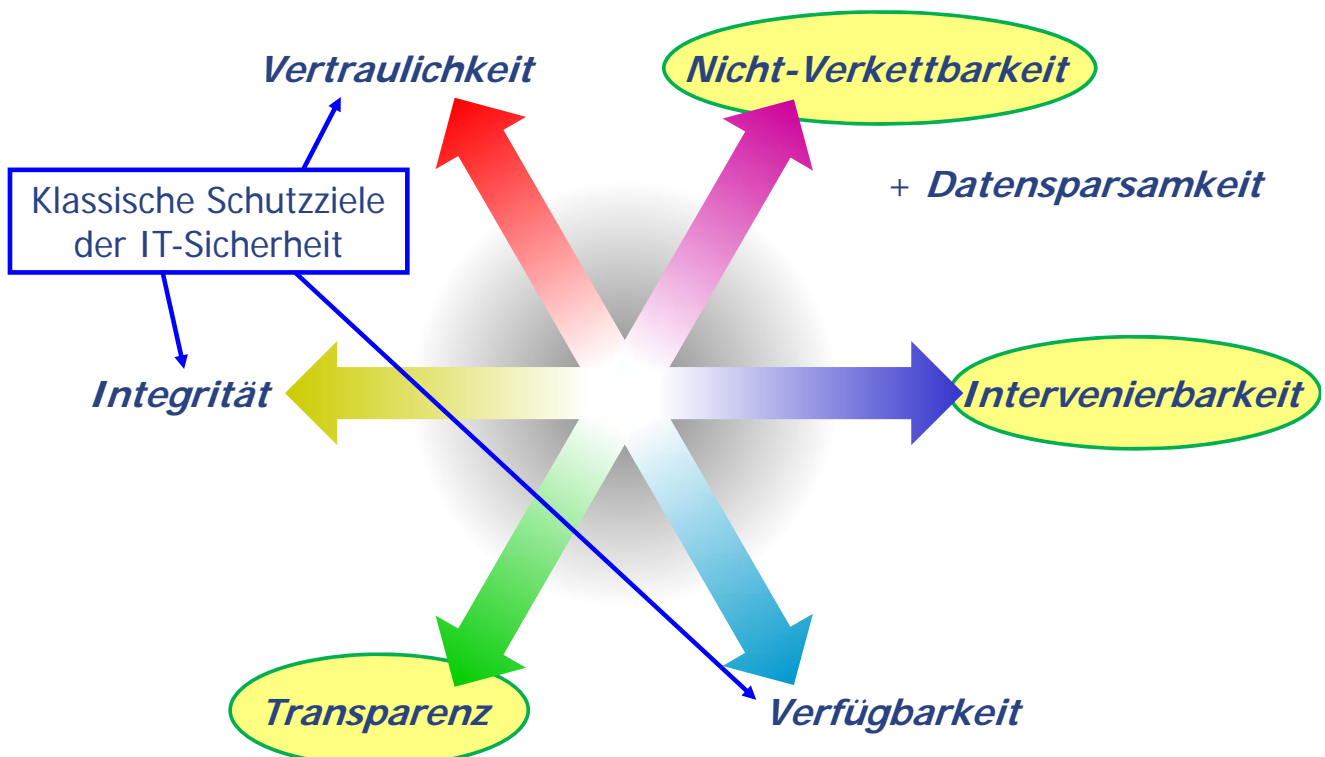
1. Technischer Datenschutz – Status Quo
2. Bisher in Deutschland
3. Technischer Datenschutz aus Europa
4. Umsetzung in Deutschland
5. Fazit

Was verstehe ich unter technischem Datenschutz?

- **Gestaltung** von IT-Systemen so, dass **Datenschutzanforderungen umgesetzt** werden (Systemdatenschutz)
 - Informationssicherheit (Art. 32 DSGVO)
 - Datenschutz (Art. 25 DSGVO)
- Untermenge von „Data Protection by Design and by Default“ (Systemgestaltung: mehr als IT!)
- Außerdem **Selbstdatenschutz**-Maßnahmen

Regulierung des technischen Datenschutzes

Gewährleistungsziele



Regulierung des technischen Datenschutzes

Wichtigkeit von „by Design“

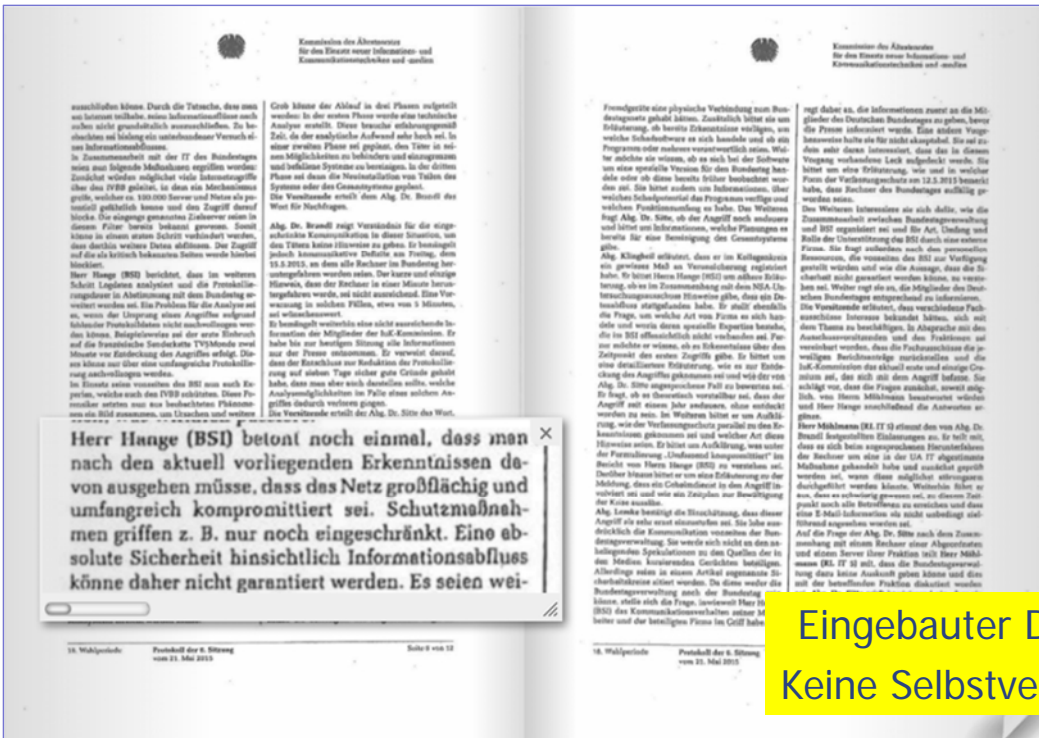
Erwägungsgrund 4

„The processing of personal data **should be designed** to serve mankind. [...]“

- Adressaten:
- Verantwortliche
 - Auftragsverarbeiter
 - Hersteller!

Regulierung des technischen Datenschutzes

Status Quo: brüchiges Fundament



Beispiel: „Bundestags-Hack“

Eingebauter Datenschutz: Keine Selbstverständlichkeit

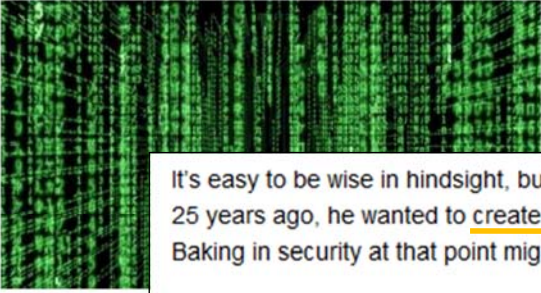
The Register
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE SCIENCE BOOTNOTES FORUMS

Security

Sir Tim Berners-Lee defends decision not to bake security into www

'The idea that privacy is dead is hopelessly sad'



More like this
Tim Berners-Lee

8 Oct 2014 at 12:24, John L...

IP Expo Sir Tim Berners-Lee wide web.

It's easy to be wise in hindsight 25 years ago, he wanted to Baking in security at that point

"[The web] might not have taken off this morning.

Sir Tim's views are in contrast regretted not building in security current push towards always-on more to do with timing and priorities than principles.

During a keynote presentation at the infrastructure conference, Sir Tim discussed a vision for the web where users are more in control of managing their privacy.

"The idea that privacy is dead is hopelessly sad," Sir Tim Berners-Lee said. "We have to build systems that allow for privacy."

http://www.theregister.co.uk/2014/10/08/sir_tim_bernerslee_defends_decision_not_to_bake_security_into_www/

Einbau schwierig

It's easy to be wise in hindsight, but Sir Tim explained that at the point he invented the world wide web 25 years ago, he wanted to create a platform that developers would find familiar and easy to use. Baking in security at that point might have worked against that goal, he said.

"[The web] might not have taken off if it had been too difficult," he told an audience at IPEXpo Europe this morning.

Sir Tim's views are in contrast with those of another internet pioneer, Vint Cerf, who recently said he regretted not building in security to basic internet protocols. Berners-Lee strongly supported the current push towards always-on crypto (https) for websites now underway, so his differing views are more to do with timing and priorities than principles.

„timing and priorities“
– Sicherheit kann nachrangig sein

Regulierung des technischen Datenschutzes

ULD

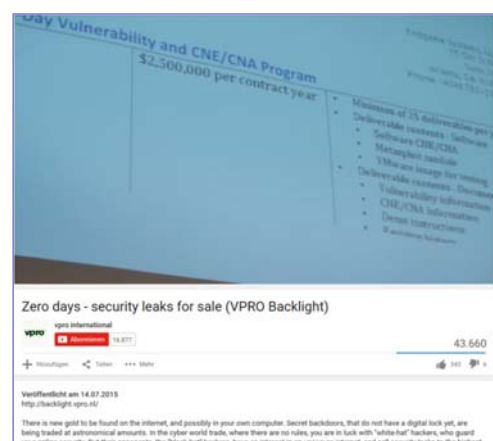


www.datenschutzzentrum.de

Alle wollen Sicherheit – oder?

- Massives Interesse an Unsicherheit

- **Lukrativer Markt** für Zero-Day-Exploits (Angriffsmöglichkeit, bevor es eine Gegenmaßnahme gibt; Entwickler haben 0 Tage Zeit zum Reagieren)



Zero days - security leaks for sale (VPRO Backlight)

VPRO International 43.660

Veröffentlicht am 14.07.2015
<http://backlight.vpro.nl/>

There is now gold to be found on the internet, and possibly in your own computer. Secret backdoors, that do not have a digital lock yet, are being traded at astronomical amounts. In the cyber world trade, where there are no rules, you are in luck with "white hat" hackers, who guard your online security. But their opponents, the "black hat" hackers, have an interest in an insecure internet, and sell security leaks to the highest bidder.

<http://tegenlicht.vpro.nl/backlight/zerodays.html>
<https://www.youtube.com/watch?v=4BTTiWkdT8Q>

- **Hintertüren:**
„insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets“
– NSA, Abt. TAO (Tailored Access Operations)

„Sicherheit“ ist nicht der Normalfall

Regulierung des technischen Datenschutzes

Überblick

1. Technischer Datenschutz – Status Quo
2. **Bisher in Deutschland**
3. Technischer Datenschutz aus Europa
4. Umsetzung in Deutschland
5. Fazit

Regulierung des technischen Datenschutzes

Technischer Datenschutz bisher in Deutschland

§ 3a BDSG Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die **Auswahl und Gestaltung von Datenverarbeitungssystemen** sind an dem **Ziel** auszurichten, **so wenig personenbezogene Daten wie möglich** zu erheben, zu verarbeiten oder zu nutzen.

Insbesondere sind personenbezogene Daten zu **anonymisieren** oder zu **pseudonymisieren**, **soweit** dies nach dem Verwendungszweck **möglich** ist und **keinen** im Verhältnis zu dem angestrebten Schutzzweck **unverhältnismäßigen Aufwand** erfordert.

Und wenn nicht?
Keine Sanktion.

§ 9 BDSG + Anlage (zu § 9 Satz 1 BDSG):
„xy-Kontrolle“ – na ja.

Regulierung des technischen Datenschutzes

Technischer Datenschutz bisher in Deutschland

- Anders in mehreren Landesdatenschutzgesetzen
 - **Schutzziel-Ansatz**
 - **Datenschutzverordnung** zum LDSG Schleswig-Holstein:
 - Dokumentationsanforderungen
 - (Rest-)Risikoanalyse
 - Test & Freigabe
 - Speziell: Notebookverschlüsselung

- Zusätzlich:
 - Sektorspezifische Regelungen

Antliche Abkürzung: DSVO	Quelle: 
Ausfertigungsdatum: 05.12.2013	Fundstelle: GVOBl. 2013, 554
Gültig ab: 01.01.2014	Gliederungs-Nr: 204-4-8
Gültig bis: 31.12.2018	
Dokumenttyp: Verordnung	

Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (Datenschutzverordnung - DSVO) Vom 5. Dezember 2013	
<small>Gesamtausgabe in der Gültigkeit vom 01.01.2014 bis 31.12.2018</small>	
Nichtamtliches Inhaltsverzeichnis	
Titel	Gültig ab
<small>Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (Datenschutzverordnung - DSVO) vom 5. Dezember 2013</small>	<small>01.01.2014 bis 31.12.2018</small>

Regulierung des technischen Datenschutzes

Überblick

1. Technischer Datenschutz – Status Quo
2. Bisher in Deutschland
3. **Technischer Datenschutz aus Europa**
4. Umsetzung in Deutschland
5. Fazit

Regulierung des technischen Datenschutzes

Technischer Datenschutz der DSGVO als „Game Changer“



Source: Johan Aulin

- **Marktortprinzip** (Art. 3 DSGVO)
- **Datenschutz „by design“** (Art. 25(1) DSGVO)
- **Datenschutz „by default“** (Art. 25(2) DSGVO)
- **Datenschutz-Folgenabschätzung** (Art. 35 DSGVO – „Rechte und Freiheiten natürlicher Personen“)
- **Zertifizierung** (Art. 42+43 DSGVO)
- **Bußgelder & Sanktionen** (Art. 83+84 DSGVO)
- **Gerichte**

Mächtige Toolbox, wenn entsprechend implementiert

Regulierung des technischen Datenschutzes

Datenschutz durch Technikgestaltung

Artikel 25 Datenschutz durch Technikgestaltung [...]

- (1) Unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen **Risiken für die Rechte und Freiheiten natürlicher Personen**

Viele möglicherweise begrenzende Bedingungen!

trifft der **Verantwortliche** sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung **geeignete technische und organisatorische Maßnahmen** – wie z. B. Pseudonymisierung – trifft, die **dafür ausgelegt sind**, die **Datenschutzgrundsätze** wie etwa Datenminimierung **wirksam umzusetzen** und die **notwendigen Garantien in die Verarbeitung aufzunehmen**, um den Anforderungen dieser **Verordnung** zu genügen und die **Rechte der betroffenen Personen** zu schützen.

Regulierung des technischen Datenschutzes

Begrenzung durch „Stand der Technik“ und „Implementierungskosten“?

Identische Formulierung in Art. 32 „Sicherheit der Verarbeitung“

<p style="text-align: center;">Artikel 25</p> <p style="text-align: center;">Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen</p> <p>(1) Unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung geeignete technische und organisatorische Maßnahmen, die den Grundsätzen wie etwa Datenminimierung entsprechen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:</p> <p>(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:</p> <p>(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 Absatz 1 kann als Mittel zur Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Pflichten angesehen werden.</p>	<p style="text-align: center;">Artikel 32</p> <p style="text-align: center;">Sicherheit der Verarbeitung</p> <p>(1) Unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:</p> <ol style="list-style-type: none"> a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten; b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen Zwischenfall rasch wiederherzustellen; d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. <p>(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.</p>
--	--

Begrenzung durch „Stand der Technik“ und „Implementierungskosten“?

<p style="text-align: center;">Article 17</p> <p style="text-align: center;">Security of processing</p> <p>1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.</p> <p>Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.</p> <p>2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.</p>	<p style="font-size: 1.2em;">Auf EU-Ebene nichts Neues, siehe EU-Datenschutz-Richtlinie 95/46/EG</p>
--	--

Begrenzung durch „Stand der Technik“ und „Implementierungskosten“?

Nicht enthalten in Art. 24 DSGVO: „Verantwortung“

Artikel 24

Verantwortung des für die Verarbeitung Verantwortlichen

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch

ErwGr 53 JI-RL:
„Die Umsetzung dieser Maßnahmen sollte nicht ausschließlich von wirtschaftlichen Erwägungen abhängig gemacht werden.“

gemäß Artikel 40
herangezogen werden

„Stand der Technik“ und
„Implementierungskosten“
können bei hohen Risiken
nicht als „Ausrede“ dienen
(z.B. Art. 36 Vorherige Konsultation)

des technischen Datenschutzes

Geeignete Basis für technischen Datenschutz?

- **Hersteller** sind nicht unmittelbar adressiert
- Indirekte Effekte möglich:
 - „... sollten die Hersteller der Produkte, Dienste und Anwendungen **ermutigt** werden ...“ (ErwGr 78)
 - Öffentliche **Ausschreibung** (ErwGr 78)
 - Verpflichtung der Verantwortlichen zum Nachweis der DSGVO-Compliance, z.B. **Datenschutz-Folgenabschätzung** bei hohem Risiko (Art. 35 DSGVO) und bei **Zertifizierung** (Art. 42 DSGVO): DSGVO-Compliance und Informationen der Hersteller und Dienstleister **müssen eingefordert werden**
- Staatliche Unterstützung durch **Förderung** sinnvoll

Geeignete Basis für technischen Datenschutz?

- „Stand der Technik“ kann obere und untere Grenze sein
- Wer **definiert** „Stand der Technik“ und **schreibt fort**?
- „Technology Readiness Level“ ohne „**Quality**“ sinnlos:
Arbeiten zu „PET Maturity“
- **Lücke** zwischen Forschung und Praxis
- Wünschenswert: **Repositories** mit Konzepten und Implementierungen



<https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pets> (2015)

Regulierung des technischen Datenschutzes

Geeignete Basis für technischen Datenschutz?

- Ziel der Technikneutralität:
Mindesthaltbarkeit der DSGVO: mehrere Jahrzehnte
- Wirklich technikneutral?
 - **Wünschenswert?**
 - Sehr abstrakt: Rechtsunsicherheit für alle Beteiligten
 - Die Gerichte werden's richten
 - **Erreicht?**
Wirkung in Bezug auf technischen Datenschutz:
fördernd / hemmend / neutral?

Regulierung des technischen Datenschutzes

Anmerkungen zur Technikneutralität

- Implizite Annahmen
 - **Vertrauensmodell:** Verantwortlichem mit nachgewiesener Compliance wird vertraut; geringe Anreize für **weitergehende Datenminimierung, Transparenz + Schnittstellen zum Selbstschutz**
 - Konkretisierung im Recht zumeist durch Beschränkung des Datenkatalogs ⇒ **erschwert Lösungen, die Nachweise oder Funktionalität erbringen, ohne personenbezogene Daten zu offenbaren**
- Auswirkungen unklar:
 - Von / auf **Infrastrukturen**
 - Für Datenschutztechnik häufig **mehrere Parteien** nötig; Dienstleister-Einbindung erhöht **Komplexität und Abhängigkeit** und erfordert Kontrolle durch den Verantwortlichen

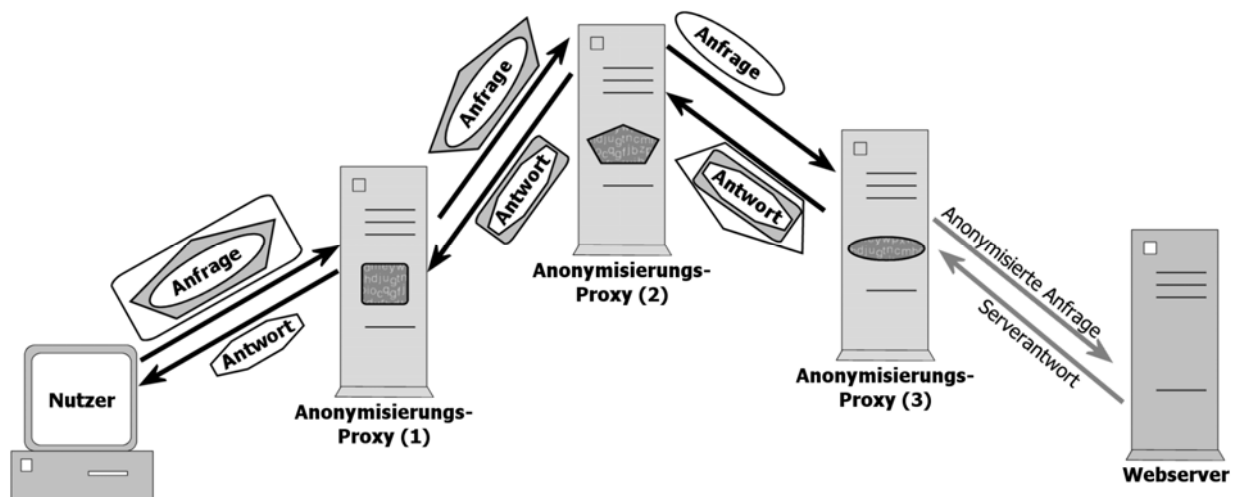
Lösungen sind nicht immer intuitiv

Koordinatoren im Sinne einer „Bauleitung“?

Regulierung des technischen Datenschutzes

Anmerkungen zur Technikneutralität – Bsp.

Selbstschutz für Anonymität und Unbeobachtbarkeit: Mix-System



Anmerkungen zur Technikneutralität – Bsp.

Selbstdatenschutz für Transparenz: „Data Track“

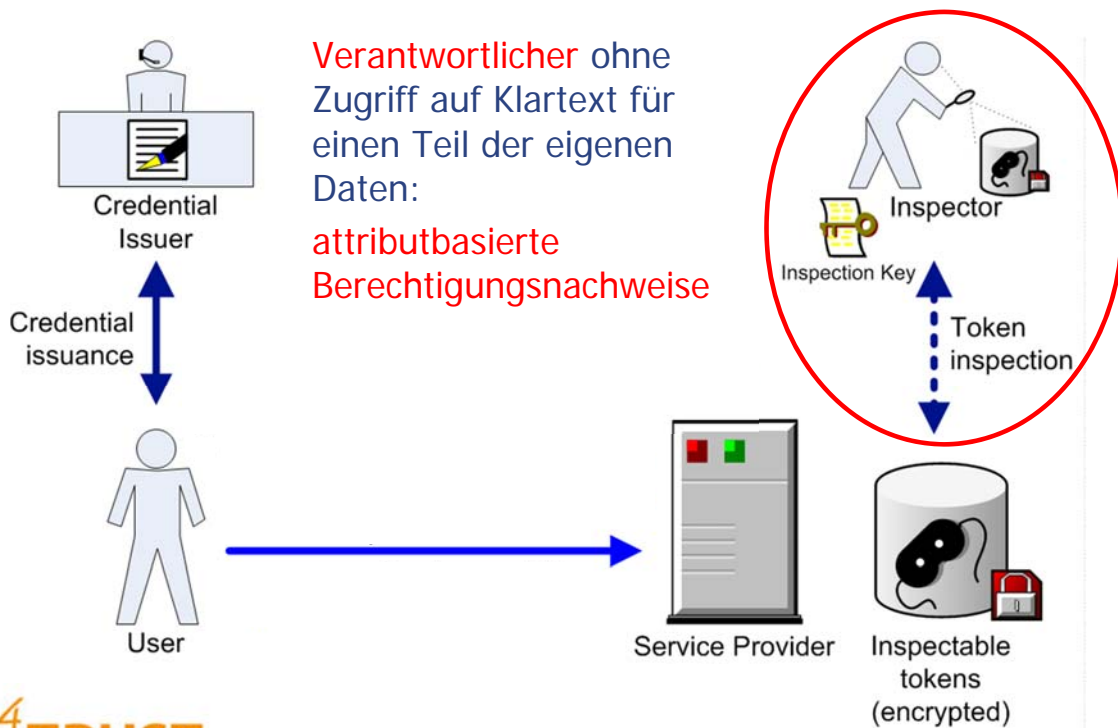


Source: Angulo et al. (2015): Usable Transparency with the Data Track: A Tool for Visualizing Data Disclosures, CHI EA '15, <http://dx.doi.org/10.1145/2702613.2732701>



Regulierung des technischen Datenschutzes

Anmerkungen zur Technikneutralität – Bsp.



Verantwortlicher ohne Zugriff auf Klartext für einen Teil der eigenen Daten:
attributbasierte Berechtigungsnachweise



Regulierung des technischen Datenschutzes

Anmerkungen zur Technikneutralität – Bsp.

Typisches Gesetz: Aufzählung der Daten

Aber oft aggregierte Informationen ausreichend

Konzept

„Nachweise statt Daten“

§ 8 Datenverarbeitung; Betreten der Wohnung

(1) Die Gemeinde ist befugt, folgende Daten der Verfügungsberechtigten, Nutzungsberechtigten und sonstigen Bewohnerinnen und Bewohnern des befangenen Wohnraums zu erheben und zu verarbeiten, soweit dies zur Erfüllung der Aufgaben nach diesem Gesetz erforderlich ist:

1. Personendaten:
Familienname, Vorname, gegenwärtige und letzte frühere Anschrift, Geburtsdatum, Familienstand;
2. Wohnungsdaten:
 Lage, Größe (Fläche), Anzahl der Zimmer, Anzahl der Bewohnerinnen und Bewohner, Bestehen einer öffentlichen Förderung des befangenen Wohnraums;
3. Nutzungsnachweise:
 Mietvertrag und gegebenenfalls frühere Mietverträge zu dem befangenen Wohnraum, Nutzungsart des befangenen Wohnraums, Beginn und Dauer des Mietverhältnisses, Miethöhe, Mietzahlungsbelege;
4. Gewerbedaten:
 Firmenname, Gesellschafterinnen, Gesellschafter, Gewerbeat.

Geeignete Basis für technischen Datenschutz?

- Anforderungen „zwischen den Zeilen“ der DSGVO – „Easter-Eggs“ eingewoben in die DSGVO



- Insbesondere:
 - Einrichtung von **Datenschutz-Management-Systemen** für den gesamten Lebenszyklus
 - Parallel: Informationssicherheit-Management-Systeme (ISMS)
- Erweiterung der Ausrichtung auf „Risiken für Rechte und Freiheiten natürlicher Personen“

Überblick

1. Technischer Datenschutz – Status Quo
2. Bisher in Deutschland
3. Technischer Datenschutz aus Europa
4. **Umsetzung in Deutschland**
5. Fazit

Regulierung des technischen Datenschutzes

Hersteller-Adressierung?

- Bislang im nationalen Recht nicht aufgegriffen
- Möglicherweise in Spezialgesetzen (Fahrzeugzulassung o.ä.)
- Wo ist die **Ermutigung der Hersteller?**
- Berücksichtigung im **Ausschreibungsrecht?**
- **Steuerliche** Auswirkungen möglich?



Regulierung des technischen Datenschutzes

Konkretisierungen „Stand der Technik“

- Bislang im nationalen Recht nicht aufgegriffen
- Möglicherweise Entwicklung zusammen mit dem BSI oder der ENISA
- Arbeiten von TeleTrusT zum Stand der Technik gemäß IT-Sicherheitsgesetz
- Vgl. Katalog von Maßnahmen nach IT-Grundschutz + (künftig) Standard-Datenschutzmodell



Regulierung des technischen Datenschutzes

Technikneutralität?

- Diskussionsbedarf zu **(Neben-)Wirkungen**
- Implizite Annahmen betreffen **Datenverarbeitung generell**, nicht nur technischen Datenschutz
- Forschungsfragen zur **Datenschutz-Governance**



Datenminimierung / Datenschutz-Folgenabschätzung

- **Datenminimierung** / Art. 25-Anforderungen in Spezialgesetzen
 - Z.B. bei der Infrastruktur des Personalausweises
 - Weiteres denkbar, auch untergesetzlich
 - „To do“ für **1.000 Fachgesetze!**
- **Datenschutz-Folgenabschätzung**
 - Durchführung einer DSFA schon im Gesetzgebungsprozess: nach Art. 35 Abs. 10 DSGVO keine konkrete DSFA notwendig, es sei denn, der Gesetzgeber fordert dies
 - Von dieser Öffnungsklausel sollte Gebrauch gemacht werden!

Regulierung des technischen Datenschutzes

Datenschutz-Management / Rechte und Freiheiten natürlicher Personen

- **Datenschutz-Management** nicht erwähnt – weiter zwischen den Zeilen
- „Rechte und Freiheiten **natürlicher Personen**“: erweiterter Blick über die aktuell betroffenen Personen hinaus, d.h. auch gesellschaftliche Aspekte adressierbar (Überwachung, Diskriminierung, ...)
- Formulierungsänderung in BDSG-neu **fehlerhaft reduzierend**: „mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen“
(§ 71 DSAnpUG-EU – Entwurf vom 01.02.2017)



Regulierung des technischen Datenschutzes

„... erhebliche Gefahr für die Rechtsgüter betroffener Personen ...“

§ 67

Durchführung einer Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvor...

(2) Für die ...
hohem Gefahren
genommen werde

(3) Der Verar
tragten an der Du

(4) Die Folge
Personen Rechne

1. eine sys
der Zwecke der V

2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,

3. eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und

4. die Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden soll, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden soll.

(5) Soweit erforderlich hat der Verantwortliche eine Überprüfung durchzuführen, ob die Verarbeitung den Maßgaben folgt, die sich aus der Folgenabschätzung ergeben haben.

Art. 27 JI-RL:

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein **hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge ...

Überblick

1. Technischer Datenschutz – keine Selbstverständlichkeit
2. Technischer Datenschutz aus Europa
3. Technikneutralität?
4. Umsetzung in Deutschland
5. **Fazit**

Fazit



 Bild: Rob Pongsajapan

- Technischer Datenschutz insgesamt **unbefriedigend**:
 - Status Quo
 - europarechtlich
 - nationalgesetzlich
- **Ungenutzte Spielräume**
- **Unverständliche Fehler** wie bei „Rechten und Freiheiten“
- Dringender **Änderungsbedarf** der Gesamt-Umsetzung

Regulierung des technischen Datenschutzes



Vielen Dank für die Aufmerksamkeit!

Marit Hansen

<https://www.datenschutzzentrum.de/>