
# Technischer Datenschutz – Anforderungen aus Europa

Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein

EAID-Veranstaltung „Technologischer Datenschutz – Vorgaben der Datenschutzgrundverordnung“
Berlin, 02.03.2017

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein



## *Überblick*

1. Datenschutz: mehr als Informationssicherheit
2. Technischer Datenschutz bisher in Deutschland
3. Neues aus Europa
4. Wirkung?
5. Fazit

# Vorbemerkung: Wichtigkeit von „by Design“

Erwägungsgrund 4

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





# 1. Datenschutz: mehr als Informationssicherheit

Building Security In
Editor: Gary McGraw, gem@cigital.com

Software Security

Software security is the idea of engineering software so that it continues to function correctly under malicious attack. Most technologists acknowledge this undertaking's importance, but they need some help in understanding how to tackle it. This new department aims to provide that help by exploring software security best practices.

The software security field is a relatively new one. The first books and academic classes on the topic appeared in 2001, demonstrating how recently developers, architects, and computer scientists have started systematically studying how to build secure software. The field's recent appearance is one reason why best practices are neither widely adopted nor obvious.

A central and critical aspect of the computer security problem is a software problem. Software defects with security ramifications—including implementation bugs such as buffer overflows and design flaws such as inconsistent error handling—continue to be with us for years. All too often, malicious intruders can hack into systems by exploiting software defects. Internet-enabled software applications present the most common security risk encountered today, with software's ever-expanding complexity and extensibility adding further fuel to the fire. By any measure, security holes in software are common, and the problem is growing. CERT Coordination Center identified 4,129 reported vulnerabilities in 2003 (a 70 percent increase over 2002, and an almost fourfold increase since 2001).[1,2]

Software security best practices leverage good software engineering practice and involve thinking about security early in the software life cycle, knowing and understanding common threats (including language-based flaws and pitfalls), designing for security, and subjecting all software artifacts to thorough objective risk analyses and testing. Let's look at how software security fits into the overall concept of operational security and examine some best practices for building security in.

...versus application security

Application security means many different things to many different people. In *IEEE Security & Privacy* magazine, it has come to mean the protection of software after it's already built. Although the notion of protecting software is an important one, it's just plain easier to protect something that's a defect-free than something riddled with vulnerabilities.

Pondering the question, "What is the most effective way to protect software?" can help untangle software security and application security. On one hand, software security is about building secure software: designing software to be secure, making sure that software is secure, and educating software developers, architects, and users about how to build secure things. On the other hand, application security is about protecting software and the systems that software runs in a post-facto way, after development is complete. Issues critical to this subfield include sandboxing code (a la Java virtual machine done), protecting against malicious code, obfuscating code, locking down executables, monitoring programs as they run (especially their input), enforcing the software use policy with technology, and dealing with extensible systems.

Application security follows naturally from a network-centric approach to security, by embracing standard approaches such as perimeter and patch[3] and input filtering (trying to block malicious input) and by providing value in a reactive way. Put succinctly, application security is based primarily on finding and fixing known security problems after they've been exploited in fielded systems. Software security—the process of designing, building, and testing software for security—identifies and expunges problems in the software itself. In this way, software security practitioners attempt to build software that can withstand attack proactively. Let me give you a specific example although there's some real value in stopping buffer overflow attacks by observing HTTP traffic as it arrives over port 80, a superior approach is to fix the broken code and avoid the buffer overflow completely.

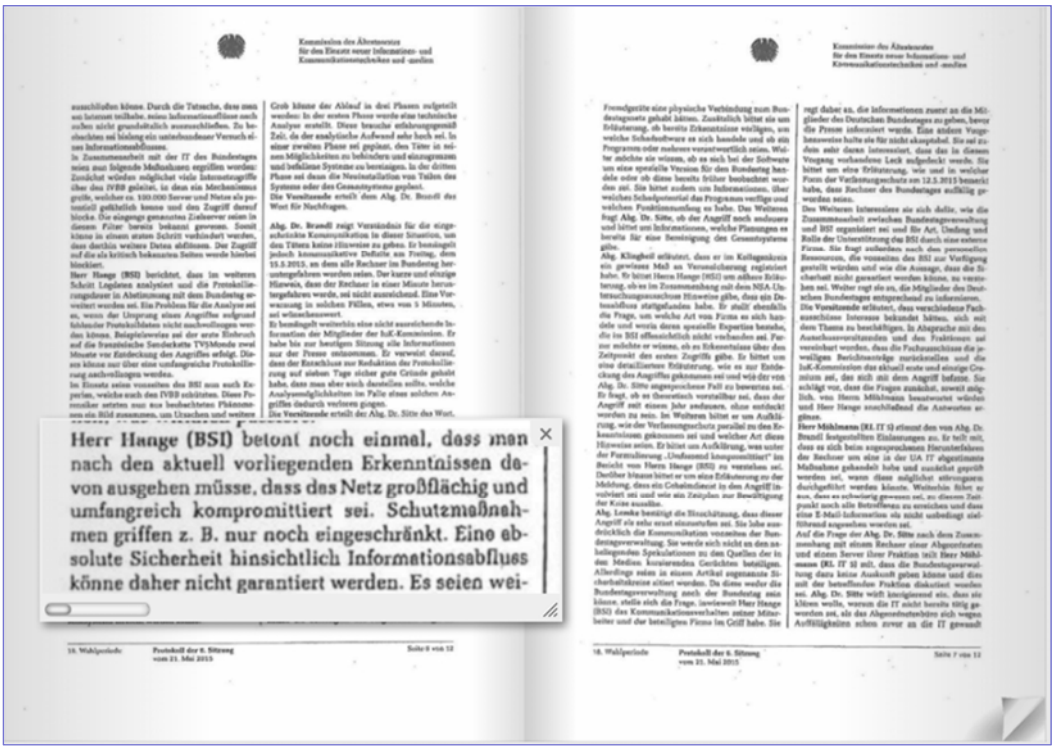
...as practiced by operations people

One reason that application security technologies such as firewalls have evolved the way they have is because


„Building Security In“ – Gary McGraw, 2004

> The software security field is a relatively new one. The first books and academic classes on the topic appeared in 2001, demonstrating how recently developers, architects, and computer scientists have started systematically studying how to build secure software. The field's recent appearance is one reason why best practices are neither widely adopted nor obvious.

# Brüchiges Fundament?



Herr Hange (BSI) betont noch einmal, dass man nach den aktuell vorliegenden Erkenntnissen davon ausgehen müsse, dass das Netz großflächig und umfangreich kompromittiert sei. Schutzmaßnahmen griffen z. B. nur noch eingeschränkt. Eine absolute Sicherheit hinsichtlich Informationsabfluss könne daher nicht garantiert werden. Es seien wei-

Beispiel: „Bundestags-Hack“

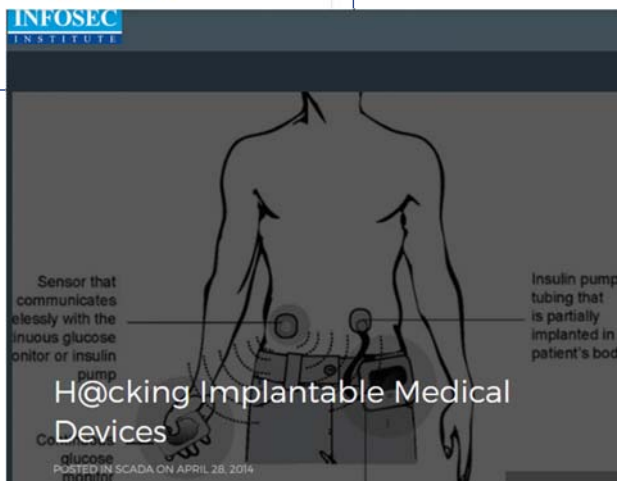
Kommission des Ältestenrates für den Einsatz neuer Informations- und Kommunikationstechniken und –medien, Protokoll vom 21.05.2015





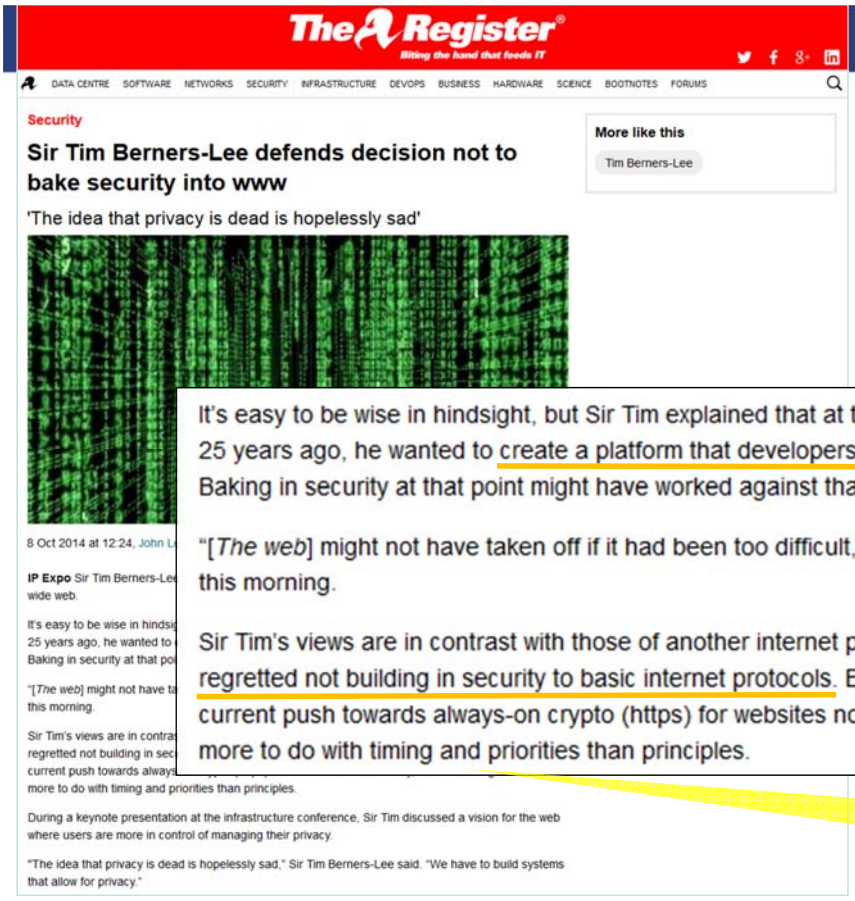
# Sicherheit durch Ausbauen


http://www.theverge.com/2013/10/21/4863872/dick-cheney-pacemaker-wireless-disabled-2007




http://resources.infosecinstitute.com/hcking-implantable-medical-devices/

# WWW mit oder ohne



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 hindsig 25 years ago, he wanted to Baking in security at that po

"[*The web*] might not have ta this morning.

Sir Tim's views are in contras regretted not building in sec current push towards always 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."

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

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





# 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)


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

# Beim Datenschutz geht es um ~~Daten~~

Bild: Ashtyn Renee

## Menschen mit ihren Rechten

Prüffragen bei der Gestaltung:

- Auswirkungen auf Menschen?
- Auswirkungen auf die Gesellschaft?





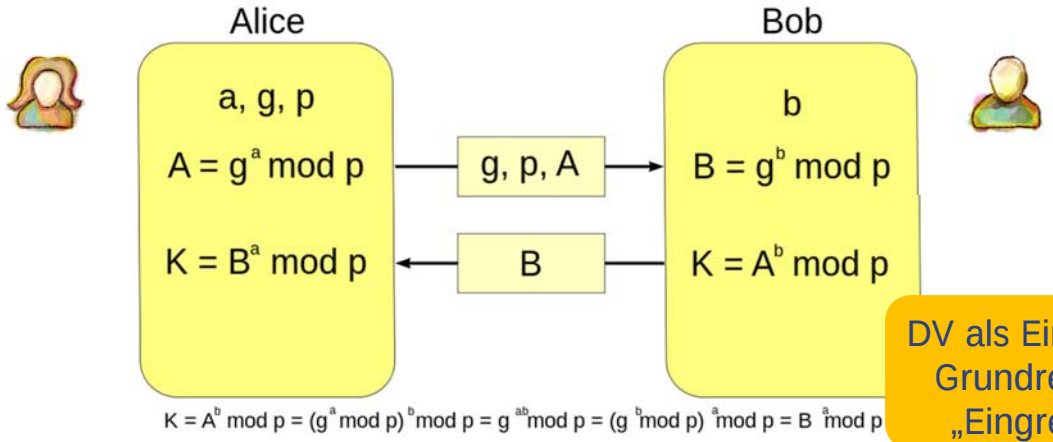
Datenschutz nötig: Machtgefälle

Wichtig: Perspektive der Betroffenen

Ansatzpunkt: personen-bezogene Daten

Bild: Azureon2

# Perspektive: Alice & Bob




DV als Eingriff in Grundrechte: „Eingreifer“

IT-Sicherheit: Der Angreifer ist Eve (oder Mallory).

Datenschutz: Der Angreifer ist Bob!
(Jedenfalls auch.)





# 2. 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.

# 3. Neues aus Europa

- Europäische Datenschutz-Reform
  - Art. 25 Datenschutz-Grundverordnung
  - Art. 20 JI-Richtlinie

- eIDAS-Verordnung
  VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

Art. 12 (3) eIDAS-VO

Der Interoperabilitätsrahmen muss folgende Kriterien erfüllen:

[…]

c) er fördert die Umsetzung des Grundsatzes des „eingebauten Datenschutzes“ (privacy by design)

[…]





# Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

*Artikel 25*

**Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**

(1) Unter Berücksichtigung des Stands 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 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.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

# Datenschutz durch Technikgestaltung

## Artikel 25 Datenschutz durch Technikgestaltung […]

(1) Unter Berücksichtigung
des Stands 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.





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

Identische Formulierung in Art. 32 „Sicherheit der Verarbeitung“

*Artikel 25*

**Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**

(1) Unter Berücksichtigung des Stands 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 Maßn ausgelegt sind, die Datenschutzgrundsätze wie etwa Daten Garantien in die Verarbeitung aufzunehmen, um den Anforde betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und o Voreinstellung grundsätzlich nur personenbezogene Daten, d tungszweck erforderlich ist, verarbeitet werden. Diese Ver bezogenen Daten, den Umfang ihrer Verarbeitung, ihre Sp müssen insbesondere sicherstellen, dass personenbezogene Person einer unbestimmten Zahl von natürlichen Personen zu

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Art Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artik

*Artikel 32*

**Sicherheit der Verarbeitung**

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des U Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und S Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftrag geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schut gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem phys technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der techr organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtu Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

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

*Article 17*

**Security of processing**

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.

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.

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.

Auf EU-Ebene nichts Neues, siehe EU-Datenschutz-Richtlinie 95/46/EG



ULD www.datenschutzzentrum.de

# 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

gemäß Artikel 40
herangezogen wer

„Stand der Technik“ und „Implementierungskosten“ können bei hohen Risiken nicht als „Ausrede“ dienen

(z.B. Art. 36 Vorherige Konsultation)

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

# Datenschutz durch datenschutzfreundliche Voreinstellungen

**Artikel 25 Datenschutz […] durch datenschutzfreundliche Voreinstellungen**

Betont das Erforderlichkeits-prinzip (Artikel 5)

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Bsp.: Social Networks



ULD www.datenschutzzentrum.de

# Datenschutz durch datenschutzfreundliche Voreinstellungen

**Artikel 25 Datenschutz […] durch datenschutzfreundliche Voreinstellungen**

Keine relativierenden Bedingungen!

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

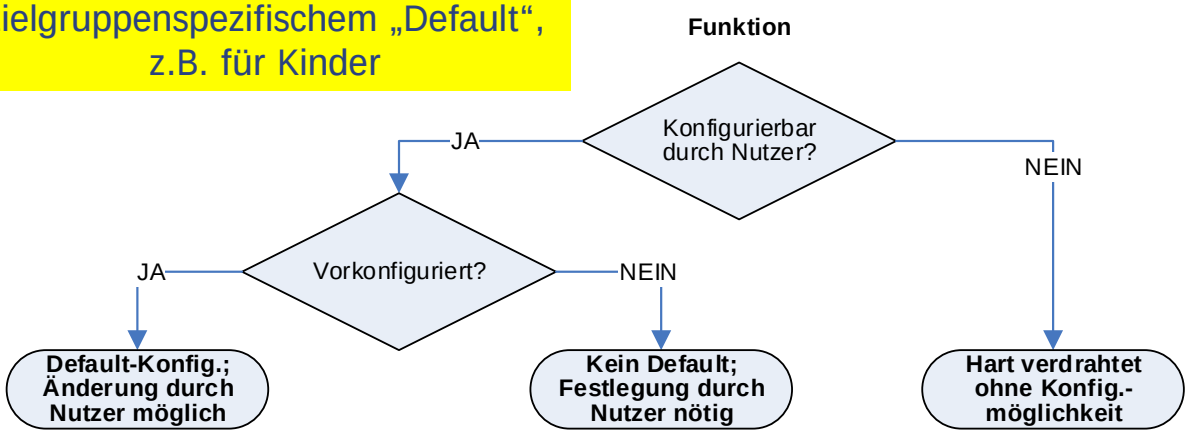
Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Nicht nur minimaler Datenkatalog; auch generelle Risikominimierung

Technischer Datenschutz – Anforderungen aus Europa

# „... by Default“: Drei Fälle der (Vor-)Konfiguration

„One size fits all“ vs. zielgruppenspezifischem „Default“, z.B. für Kinder




**Bsp.: anonyme Nutzung, kein Tracking**

**Bsp.: Auswahl des Bezahl-Systems**

**Bsp.: verschlüsselte Kommunikation**

s.a.: Marit Hansen: Data Protection by Default in Identity-Related Applications. Proc. IDMAN 2013, IFIP AICT 396, S. 4-17.





# Datenschutz „by Design“ & „by Default“ gemäß Erwägungsgrund 78 DSGVO

- Nachweis durch interne Strategien & t+o Maßnahmen, u.a.
  - Datenminimierung
  - Schnellstmögliche Pseudonymisierung
  - Transparenz in Bezug auf Funktionen+Verarbeitung
  - Ermöglichung der Überwachung der Verarbeitung durch die betroffenen Personen
  - Ermöglichung für Sicherheitsfunktionen „on top“ durch Verantwortlichen
- Ermutigung für Hersteller
- Berücksichtigung in öffentlichen Ausschreibungen

(78) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.

## Anmerkung: „by Design“ = „durch Technikgestaltung“?

- [FR] Article 25: Protection des données dès la conception et protection des données par défaut
- [ES] Artículo 25: Protección de datos desde el diseño y por defecto
- [DE] Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- [SV] Artikel 25: Inbyggt dataskydd och dataskydd som standard
- [NL] Artikel 25: Gegevensbescherming door ontwerp en door standaardinstellingen

„Technik“ nur in der deutschen Fassung; d.h. breiter zu verstehen





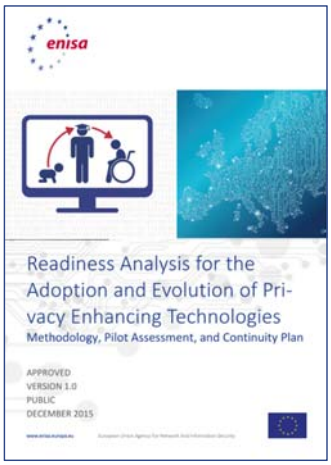
## 4. Wirkung? Hersteller mit ins Boot nehmen

- Hersteller sind nicht unmittelbarer Adressat
- Indirekte Effekte möglich:
  - „Ermutigung“ (ErwGr 78)
  - Öffentliche Ausschreibung
  - Art. 42+43 DSGVO: freiwillige Zertifizierung
  - Verpflichtung der Verantwortlichen zum Nachweis der DSGVO-Compliance und Datenschutz-Folgenabschätzung bei hohem Risiko (Art. 35 DSGVO):
    DSGVO-Compliance und Informationen der Hersteller und Dienstleister müssen eingefordert werden
- Staatliche Unterstützung durch Förderung sinnvoll

# Wirkung? „Stand der Technik“

- „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)








# Wirkung? Versuch der Technikneutralität

- Technikneutralität Ziel der DSGVO
- Aber: implizite Annahmen
  - Vertrauensmodell: Verantwortlichem mit nachgewiesener Compliance wird vertraut; geringe Anreize für weitergehende Datenminimierung
  - Konkretisierung im Recht zumeist durch Beschränkung des Datenkatalogs ⇒ erschwert Lösungen, die Nachweise oder Funktionalität erbringen, ohne personenbezogene Daten zu offenbaren
- Kenntnis des Lösungsraums voraussetzungsvoll:
  - Lösungen sind nicht immer intuitiv
  - Hohe Anforderungen an Aufsichtsbehörden

# Wirkung? Implementierungskosten

- Betrifft nicht nur Anschaffungskosten
- Auswirkungen von / auf Infrastrukturen
- Datenschutztechnik erfordert häufig mehrere Parteien; Dienstleister-Einbindung erhöht Komplexität und Abhängigkeit und erfordert Kontrolle durch den Verantwortlichen
  ⇒ Geschäftsmodelle für Koordinatoren à la „Bauleitung“?
- Wünschenswert:
  - Good+Best-Practice-Lösungen
  - Dokumentenpakete für konkreten Einsatz und Nachweis der DSGVO-Compliance (mind. bei Zertifizierung!)
  - Technikunterstützung zur korrekten Konfiguration





# Risikobewertung

Besonders schwierig!

- Risk = Impact x Probability

  Übliche Risiko-Formel liefert nur scheinbar objektive Messbarkeit.

$$R = \sum_{k=1}^{n} I_k \times p(I_k)$$

- „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)

# Zusammenfassung: Datenschutz „by …“

| Daten-schutz | Was? | Wirklich neu? | Wird es klappen? | Bemerkungen |
|---|---|---|---|---|
| … by Design | Techn.+org. Maßnahmen für alle Anforderungen aus DS-GVO: optimal „eingebauter Datenschutz“ | Nein (§ 3a BDSG), aber bislang kaum durchgesetzt | + mächtiges Werkzeug<br>– erfordert viel Know-how beim Verantwortlichen und der Aufsichtsbehörde<br>– „Feigenblatt“-Methode möglich: Mini-Schritte und Dokumentation | Hersteller sind nicht Adressat.<br><br>Wer kümmert sich um Infrastrukturen?<br><br>Ausschreibungen! |
| … by Default | | | | |



ULD www.datenschutzzentrum.de

# Zusammenfassung: Datenschutz „by …“

| Daten-schutz | Was? | Wirklich neu? | Wird es klappen? | Bemerkungen |
|---|---|---|---|---|
| … by Design | Techn.+org. Maßnahmen für alle Anforderungen aus DS-GVO: optimal „eingebauter Datenschutz“ | Nein (§ 3a BDSG), aber bislang kaum durchgesetzt | + mächtiges Werkzeug<br>– erfordert viel Know-how beim Verantwortlichen und der Aufsichtsbehörde<br>– „Feigenblatt“-Methode möglich: Mini-Schritte und Dokumentation | Hersteller sind nicht Adressat.<br><br>Wer kümmert sich um Infrastrukturen?<br><br>Ausschreibungen! |
| … by Default | Primär als umgesetztes Erforderlichkeits-prinzip verstanden | Teilweise; Durchsetzung war bislang schwierig | + mächtiges Werkzeug<br>– Effekt kann geschwächt werden durch datenreiche Angebote auf Einwilligungsbasis | Konzept in Art. 25(2) DSGVO ermöglicht weite Auslegung |

# 5. Fazit

Bild: Rob Pongsajapan

- Nicht nur Technikgestaltung
- Vieles nicht neu,
  aber mittlerweile bessere
  Chancen auf Realisierung
  - Privacy by Disaster (leider!)
  - Datenschutz-Grundverordnung
    (mit Professionalisierung+Sanktionen!)
- Wichtig:
  Lösungsraum kennen
  und erweitern




# Vielen Dank für die Aufmerksamkeit!

Marit Hansen
https://www.datenschutzzentrum.de/

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

ipen