



Privacy by Design – die (neuen) rechtlichen Anforderungen

Harald Zwingelberg

mit Inhalten von Marit Hansen, Wolfram Felber
Unabhängiges Landeszentrum für Datenschutz (ULD)

GI Workshop „Wie sicher ist der neue Datenschutz“
GI Fachgruppen SECMGT & PET
Frankfurt 10. März 2017



SPECIAL



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein



Überblick

- 1. Datenschutz: mehr als Informationssicherheit**
2. Technischer Datenschutz bisher in Deutschland
3. Neues aus Europa (DSGVO, ePrivacyVO)
4. Um- und Durchsetzung
5. Fazit

Autoren:

Marit Hansen, ULD	Forum Privatheit
W. Felber, ULD	AppPETs, AN.ON-Next
H. Zwingelberg, ULD	SPECIAL, Privacy&Us



Vorbemerkung 1: Wichtigkeit von „by Design“

Erwägungsgrund 4 zur DSGVO

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

Die Deutsche Übersetzung ist hier ungenau:

„Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen. [...]“



Vorbemerkung 2: „by Design“ ≠ „durch Technikgestaltung“!

- [DE] Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- [EN] Article 25: Data protection by design and by default
- [DK] Artikel 25: Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger
- [SV] Artikel 25: Inbyggd dataskydd och dataskydd som standard
- [NL] Artikel 25: Gegevensbescherming door ontwerp en door standaardinstellingen

„Technik“ nur in der deutschen Fassung;

- [ES] Artículo 25: P d.h. weiter zu verstehen: Konzeption, Organisation

Transparenz, Intervenierbarkeit...



1. Datenschutz: mehr als Informationssicherheit

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

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 (as the Java virtual machine does), 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 penetration and patch⁴ 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 is 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.

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

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.

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

Gary McGraw
Cigital

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—promise to be with us for years. All too often, malicious intruders can hack into systems by exploiting software defects.¹ 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).^{2,3} 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 analysis 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 is 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

80

PUBLISHED BY THE IEEE COMPUTER SOCIETY ■ 1540-7993/04/\$20.00 © 2004 IEEE ■ IEEE SECURITY & PRIVACY

„Building Security In“
— Gary McGraw,
2004



Brüchiges Fundament?

Beispiel: „Bundestags- Hack“

ausschließen könne. Durch die Tatsache, dass man so Internet nutze, seien Informationsflüsse nach außen nicht grundsätzlich auszuschließen. Zu beobachten sei bislang ein unternehmender Versuch eines Informationsabflusses.

In Zusammenarbeit mit der IT des Bundestages seien nun folgende Maßnahmen ergriffen worden: Zunächst würden möglichst viele Internetzugriffe über das TVBB geleitet, in dem ein Mechanismus gelte, welcher ca. 150.000 Server und Netze als potentiell gefährlich kenne und den Zugriff darauf blockiere. Die einzigen genehmigten Zielserver seien in diesem Filter bereits bekannt gewesen. Somit könne in einem ersten Schritt verhindert werden, dass darüber weitere Daten abfließen. Der Zugriff auf die als kritisch bekannten Seiten werde hierbei blockiert.

Herr Hange (BSI) berichtet, dass im weiteren Schritt Logdaten analysiert und die Protokollierungsdauer in Abstimmung mit dem Bundestag erweitert werden sei. Ein Problem für die Analyse sei es, wenn der Ursprung eines Angriffes aufgrund fehlender Protokolldaten nicht nachvollzogen werden könne. Beispielsweise sei der erste Einbruch auf die französische Sendekette TV5Mundo zwei Monate vor Entdeckung des Angriffes erfolgt. Dies könne nur über eine umfangreiche Protokollierung nachvollzogen werden.

Im Einsatz seien vornehmlich das BSI sowie auch Experten, welche auch den TVBB schützten. Diese Formulierungen seien aus beschriebenen Phänomenen ein Bild zusammen, um Ursachen und weitere

Grob könne der Ablauf in drei Phasen aufgeteilt werden: In der ersten Phase werde eine technische Analyse erstellt. Diese bestehe erfahrungsgemäß Zeit, da der analytische Aufwand sehr hoch sei. In einer zweiten Phase sei geplant, den Täter in seinen Möglichkeiten zu behindern und einzugrenzen und defekte Systeme zu beseitigen. In der dritten Phase sei dann die Neuinstallation von Teilen des Systems oder des Gesamtsystems geplant. Die Vorsitzende erteilt dem Abg. Dr. Brandt das Wort für Nachfragen.

Abg. Dr. Brandt zeigt Verständnis für die eingeschränkte Kommunikation in dieser Situation, um den Tägern keine Hinweise zu geben. Er bemängelt jedoch kommunikative Defizite am Freitag, dem 15.5.2015, an dem alle Rechner im Bundestag heruntergefahren werden seien. Der kurze und einzige Hinweis, dass der Rechner in einer Minute heruntergefahren werde, sei nicht ausreichend. Eine Verwarnung in solchen Fällen, etwa von 5 Minuten, sei wünschenswert.

Er bemängelt weiterhin eine nicht ausreichende Information der Mitglieder der IuK-Kommission. Er habe bis zur heutigen Sitzung alle Informationen zur der Presse mitgenommen. Er verwies darauf, dass der Entschluss zur Reduktion der Protokollierung auf sieben Tage sicher gute Gründe gehabt habe, dass man sich aber darüber wisse, welche Analysemöglichkeiten im Falle eines solchen Angriffes dadurch verloren gingen. Die Vorsitzende erteilt dem Abg. Dr. Sittig das Wort.

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 Informationsabflusses könne daher nicht garantiert werden. Es seien wei-

Kommission des Ältestenrates
für den Einsatz neuer Informations- und
Kommunikationstechniken und -medien

Fremdgeräte eine physische Verbindung zum Bundestag gehabt hätten. Zusätzlich bittet sie um Erläuterung, ob bereits Erkenntnisse vorlägen, um welche Schadsoftware es sich handle und ob ein Programm oder mehrere verantwortlich seien. Weiter möchte sie wissen, ab wann bei der Software um eine spezielle Version für den Bundestag handle oder ob diese bereits früher beobachtet worden sei. Sie bittet zudem um Informationen, über welchen Schutzniveau das Programm verfüge und welchen Funktionsumfang es habe. Die Weiteren fragt Abg. Dr. Sittig, ob der Angriff noch andauere und bittet um Informationen, welche Pläneungen es bereits für eine Beseitigung des Gesamtsystems gäbe.

Abg. Klingbeil erläutert, dass er im Kollegenkreis ein gewisses Maß an Verunsicherung registriert habe. Er bittet Herrn Hange (BSI) um weitere Erläuterung, ob es im Zusammenhang mit dem NSA-Untersuchungsausschuss Hinweise gäbe, dass ein Datenabfluss stattgefunden habe. Er stellt ebenfalls die Frage, um welche Art von Firma es sich handle und worin deren spezielle Expertise bestünde, die im BSI offensichtlich nicht vorhanden sei. Ferner möchte er wissen, ob es Erkenntnisse über den Zeitpunkt des ersten Zugriffs gäbe. Er bittet um eine detaillierte Erläuterung, wie es zur Entdeckung des Angriffes gekommen sei und wie der von Abg. Dr. Sittig angesprochene Fall zu bewerten sei. Er fragt, ob es derzeit vorstellbar sei, dass der Angriff seit einem Jahr andauere, ohne entdeckt worden zu sein. Im Weiteren bittet er um Aufklärung, wie der Verfassungsschutz parallel zu den Erkenntnissen gekommen sei und welcher Art diese Hinweise seien. Er bittet um Aufklärung, was unter der Formulierung „Unfassend kompromittiert“ im Bericht von Herrn Hange (BSI) zu verstehen sei. Darüber hinaus bittet er um eine Erläuterung zu der Meldung, dass ein Geheimdienst in den Angriff involviert sei und wie ein Zeitspiel zur Bewältigung der Krise aussähe.

Abg. Lemke bemängelt die Einschätzung, dass dieser Angriff als sehr ernst einzustufen sei. Sie lobt ausdrücklich die Kommunikation vornehmlich der Bundestagsverwaltung. Sie werde sich nicht an den anhaltenden Spekulationen zu den Quellen der in den Medien kursierenden Gerüchten beteiligen. Allerdings seien in einem Artikel sogenannte Sicherheitskreise zitiert worden. In dem wieder die Bundestagsverwaltung nach der Bundestag sein könne, stelle sich die Frage, inwieweit Herr Hange (BSI) das Kommunikationsverhalten seiner Mitarbeiter und der beteiligten Firmen im Griff habe. Sie

regt dabei an, die Informationen zuerst an die Mitglieder des Deutschen Bundestages zu geben, bevor die Presse informiert werde. Eine andere Vorgehensweise halte sie für nicht akzeptabel. Sie sei zudem sehr daran interessiert, dass das in diesem Vorgang vorhandene Lück aufgedeckt werde. Sie bittet um eine Erläuterung, wie und in welcher Form der Verfassungsschutz am 12.5.2015 bemerkt habe, dass Rechner des Bundestages unfähig geworden seien.

Die Weiteren interessiert sie sich dafür, wie die Zusammenarbeit zwischen Bundestagsverwaltung und BSI organisiert sei und für Art, Umfang und Rolle der Unterstützung des BSI durch eine externe Firma. Sie fragt außerdem nach den personellen Ressourcen, die vornehmlich des BSI zur Verfügung gestellt würden und wie die Aussage, dass die Sicherheit nicht gefährdet werden könne, zu verstehen sei. Weiter regt sie an, die Mitglieder des Deutschen Bundestages entsprechend zu informieren. Die Vorsitzende erwidert, dass verschiedenen Fachauschüssen Interesse bekannt hätten, sich mit dem Thema zu beschäftigen. In Absprache mit den Ausschussvorsitzenden und den Fraktionen sei vereinbart worden, dass die Fachauschüsse die jeweiligen Berichtsanträge zurückstellen und die IuK-Kommission das aktuell erste und einzige Gremium sei, das sich mit dem Angriff befasse. Sie schlägt vor, dass die Fragen zunächst, soweit möglich, von Herrn Mühlmann beantwortet würden und Herr Hange anschließend die Antworten ergänze.

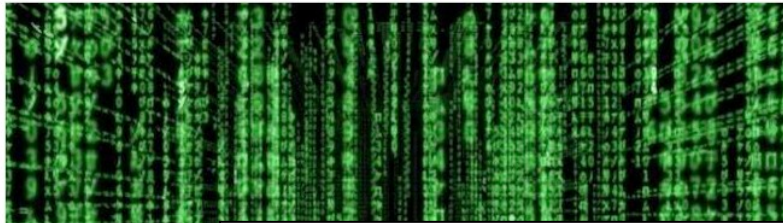
Herr Mühlmann (CDU IT 5) stimmt dem von Abg. Dr. Brandt festgestellten Einlassungen zu. Er teilt mit, dass es sich beim angesprochenen Herunterfahren der Rechner um eine in der UA IT abgestimmte Maßnahme gehandelt habe und zunächst geprüft werden sei, wann diese möglichst störungsarm durchgeführt werden könnte. Weiterhin führt er aus, dass es schwierig gewesen sei, zu diesem Zeitpunkt noch alle Betroffenen zu erreichen und dass eine E-Mail-Information als nicht unbedingt störfördernd angesehen werden sei.

Auf die Frage der Abg. Dr. Sittig nach dem Zusammenhang mit einem Rechner einer Abgeordneten und einem Server ihrer Fraktion teilt Herr Mühlmann (CDU IT 5) mit, dass die Bundestagsverwaltung dazu keine Auskunft geben könne und dies mit der betreffenden Fraktion diskutiert werden sei. Abg. Dr. Sittig wirft konigierend ein, dass sie klären wolle, warum die IT nicht bereits tätig geworden sei, als der Abgeordnete über sich wegen Auffälligkeiten schon zuvor an die IT gewandt

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

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.

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

WWW mit oder ohne

„timing and priorities“
– Sicherheit kann
nachrangig sein
Erfahrung: Sicherheit
und Datenschutz
werden nachrangig
behandelt

Sicherheit durch Ausbauen

THE VERGE

US & WORLD

TRENDING NOW

This is VAIO's Windows phone



39
NEW ARTICLES

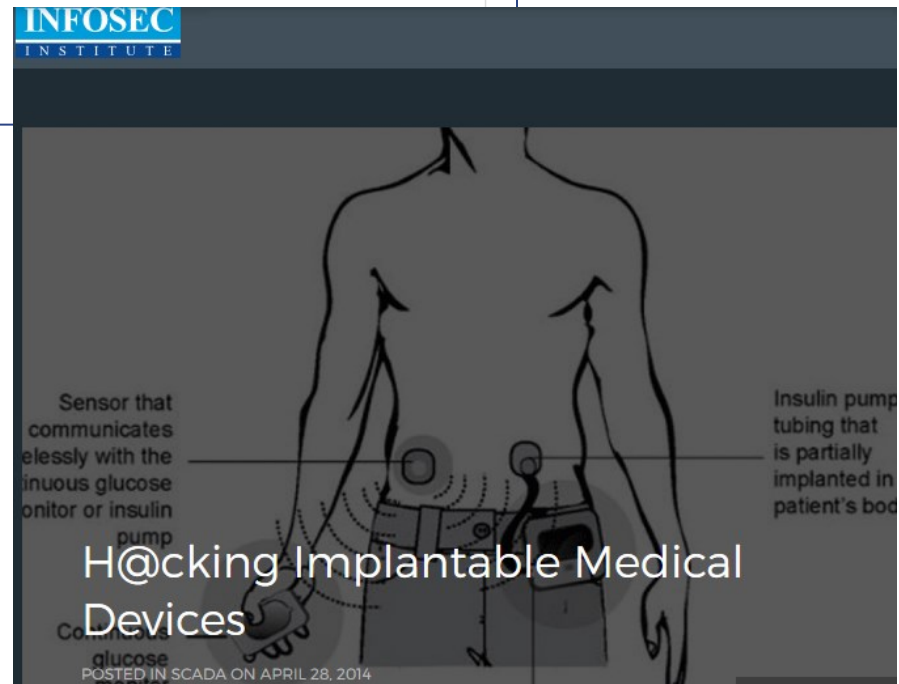
63
COMMENTS

Dick Cheney had the wireless disabled on his pacemaker to avoid risk of terrorist tampering

By Carl Franzen on October 21, 2013 06:54 pm [Email](#) [@carlfranz](#)

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

(Total-)Verzicht ist Option
darf aber nicht einzige Lösung
sein, insbes. Wenn DV
wichtig für betr. Person für
Gesundheit, Teilhabe etc.



<http://resources.infosecinstitute.com/hacking-implantable-medical-devices/>

Beim Datenschutz geht es um ~~Daten~~



Menschen mit ihren Rechten

Prüffragen bei der
Gestaltung von Technik:

- Auswirkungen auf Menschen?
- Auswirkungen auf die Gesellschaft?



Datenschutz
Nötig wegen
Machtgefälle

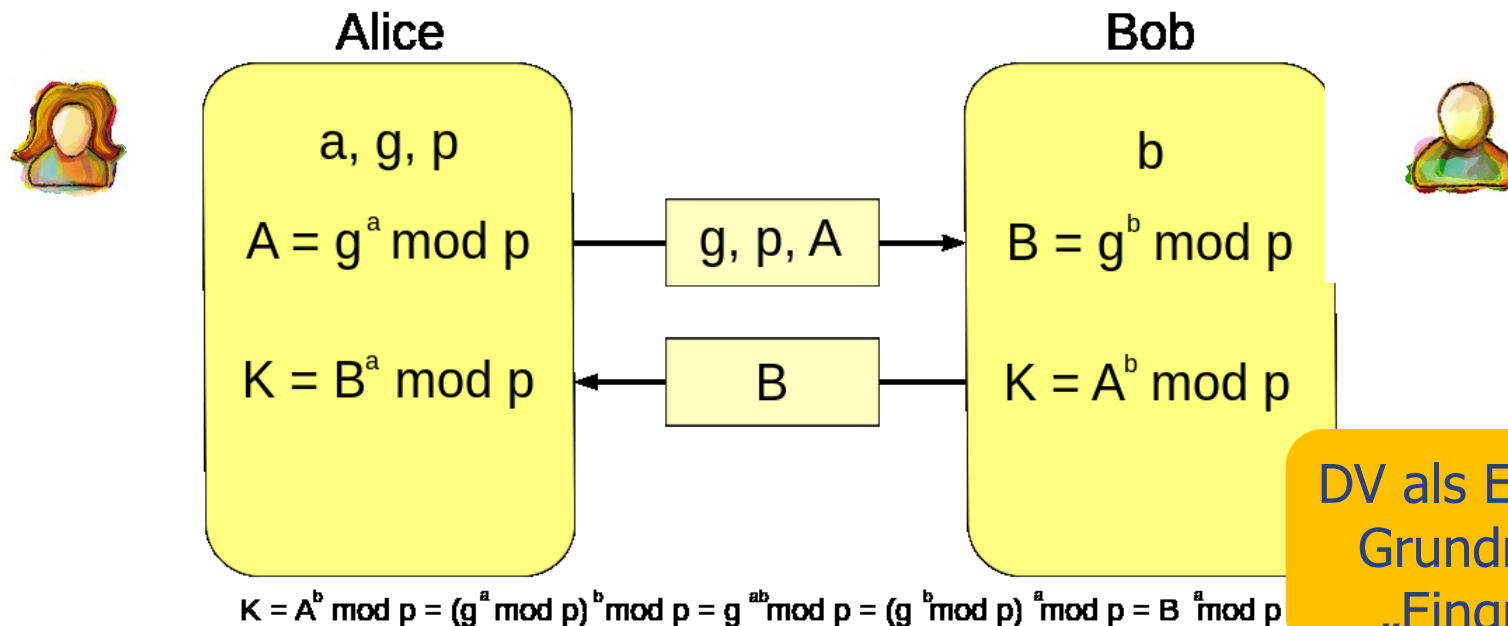
Die
Perspektive
der
Betroffenen

Ansatzpunkt:
personen-
bezogene
Daten



Bild: Azureon2

Perspektive: Alice & Bob



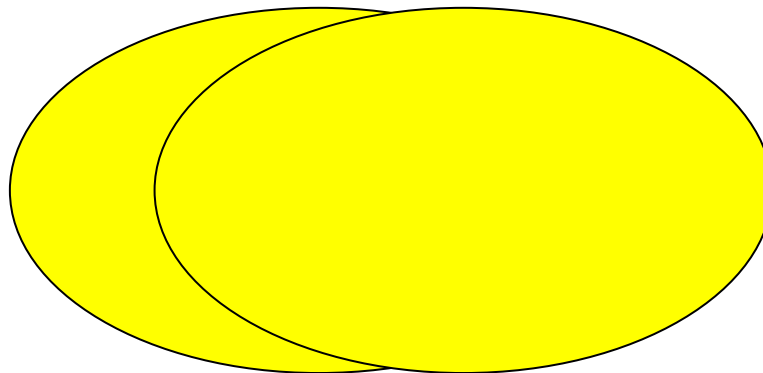
DV als Eingriff in
Grundrechte:
„Eingreifer“

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

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

Zwischenergebnis

- Datenschutz $\neq$ Informationssicherheit
- Privacy by Design $\neq$ Security by Design
- Sie dienen ganz unterschiedlichen Schutzgegenständen – wenn auch mit überwiegend identischen Maßnahmen.
- Informationssicherheit und Datenschutz ergänzen einander.





Überblick

1. Datenschutz: mehr als Informationssicherheit
- 2. Technischer Datenschutz bisher in Deutschland**
3. Neues aus Europa (DSGVO, ePrivacyVO)
4. Um- und Durchsetzung
5. Fazit



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.

Datenminimierung ist nur
Programmsatz. Konkreter aber
§ 3 VI TMG zur
Anonymisierung und
Pseudonymisierung^[1]

Und wenn nicht?
Keine Sanktion für Verstöße
gegen § 3a BDSG
oder § 13 VI TMG

[1] Borges/Schwenk, Cloud Computing S. 38.



Technischer Datenschutz bisher in Deutschland

§ 9 BDSG Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die **technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind**, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. **Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.**

Anlage zu § 9 BDSG:

Maßnahmenzentriert: Wesentliche Aspekte durch den Katalog abgedeckt. Aber Maßnahmen entwickeln und ändern sich, daher zielorientierter Katalog geeigneter. (Standarddatenschutzmodell)



Überblick

1. Datenschutz: mehr als Informationssicherheit
2. Technischer Datenschutz bisher in Deutschland
- 3. Neues aus Europa (DSGVO, ePrivacyVO)**
4. Um- und Durchsetzung
5. Fazit



Neues aus Europa Überblick

- Europäische Datenschutz-Reform
 - Art. 5 Datenschutz-Grundverordnung (DSGVO)
 - **Art. 25 DSGVO**
 - Art. 32 DSGVO
 - Art. 20 JI-Richtlinie

- Entwurf der E-Privacy-VO

- 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**)

[...]

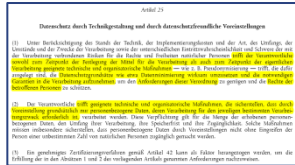


Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

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 (1) 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!

Unklar, wie sich
Zweck auswirken
soll: Genügt
unsichere DV für
„gute“ Zwecke?
M.E. zurückhaltend
zu handhaben

[...] **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 **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 als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42, das die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels sicherstellt, kann als Nachweis für die Einhaltung der in den Absätzen 1 und 2 des vorliegenden Artikels angesehen werden.

Artikel 32

Sicherheit der Verarbeitung

(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 des Risikos 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:

- 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 oder technischen 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.

(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.



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.

Der Fairness halber mitgeteilt: Auf EU-Ebene ist eine Beschränkung mit Blick auf die Implementierungskosten nicht neu, siehe Art. 17 der Datenschutz-Richtlinie (95/46/EG)



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

Keine Beschränkung der **Verantwortung** in Art. 24 DSGVO:

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 Verarbeitungszwecken steht, kann der Verantwortliche gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen

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

gemäß A
nerangezo

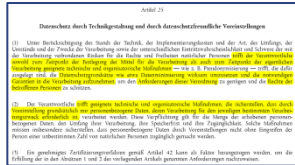
„Stand der Technik“ und
„Implementierungskosten“
können bei hohen Risiken
nicht als „Ausrede“ dienen.

**Verantwortlicher ist
verantwortlich unabhängig
von den Kosten.**

ETs und d



Datenschutz durch datenschutzfreundliche Voreinstellungen



Artikel 25 Datenschutz [...] durch datenschutzfreundliche Voreinstellungen

Betont das Erforderlichkeitsprinzip (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.

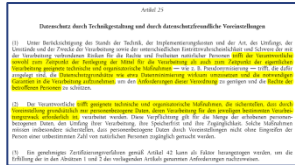
Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. s

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



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.

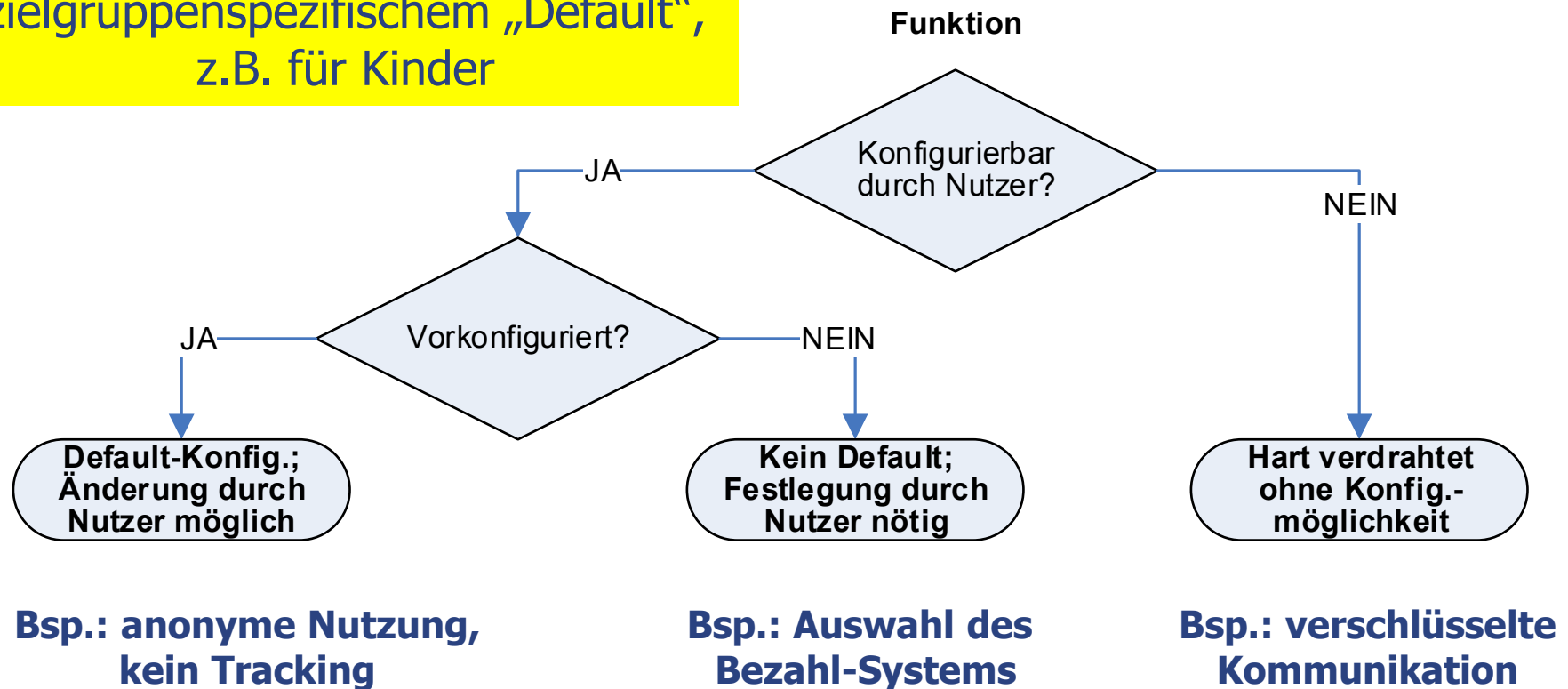
Diese Verpflichtung gilt für die **Menge** der erhobenen personenbezogenen Daten, den **Umfang ihrer Verarbeitung**, ihre **Speicherfrist** und ihre **Zugänglichkeit**.

Solche Maßnahmen müssen insbesondere sicherstellen, dass nur personenbezogene Daten durch Voreinstellung der Person einer unbestimmten Personengruppe zugänglich gemacht werden.

Nicht nur minimaler Datenkatalog; auch generelle Risikominimierung. Menge und Frist sind explizit genannt, so dass Umfang eine eigenständige Bedeutung zukommt.

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

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





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, **Transparent** 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.



Überblick

1. Datenschutz: mehr als Informationssicherheit
2. Technischer Datenschutz bisher in Deutschland
3. Neues aus Europa (DSGVO, ePrivacyVO)
- 4. Um- und Durchsetzung**
5. Fazit

Durchsetzung durch Aufsichtsbehörden

- Art. 25 unterfällt allgemeiner Verantwortung zur Überwachung der DSGVO durch die Aufsichtsbehörden, Art. 57 (1) (a) DSGVO [Paal/Pauly/Martini Art 25 Rn. 5]
- Aufsichtsbehörden haben Befugnisse nach Art. 58 (2) DSGVO zu
 - „warnen“ => voraussichtliche Verstöße bei DV
 - „verwarnen“ => Verstöße bei DV
 - „anweisen“ => mit Ziel die DV in Einklang mit der VO zu bringen
- Bußgeldbewährt bei Nichtbefolgung einer Anweisung und in Sonderfällen ohne Vorwarnung Art. 83 (5) und (6)



Unterstützung durch Datenschutzbeauftragte?

- Beschränkte Ansatzpunkte zur Förderung von PETs vorhanden in Art. 39 DSGVO:
 - Als Teil der Überwachung der Einhaltung der VO
 - Beratung bei der Gestaltung der Datenverarbeitung
 - Als Gegenstand der zu erwägenden Abhilfemaßnahmen bei einer Datenschutzfolgenabschätzung

Denkbare Herangehensweisen

- ⇒ Hinwirken bei Ausschreibungen, insbes. öffentl. Stellen
- ⇒ Hinwirken bei Auswahl von Maßnahmen
- ⇒ Hinweis, dass Verantwortung unabhängig ist von Implementierungskosten

Was fehlt?

- Fehlende normative Vorteile für PET-Einsatz:
Leider gibt es keine Norm in der DSGVO, die deutlich ein „Mehr“ an Verarbeitung oder ein Weniger an Haftung zusagt, wenn PETs sinnvoll und effektiv eingesetzt werden.

Keine klare Zusage des Normgebers für besonders gelagerte Fällen in denen z.B. ein opt-out in Betracht kommen könnte, wo es andernfalls einer informierten Einwilligung bedürfte.

- Ist Herleitung möglich durch Verweis auf eine Gesamtwürdigung bei geringem Risiko, verbesserten Schutz, erhöhte Transparenz und Einflussmöglichkeiten der Betroffenen?
=> Bisher keine hinreichend rechtssichere Antwort absehbar
=> Forschungsfrage für PET-Begleitforschung



Beispiel

Widerruf per automatisiertem Verfahren

- Art. 21 (5) DSGVO ist Ausfluss des PbD-Prinzips ^[1]

Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels **automatisierter Verfahren** ausüben, bei denen **technische Spezifikationen** verwendet werden.

- Widerspruch soll unkompliziert sein. Denkbar automatisierte Verfahren auf Basis lokal gesetzter Voreinstellungen.^[2]

[1] Paal/Pauly/Martini Art. 25 DSGVO Rn. 32.

[2] Paal/Pauly/Martini Art. 21 DSGVO Rn. 72.



Beispiel Widerruf per automatisiertem Verfahren

- Umsetzung eines automatisierten Widerspruchs bedarf geeigneter Spezifikationen für die Kommunikation und eine geeignete Semantik zur Definition der Voreinstellungen „Privacy Preferences“.
- Hier sollte auf bestehende Ergebnisse aus der Datenschutz-Forschung aufgebaut werden (P3P, PrimeLife Policy Language)
- Das Projekt „Scalable Policy-aware linked data arChitecture for prIvacy, trAnsparency and compliance“ (SPECIAL) nimmt sich Teilen dieser Aufgabe im Themenkreis Big Data an.
Partner u.a. W3C, WU Wien, ULD und Unternehmen.
- <https://www.specialprivacy.eu/>



Ausblick e-PrivacyVO

- Entwurfsfassung im Februar 2017 veröffentlicht
<http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52017PC0010>
- Trend weg von Privacy by Design und Default.
Verschiebung von Pflichten und Risiken zu den betroffenen Personen. „Pflicht“ zum Selbstdatenschutz, d.h. Betroffene müssen selbst aktiv werden.
- Keine sinnvolle Begründung für Abweichung von Grundsätzen der DSGVO erkennbar z.B. aus der Eigenart der elektronischen Kommunikation. Im Gegenteil sind Kommunikationsdaten in Masse besonders schutzbedürftig.

Art. 10 ePrivacyVO

Art. 10 – Bereitzustellende Information und Einstellungsmöglichkeiten zur Privatsphäre

massive Abschwächung zum inoffiziellen Vorentwurf

E1 (Dezember 2016)	E2 (Januar 2017)
Article 10 Privacy by design 1. The settings of all the components of the terminal equipment placed on the market shall be configured to, by default, prevent third parties from storing Information, processing information already stored in the terminal equipment and preventing the use by third parties of the equipment's processing capabilities. 2. Software placed on the market permitting electronic Communications, including the retrieval and presentation of information on the Internet, shall be configured to by default prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment. Quelle zum Leak des Entwurfs vom Dez 2016: http://www.politico.eu/wp-content/uploads/2016/12/POLITICO-e-privacy-directive-review-draft-december.pdf	Article 10 - Information and options for privacy settings to be provided 1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment. 2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting. 3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.



Art. 10 ePrivacyVO

Art. 10 – Bereitzustellende Information und Einstellungsmöglichkeiten zur

Adressat klar:
Hersteller von
terminal equipment

Adressat? Inverkehrbringen von
welcher Software: OS? Browser?
Apps? Einstellungen pro App oder
global möglich?

1. The settings of all the components of the terminal equipment placed on the market **shall be configured to, by default, prevent** third parties from storing information, processing information already stored in the terminal equipment and preventing the use by third parties of the equipment's processing capabilities.

2. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, **shall offer the option to prevent** third parties from storing information already stored on that equipment.

Abkehr vom PbD-
Ansatz. Nutzer muss
selbst aktiv werden.

1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, **shall offer the option to prevent** third parties from storing information already stored on that equipment.

2. Upon installation, the software shall inform the end-user about the privacy settings options and shall require the end-user to consent.

3. In the case of software placed on the market after 25 May 2018, the requirements at the time of the first placing on the market shall apply from 25 May 2018.

Auswahl der Optionen
sollte einfach
(Standardmodus) und
feingranular (Experte)
möglich sein und
Nutzer assistieren.

Quelle zum Leak des Entwurfs vom Dez 2016:
<http://www.politico.eu/wp-content/uploads/2016/12/POLITICO-e-privacy-directive-review-draft-december.pdf>

Beispiele: Handreichungen für Hersteller und Nutzer

- **AppPETs:** Library für App-Entwickler
 - Quelloffene Library, die typische Abläufe als PET implementiert
 - Automatisierte Prüfung von Software und Updates
 - Vereinfachte spätere Zertifizierung



- **AN.ON-Next:** „zero effort privacy“
 - Anonymisierungsdienst beim ISP



- Weitere Förderung der Forschung & Entwicklung nötig z.B. durch
 - EU-Kommission (H2020-Programm)
 - Bund (BMBF, BMWi) und Ländern



Überblick

1. Datenschutz: mehr als Informationssicherheit
2. Technischer Datenschutz bisher in Deutschland
3. Neues aus Europa (DSGVO, ePrivacyVO)
4. Um- und Durchsetzung
- 5. Fazit**

Fazit

- Privacy by Design ist zentral angelegter Grundsatz
- Pflichten zu PbD in Art. 25 stark eingeschränkt
- Durchsetzbarkeit durch Aufsichtsbehörden wäre gegeben aber Umfang der Pflichten bedarf der Konkretisierung
- Adressaten: Nur die Verantwortlichen
Mittelbar die Hersteller verpflichten. Nötig dazu „verantwortliche“ Abnehmer mit nötiger Marktmacht, z.B. Mitwagenfirmen für den Automobilbereich.



**AppPETs – Datenschutzfreundliche
Smartphone-Anwendungen ohne
Kompromisse**



**Forum Privatheit und selbstbestimmtes
Leben in der Digitalen Welt
(Privacy-Forum)**

Beide Projekte gefördert
vom Bundesministerium
für Bildung und Forschung:



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

Förderhinweis



SPECIAL

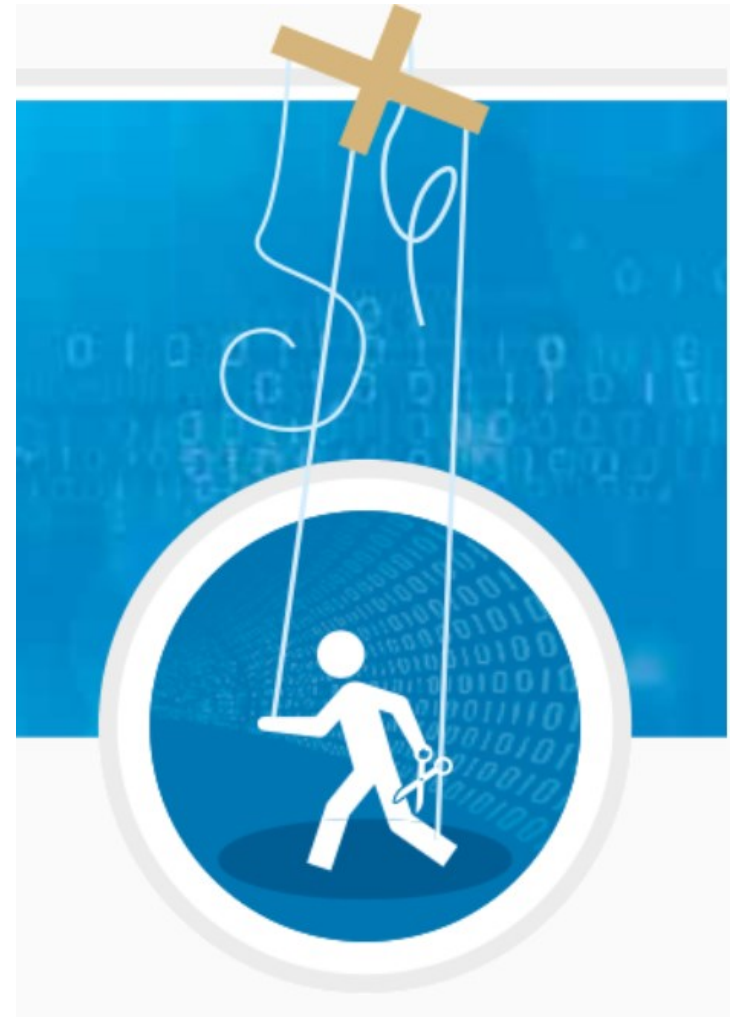
**Scalable Policy-awareE linked data
arChitecture for prIvacy, trAnsparency and
compliance (SPECIAL)**

Gefördert durch die
Europäische Kommission im
H2020 Rahmenprogramm
unter Grant Agreement
[731601](#)



Veranstaltungshinweis ULD Sommerakademie 2017

- **Montag, 18. September 2017**
- Thema: „Herausforderung ‚Informationelle Nichtbestimmung‘ – Privacy by Default für Technik, Wirtschaft und Politik“
- <https://datenschutzzentrum.de/sommerakademie/2017/>



Zeit für Fragen und Diskussion



Kontakt:

Harald Zwingelberg

uld6@datenschutzzentrum.de

www.datenschutzzentrum.de

0431/988-1222

ULD



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein