Kompetenzzentrum
Öffentliche IT

KOMPETENZZENTRUM ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

# DATENSCHUTZ UND TECHNIK: EIN INFORMATIONSPAPIER

Petra Hoepner

Fraunhofer
FOKUS

# IMPRESSUM

Autoren:
Petra Hoepner

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

ISBN: 978-3-9816025-5-5

1. Auflage April 2017

# VORWORT

Datenschutz hat in Deutschland eine lange Tradition. Datenschutzfreundliche Technologien zur Unterstützung der Datenminimierung wurden bereits 1997 von der nationalen Datenschutzkonferenz[1] gefordert. [DSK 1997] Neue technologische Entwicklungen verstärken diese Forderungen, da die Menge schutzbedürftiger Daten deutlich zugenommen hat.

Das Internet verbindet heute nicht nur Computer, sondern viele Dinge des täglichen Lebens. [Karaboga et al. 2015] Möglich wird dies durch Mikroelektronik und -sensorik, das heißt durch Kleinstkomponenten mit elektromechanischen und elektronischen Teilen. Dadurch verfügen diese Dinge nicht nur über die Fähigkeit, Umgebungsdaten zu erfassen, sondern diese auch zu kommunizieren. Ein Beispiel hierfür sind Wearables, die Körperdaten erfassen, verarbeiten und weiterleiten. Sie können dabei als separate Accessoires in Form von Armbändern, Uhren oder Kopfhörern genutzt werden oder aber als zusätzliche, integrierte Funktionalität beispielsweise in Bekleidung und Brillen auftreten. [Hoepner et al. 2016]

Unzählige Daten werden auch in intelligenten Verkehrssystemen erhoben und verarbeitet. Nachrichten zwischen Fahrzeugen und Verkehrsinfrastruktur umfassen unter anderem die aktuelle Position, Richtung und Geschwindigkeit. Diese Nachrichten können sehr einfach auf den Fahrer zurückgeführt werden und wären beispielsweise für Versicherungen zur Risikoabschätzung von großem Interesse.

Ein Teil der Daten, die in diesen intelligenten Infrastrukturen erhoben und verarbeitet werden, sind personenbezogen oder personenbeziehbar. Datenschutz wird daher immer wichtiger. Um Nutzer über die Preisgabe und Verwendung ihrer persönlichen Daten zu informieren, werden deswegen in vielen Online-Diensten Aktionen zu AGBs, Cookies oder Datenschutzerklärungen explizit angefordert. Allerdings »klicken« Nutzer zustimmend, da man sie entweder nicht versteht oder aber ansonsten die Dienste nicht nutzen kann.

In diesem Spannungsfeld möchte unser White Paper über aktuelle Entwicklungen zum Datenschutz, wie etwa die Europäische Datenschutz-Grundverordnung [EU-Datenschutz-Grundverordnung 2016], mit einem technischen Schwerpunkt informieren.

Ihr Kompetenzzentrum Öffentliche IT

[1] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI): Die Datenschutzbeauftragten des Bundes und der Länder tagen zweimal jährlich unter turnusmäßig wechselndem Vorsitz. Die Konferenz verabschiedet abgestimmte Entschließungen, die die Haltung der Datenschützer des Bundes und der Länder in Fragen aus Technik, Wirtschaft oder Recht darlegen.

DAS KOMPETENZZENTRUM ÖFFENTLICHE IT ERFORSCHT PRAXISRELEVANTE KONZEPTE UND ENTWICKELT ANWENDUNGEN FÜR DIE BEREICHSÜBERGREIFENDE ZUSAMMENARBEIT ZWISCHEN ÖFFENTLICHER VERWALTUNG, ZIVILGESELLSCHAFT UND WIRTSCHAFT.

# INHALTSVERZEICHNIS

# 1. THESEN

**Informationelle Selbstbestimmung ist nur ein Ideal, denn Selbstdatenschutz schränkt häufig »meine« virtuelle Welt ein.**

Das Grundrecht auf informationelle Selbstbestimmung verleiht dem Einzelnen die Befugnis, grundsätzlich selbst zu bestimmen, wann und in welchem Umfang er persönliche Lebenssachverhalte preisgeben möchte. Um dieses Recht zu stärken, existiert eine Zustimmungspflicht. Selbstdatenschutz beziehungsweise die digitale Selbstverteidigung wird auch von Datenschutzbeauftragen gefordert. Allerdings klickt im Internet fast jeder bei Datenschutzbestimmungen, Cookie-Nachfragen und AGBs zustimmend, um schnellstmöglich Dienstleistungen in Anspruch nehmen zu können, frei nach dem Motto »Ich habe nichts zu verbergen«. Erfahrungen zeigen, dass viele Dienste gar nicht oder nur eingeschränkt genutzt werden können, wenn man seine Daten schützt. Persönliche Vorteile, Benutzbarkeit und Bequemlichkeit gehen verloren. So wird Datenschutz nicht nur zur Spaßbremse, sondern man schließt sich gegebenenfalls auch aus sozialen Online-Gemeinschaften aus.

**Pseudonyme gaukeln Datenschutz nur vor.**

Wenn man seine Identität nicht preisgeben möchte, werden häufig Pseudonyme als Schutzmethode eingesetzt. Ein Pseudonym kann aber immer auf eine entsprechende Person zurückgeführt werden. Es variiert hier nur der Schwierigkeitsgrad für das Aufdecken der realen Person.

**Die Zweckbindung von Daten kostet Zeit und Geld.**

Die Zweckbindung von Daten erlaubt deren Verwendung nur für den Zweck, für den sie erhoben wurden. Eine Wiederverwendung dieser Daten für andere Dienstleistungen im gleichen Kontext könnte auch Zeit und Geld sparen. Beispielsweise für Verwaltungsleistungen wäre eine gemeinsame Nutzung oder die aktive Übermittlung der Daten häufig wünschenswert. Daten und Dokumente der Bürger und Unternehmen müssten so nur genau einmal – once only – produziert oder erfasst werden.

**Datenschutz ist schwer zu vergleichen.**

Es existieren ca. 30 verschiedene Datenschutzsiegel [Stiftung Datenschutz 2017]. Dadurch ist eine Vergleichbarkeit für Bürgerinnen und Bürger schwierig, anders als z. B. bei der Energieeffizienzklasse (A+++ – D). Die Überflutung mit Siegeln verunsichert die Verbraucher und mindert das Vertrauen in diese Siegel.

**Datenschutzfördernde Technologien lösen keine Regulierungsprobleme.**

Die Regulierung von Datenschutz muss durch geeignete Technologien unterstützt werden. Dies betrifft einerseits die Technologien, die dem Datenschutz nützen sollen und andererseits neue Technologien, die datenschutzgerecht eingesetzt werden müssen. Technologien allein können die politische Zielsetzung und Regulierung allerdings nicht ersetzen.

**Datenschutz und Kriminalitätsbekämpfung werden als Widerspruch wahrgenommen.**

Nach Sicherheitsvorfällen wird oft die Frage gestellt, ob Anonymität, Zweckbindung und Löschung von Daten kriminelle Handlungen erleichtern beziehungsweise deren Entdeckung erschweren. Keiner möchte ständig überwacht werden, damit Verbrechen leichter aufgeklärt werden können. Jeder möchte jedoch vor Gefahren geschützt werden. Dieses Spannungsfeld ist nicht einfach lösbar.

# 2. DATENSCHUTZ UND PRIVATHEIT

Die informationelle Selbstbestimmung ist in Deutschland ein Grundrecht, dessen Fundament 1983 durch das Bundesverfassungsgericht im sogenannten Volkszählungsurteil gebildet wurde. [Bundesverfassungsgericht, Urteil vom 15.12.1983] Es verleiht dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Häufig wird dieses Recht auch durch die Begriffe Datenschutz beziehungsweise Privatheit charakterisiert. Ob ein Unterschied zwischen Datenschutz und Privatheit besteht und wie dieser definiert wird, hängt unter anderem von der Nation, dem Kulturkreis und der Sprache ab. [Gilbert 2014]

Der Schutz personenbezogener Daten ist rechtlich schon lange geregelt: durch die Datenschutzgesetze des Bundes und der Länder, ab 1995 durch die EU-Datenschutzrichtlinie, die jetzt durch die EU-Datenschutz-Grundverordnung (siehe Abschnitt Datenschutz-Grundverordnung) abgelöst wird.

Doch welche Gefahren lauern ohne Datenschutz? Im Erwägungsgrund 85 der Datenschutz-Grundverordnung werden die Schäden als physische, materielle oder immaterielle Schäden für natürliche Personen abstrakt beschrieben. Beispiele werden benannt, wie der Verlust oder die Einschränkung der Kontrolle über die personenbezogenen Daten, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von Daten, die dem Berufsgeheimnis unterliegen, oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.

Trotzdem ist die Vorstellungskraft, wie sich diese Schäden auf die eigene Person auswirken können, bei vielen Menschen nicht präsent. »Ich habe nichts zu verbergen« kennzeichnet deren Einstellung. Dabei gehen die Betroffenen davon aus, dass ihre Daten von den abfragenden Firmen oder Organisationen geschützt werden. Dass dies ein Trugschluss sein kann, beweisen die vielen Datenschutzskandale, die willentlich oder aus Unachtsamkeit geschehen konnten. Datenschutzvorfälle[2] häufen sich. Der Verlust von Gesundheitsdaten, Zugang zu fremden Online-Konten, der NSA-Skandal oder der fehlerhafte Versand von sensiblen Kundendaten per E-Mail sind nur einige Beispiele.

Neben diesen Vorfällen sind jedoch auch Schäden relevant, die auf der Erstellung von persönlichen Profilen basieren, um Verhaltensweisen zu prognostizieren, persönliche Vorlieben und Interessen auszunutzen oder um die Gesundheit, Zuverlässigkeit und wirtschaftliche Lage einzuschätzen. Problematisch für Betroffene ist hier, dass sie weder wissen, auf welchen Daten diese Profile basieren oder welche Algorithmen verwendet werden, noch wer die Daten in welcher Weise nutzt. Häufig wird diese Datenauswertung auch mit dem Sammelbegriff Big Data assoziiert, der allerdings auch viele andere Anwendungsbereiche umfasst.

Um Datenschutzrisiken und mögliche Schäden zu verhindern, müssen diese zuerst identifiziert und bewertet werden. Dann kann man rechtliche und organisatorische Regelungen und konkrete Maßnahmen organisatorischer oder technischer Art festlegen, die die Ziele des Datenschutzes unterstützen.

## 2.1 DATENSCHUTZPRINZIPIEN

Für die Informationssicherheit[3] hat sich die IT-Grundschutz-Vorgehensweise gemäß BSI-Standard 100-2 und den IT-Grundschutz-Katalogen bewährt. [BSI-Standard 100-2 2008; BSI IT-Grundschutz] Die Schutzziele der Informationssicherheit (im BSI-Standard als Grundwerte bezeichnet) Vertraulichkeit, Integrität und Verfügbarkeit gilt es dabei mit einem bestimmten Sicherheitsniveau (normal, hoch oder sehr hoch) durch konkrete Sicherheitsmaßnahmen zu erreichen.

Ein ähnliches Vorgehen wurde auch für den Datenschutz vorgeschlagen [Rost 2012; Probst 2012]. Als grundlegendes Ziel ist immer die Datenminimierung (wird teilweise auch als Datensparsamkeit bezeichnet) zu nennen, denn Daten, die nicht erhoben werden, müssen auch nicht geschützt werden. Daneben

[2] »Projekt Datenschutz« dokumentiert Fälle von Datenpannen und Datenmissbrauch, die an die Öffentlichkeit gelangen, http://www.projekt-datenschutz.de/datenschutzvorfaelle.

[3] Basierend auf BSI Glossar: Informationssicherheit (auch oft als Datensicherheit bezeichnet) hat den Schutz von Informationen (in jeglicher Form) als Ziel. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung, sowie mit dem Schutz der IT-Systeme. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kataloge/Inhalt/Glossar/glossar_node.html.

DIE INFORMATIONELLE SELBSTBESTIMMUNG
IST IN DEUTSCHLAND EIN GRUNDRECHT.

sind für den Datenschutz sechs Schutzziele (auch als Gewährleistungsziele bezeichnet) relevant. Sie umfassen die drei klassischen Schutzziele der Informationssicherheit hinsichtlich der personenbezogenen Daten und drei spezifische Datenschutzziele:

- **Vertraulichkeit:**
  Nur Befugte dürfen in zulässiger Weise zugreifen.
- **Integrität:**
  Die Daten sind vollständig und unverändert.
- **Verfügbarkeit:**
  Die Daten können immer wie vorgesehen genutzt werden.
- **Transparenz:**
  Die Verarbeitung der Daten kann nachvollzogen, überprüft und bewertet werden.
- **Nichtverkettbarkeit:**
  Die Daten können nicht verknüpft werden, um sie für einen anderen als den vorgesehenen Zweck zu nutzen.
- **Intervenierbarkeit:**
  Betroffene können ihre Rechte hinsichtlich der Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung ihrer Daten jederzeit wirksam wahrnehmen.

Ebenfalls aus der IT-Sicherheit wurde das Schutzniveau mit den Stufen normal, hoch und sehr hoch übernommen. Dabei werden die Schadensauswirkungen nicht in Bezug auf Organisationen wie bei der IT-Sicherheit, sondern auf die betroffenen Menschen betrachtet:

- **Normal:**
  Schadensauswirkungen sind begrenzt und überschaubar.
- **Hoch:**
  Schadensauswirkungen sind für Betroffene beträchtlich.
- **Sehr hoch:**
  Schadensauswirkungen sind existenziell bedrohlich.

## 2.2 ZIELKONFLIKTE

Das Recht auf informationelle Selbstbestimmung ist kein absolutes Recht, sondern erfordert meist ein Abwägen der Interessen einzelner Bürgerinnen bzw. Bürger und der Gemeinschaft. [Bock und Meissner 2012] Dieses Abwägen wird durch Zielkonflikte zwischen den einzelnen Schutzzielen ebenfalls verdeutlicht. Zielkonflikte entstehen immer dann, wenn zwei konkurrierende Schutzziele die gleichen Objekte, wie etwa Daten, Systeme oder Prozesse, referenzieren. [Rost und Pfitzmann 2009] Werden nicht die gleichen Objekte referenziert, können die Schutzziele auch ergänzend wirken. Im Einzelfall ist abzuwägen, in welchem Umfang die Erreichung eines Schutzziels zu Lasten des konkurrierenden Schutzziels erfolgen soll. [Friedewald et al. 2016]

Beispiele für Zielkonflikte werden im Folgenden kurz umrissen:

**Integrität (Unversehrtheit) vs. Intervenierbarkeit (Eingreifbarkeit):** Werden personenbezogene Daten zur Wahrung von Eigentumsrechten in einem IT-System gespeichert, so sollten diese nicht mutwillig verändert werden können (Unversehrtheit). Gleichzeitig müssen diese Daten im Falle von Fehlern oder bei Änderung des Eigentums verändert werden können (Intervenierbarkeit). Wesentlich ist hier allerdings, dass zwar die gleichen Daten referenziert werden, jedoch zusätzlich das IT-System der informationsverarbeitenden Stelle integer (unversehrt) sein muss und nur Befugten die Eingriffe gestattet und somit den Zielkonflikt löst.

**Vertraulichkeit vs. Verfügbarkeit:** Vertraulichkeit, das heißt die Nichtzugreifbarkeit auf Informationen, und Verfügbarkeit, das heißt die Zugreifbarkeit auf Informationen, bilden einen Widerspruch. Beispielsweise sind Gesundheitsdaten einer Person vertraulich, müssen jedoch im Krankheitsfall verfügbar sein. Auch in diesem Beispiel werden die gleichen Daten referenziert.

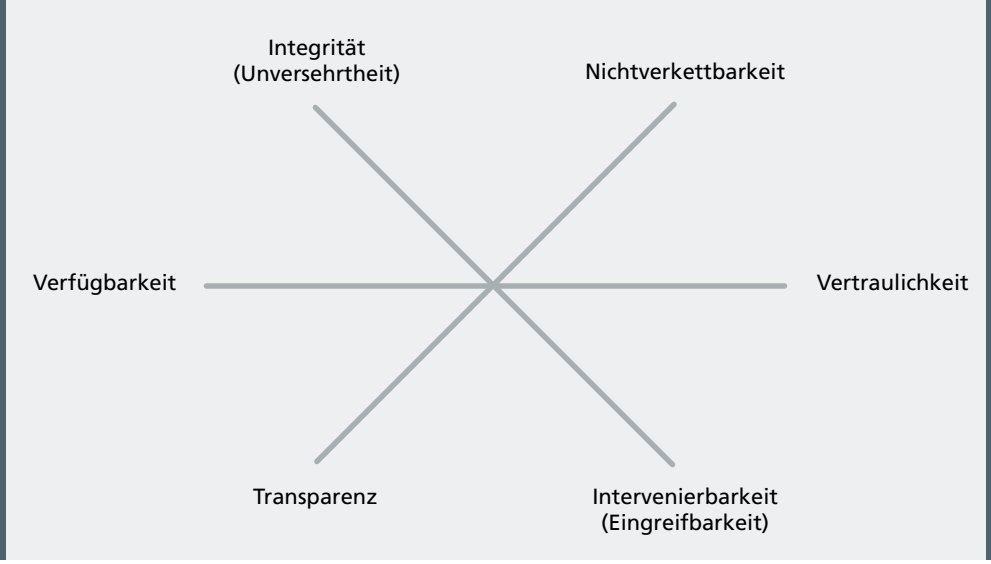



Abbildung 1: Zielkonflikte zwischen Datenschutzzielen (basierend auf [Rost und Bock 2011])

Zugreifbarkeit und Nichtzugreifbarkeit muss durch technische Berechtigungskonzepte und/oder personen- und ortsbezogene Zugangskontrolle realisiert werden.

**Transparenz vs. Nichtverkettbarkeit:** Nichtverkettbarkeit verhindert die Nutzung von personenbezogenen Daten für einen anderen als den ausgewiesenen Zweck. Transparenz dagegen ermöglicht die Beobachtbarkeit und Prüffähigkeit von Daten und Systemen. Hier kann sich ein Widerspruch einstellen, da möglicherweise Verkettungen geprüft werden müssen, die jedoch eigentlich unter dem Ziel der Nichtverkettbarkeit nicht vorhanden sein sollten.

Neben Widersprüchen zwischen Datenschutzzielen können auch Konflikte zwischen IT-Sicherheit und Datenschutz auftreten. Ein wesentlicher Grund dafür ist, dass unter diesen beiden Aspekten die jeweiligen Angreifer und Angegriffenen unterschiedlich sind. Stark vereinfacht kann man feststellen, dass IT-Sicherheit die IT-Infrastruktur und Geschäftsprozesse von Organisationen gegen kriminelle Angreifer schützen soll. Beim Datenschutz indessen werden die Rechte von Einzelnen gegen Aktivitäten dieser Organisationen und Dritter geschützt. [Rost und Bock 2011] Organisationen können unter anderem staatliche Stellen, Unternehmen, Interessenvertretungen oder Forschungsinstitutionen sein.

Datenschutz und IT-Sicherheit betrachten die Schutzziele daher aus unterschiedlichen Perspektiven mit etwas anderen Aufgaben und Schwerpunkten. Beispielsweise kann Datenminimierung (aus Datenschutzgründen) einer für die IT-Sicherheit erforderlichen Redundanz (für Datensicherung und Ausfallsicherheit) entgegenstehen. Transparenz von Verfahren als Schutzziel des Datenschutzes kann der Geheimhaltung von Schutzmechanismen und Daten in der IT-Sicherheit zuwiderlaufen. [Witt 2012]

# 3. AKTUELLE ENTWICKLUNGEN

Bisher haben die EU-Datenschutz-Richtlinie und die Datenschutzgesetze des Bundes und der Länder den Datenschutz in Deutschland reguliert. Darauf basierend wurden Gefährdungen und Schutzmaßnahmen im IT-Grundschutz-Baustein »Datenschutz« identifiziert. [BSI IT-Grundschutz Baustein B 1.5] Durch Verabschiedung der EU-Datenschutz-Grundverordnung werden sich Regelungen und Maßnahmen verändern.

## 3.1 DATENSCHUTZ-GRUNDVERORDNUNG

Die EU-Datenschutz-Richtlinie von 1995 wurde in den Mitgliedstaaten in ihren nationalen Datenschutzgesetzen unterschiedlich ausgelegt. Um eine Harmonisierung in der EU zu erreichen, wurde die EU-Datenschutz-Grundverordnung (DSGVO) verabschiedet. [EU-Datenschutz-Grundverordnung 2016] Sie ist am 25. Mai 2016 in Kraft getreten und wird am 25. Mai 2018 gültig. Als Verordnung ist sie unmittelbar in den Mitgliedstaaten verpflichtend wirksam.

Nach Art. 6 DSGVO gilt, dass die Verarbeitung personenbezogener Daten verboten ist, wenn sie nicht explizit erlaubt wird. Zulässig ist die Verarbeitung somit nur mit der Einwilligung des Betroffenen oder aufgrund von Ausnahmen laut DSGVO, wie etwa der Erfüllung von Verträgen, hoheitlichen Aufgaben oder lebenswichtigen Interessen. Die informierte Einwilligung sollte dabei durch eine eindeutige bestätigende Handlung erfolgen. Datenminimierung, Zweckbindung bezüglich Erhebung und Verarbeitung, Transparenz der Verarbeitung und Richtigkeit der Daten sind Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5. Explizit genannt ist das Recht auf Löschung, auch als Recht auf Vergessenwerden bezeichnet. Unternehmen müssen personenbezogene Daten löschen, wenn die Betroffenen dies wünschen und keine legitimen Gründe für die weitere Verarbeitung und Speicherung vorliegen.

Nach dem Marktortprinzip gilt die DSVGO nicht nur für EU-Unternehmen, sondern auch für außereuropäische Unternehmen, wenn sie auf dem europäischen Markt tätig sind. Beschwerden können jetzt immer an die Datenschutzbehörde des eigenen Mitgliedstaates gerichtet werden (One-Stop-Shop-Mechanismus). Schwere Verstöße gegen den Datenschutz müssen der nationalen Aufsichtsbehörde gemeldet und Rechtsverstöße können im Extremfall mit Bußgeldern bis zu vier Prozent des weltweiten Jahresumsatzes eines Unternehmens geahndet werden. [BfDI 2016]

### 3.1.1 Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen

Die DSGVO ist technologieneutral gestaltet (DSGVO Erwägungsgrund 15). Jedoch sind geeignete technische und organisatorische Maßnahmen erforderlich, um die rechtlichen Regelungen der DSGVO zu erfüllen. In der DSGVO werden einige Methoden und Techniken genannt (Artikel 25), wie die Verantwortlichen Datenschutz durch Technik (data protection by design) und datenschutzfreundliche Voreinstellungen (data protection by default) realisieren sollten. Konkret zu nennen sind hier etwa Verschlüsselung, Pseudonymisierung und Datenminimierung. Ebenfalls muss die Zweckbindung der erhobenen personenbezogenen Daten hinsichtlich ihrer Verarbeitung, Speicherfrist und Zugänglichkeit sichergestellt werden.

Dass für die technische Umsetzung der DSGVO Produkte, Dienste und Anwendungen entsprechend dem Stand der Technik erforderlich sind, wird nur am Rande erwähnt (Erwägungsgrund 78). Hersteller sollen »ermutigt« werden, geeignete Produkte bereitzustellen.

Datenschutzprobleme, die durch zunehmende Vernetzung und neue Technologien und Verfahren wie Big Data, Ubiquitous Computing, Cloud Computing oder das Internet der Dinge entstehen, werden nicht geregelt. [Roßnagel et al. 2016]

### 3.1.2 Datenschutz-Folgenabschätzung

Technische Innovationen, neue Systeme oder Verarbeitungsvorgänge können ungewollt auch neue Datenschutzrisiken verursachen. Wird ein hohes Risiko vermutet, so schreibt die DSGVO eine Datenschutz-Folgenabschätzung (DSFA; engl. data protection impact assessment, DPIA) vor.

Konkrete Beispiele, die eine DSFA erfordern, sind u. a. Videoüberwachung, die Verarbeitung umfangreicher Datensammlungen, die beispielsweise genetische, biometrische oder strafrechtliche Daten umfassen, oder die Bewertung von wirtschaftlichen oder gesundheitlichen Daten von Personen. Um besser einschätzen zu können, ob eine DSFA durchgeführt werden muss oder nicht, können die Aufsichtsbehörden entsprechende Bewertungslisten erstellen.

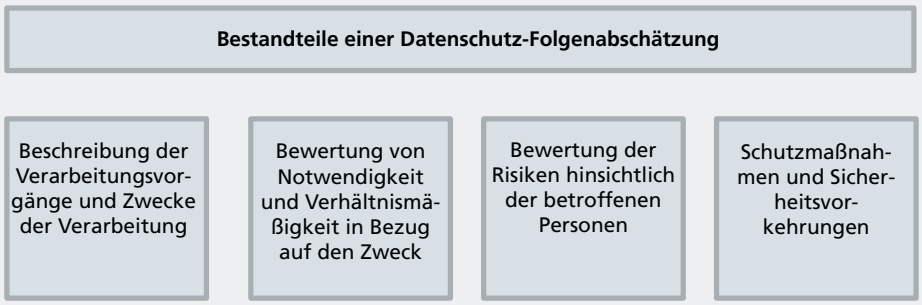



Abbildung 2: Mindestbestandteile einer Datenschutz-Folgenabschätzung gemäß DSGVO Art. 35 Abs. 7

Grundsätzlich besteht eine DSFA aus der Beschreibung der Verarbeitungsvorgänge für die personenbezogenen Daten, aus der Bewertung dieser hinsichtlich ihrer Notwendigkeit und potenzieller Risiken für die Betroffenen und aus der Beschreibung der geplanten Schutzmaßnahmen und Sicherheitsvorkehrungen, um den Risiken entgegenzuwirken. Die DSFA muss vom für die Verarbeitung Verantwortlichen durchgeführt werden. Die DSGVO legt nur die Mindestbestandteile der DSFA in Art. 35 Abs. 7 fest, es fehlen detaillierte Vorgaben und eine Beschreibung der genauen Vorgehensweise (vgl. Abbildung 2).

In den europäischen Mitgliedstaaten existieren unterschiedliche Ansätze und Prozesse zur Durchführung einer DSFA.

Ein mögliches Vorgehensmodell wird in [Friedewald et al. 2016] beschrieben und in [Hansen 2016] weiterentwickelt. Dabei werden vier Phasen durchlaufen: Vorbereitungsphase, Bewertungsphase, Maßnahmenphase und Berichtsphase (vgl. Abbildung 3). In der Vorbereitungsphase wird geprüft, ob eine DSFA überhaupt notwendig ist und falls ja, was konkret geprüft wird. In der Bewertungsphase erfolgt die Bewertung hinsichtlich der Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit. Diesbezüglich werden die Daten und deren Formate, die verwendeten IT-Systeme und deren Schnittstellen sowie Prozesse und Funktionsrollen separat betrachtet. Je nach möglichem Schadensumfang erfolgt die Bewertung in den Stufen normal, hoch und sehr hoch (vgl. Abschnitt Datenschutzprinzipien). In der Maßnahmenphase werden die Schutzmaßnahmen festgelegt, um den Risiken entgegenzuwirken. In der Berichtsphase wird der DSFA-Bericht erstellt und gegebenenfalls veröffentlicht. Die Bewertungs- und die Maßnahmenphase können konkret das Standard-Datenschutzmodell (SDM) nutzen (vgl. Abschnitt Standard-Datenschutzmodell).

### 3.1.3 Kritik an der Datenschutz-Grundverordnung

Die Ausgestaltung der DSGVO stößt allerdings auch auf Kritik, da weitreichende Öffnungsklauseln, Optionen und abstrakte Regelungen große Handlungsspielräume bieten, die die Harmonisierung infrage stellen können. [Roßnagel und Nebel 2016] »Das Hauptproblem der Datenschutz-Grundverordnung liegt jedoch in der hohen Diskrepanz zwischen der enormen Komplexität des Regelungsbedarfs einerseits und der Beschränktheit und Abstraktheit und damit Unterkomplexität ihrer Vorschriften andererseits. Sie will in 51 Artikeln des materiellen Datenschutzrechts die gleichen Probleme behandeln, für die allein im deutschen Datenschutzrecht Tausende von Vorschriften bestehen.« [Roßnagel 2016] Diese Problematik führt zu der Forderung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder an den Gesetzgeber, in allen gesetzgeberischen Bereichen die nationalen Spielräume im Sinne des Grundrechts auf informationelle Selbstbestimmung zu nutzen. [DSK 2016]

Grundsätzlich sind jedoch diese Gegensätze zwischen »einfachen« und übersichtlichen Vorschriften und hochkomplexer Detailregulierung im deutschen Recht problematisch. Um dies zu verbessern, wäre der europäische Ansatz der Konkretisierung einzelner Bereiche einer deutschen Detailausgestaltung vorzuziehen, denn nur so kann auch das deutsche Datenschutzniveau nach und nach in Europa etabliert werden.

Diese Ausgestaltungsvarianten spiegeln auch die Diskussion um den aktuellen Gesetzentwurf zur nationalen Umsetzung der EU-Datenschutz-Grundverordnung (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU)[4] wider, der Anpassungen des Bundesdatenschutzgesetzes und weiterer Gesetze vorsieht. Befürchtet wird, dass statt Rechtsklarheit mit EU-einheitlichen Regelungen wieder ein zersplittertes Datenschutzrecht mit nationalen Ausprägungen entsteht.

[4] Bundesministerium des Innern, Gesetzentwurf zur Anpassung des Bundesdatenschutzgesetzes an die Datenschutz-Grundverordnung, 1.2.2017 www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/entwurf-datenschutz-grundverordnung.html.

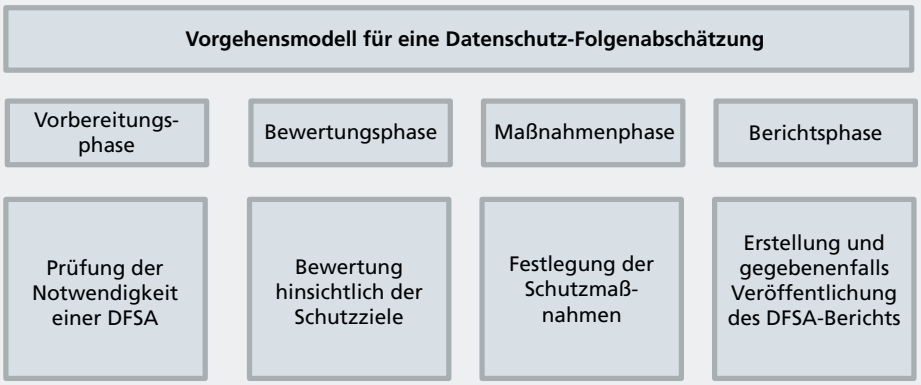



Abbildung 3: Vorgehensmodell für eine Datenschutz-Folgenabschätzung

## 3.2 STANDARD-DATENSCHUTZMODELL

Um Datenschutzanforderungen und -maßnahmen konsistent, einheitlich und nachprüfbar zu gestalten, wurde das »Standard-Datenschutzmodell« (SDM) entwickelt. [SDM 2016] Der Arbeitskreis Technik (AK Technik) der Datenschutzbeauftragten des Bundes und der Länder hat das SDM als Werkzeug für die Beratungs- und Prüftätigkeiten der Datenschutzbehörden konzipiert. Es unterstützt außerdem Organisationen bei der datenschutzgerechten Verarbeitung personenbezogener Daten.

Ähnlich der IT-Grundschutz-Methode sollen mit dem SDM Sollvorgaben nachvollziehbar mit ihrer Umsetzung verglichen werden können. Sollvorgaben konstituieren sich neben der DSGVO beispielsweise aus Normen, Verträgen, Einwilligungserklärungen und Organisationsregeln. Die Umsetzung der Vorgaben erfolgt auf der organisatorischen Ebene oder in IT-Verfahren und -Systemen.

Grundsätzlich unterscheidet das SDM (vgl. Abschnitt Datenschutzprinzipien) das generische Schutzziel der Datenminimierung, sechs Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit), drei Schutzbedarfsabstufungen (normal, hoch, sehr hoch) und drei Verfahrenskomponenten (Daten, Systeme, Prozesse). Das ergibt ein Referenzmodell für 6x3x3 (54) spezifische Datenschutzmaßnahmen, gegen die sich Verfahren standardisiert prüfen lassen. [Rost 2015]

Zudem werden verschiedene generische Schutzmaßnahmen im SDM aufgeführt und auszugsweise in Tabelle 1 dargestellt.

| Schutzziel | Generische Schutzmaßnahmen |
|---|---|
| Datenminimierung | Minimierung der erfassten Daten; automatische Sperr- und Löschroutinen; Pseudonymisierungs- und Anonymisierungsverfahren |
| Verfügbarkeit | Redundanz; Backup; Notfallmanagement und Reparaturstrategien |
| Integrität | Elektronische Siegel, Signaturen und Zeitstempel; Prüfsummen; Überprüfung von Soll-Ist-Werten |
| Vertraulichkeit | Verschlüsselung; Steganografie; Identitätsmanagement und Zugriffsbeschränkungen; räumliche und organisatorische Maßnahmen |
| Transparenz | Dokumentationspflichten beispielsweise von Verfahren, Tests, Verträgen, Einwilligungen; Protokollierung von Zugriffen und Änderungen; Nachweis von Quellen |
| Nichtverkettbarkeit | Pseudonymisierung und Anonymisierung; Trennung von Datenbeständen, IT-Systemen und Prozessen; Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten |
| Intervenierbarkeit | Ermöglichen von Rechten zur Einwilligung, Rücknahme, Widerspruch, Einsichtnahme, Korrektur, Sperrung und Löschung; Deaktivierungsmöglichkeit einzelner Funktionalitäten, Nachverfolgbarkeit von Aktivitäten |

Tabelle 1: Schutzziele und generische Schutzmaßnahmen aus dem Standard-Datenschutzmodell [SDM 2016]

FÜR DATENSCHUTZ-ZERTIFIKATE EXISTIEREN NOCH KEINE STANDARDISIERTEN ZERTIFIZIERUNGSVERFAHREN.

Um die generischen Maßnahmen in konkrete Maßnahmen umzusetzen, erarbeitet eine Arbeitsgruppe des AK Technik einen Katalog von Referenzmaßnahmen, der die technisch besten verfügbaren Schutzmaßnahmen aufführen soll. Der Katalog soll auch Elemente aus der Privacy-Forschung aufnehmen, beispielsweise attributbasierte Berechtigungsnachweise, verständliche Datenschutz-Piktogramme für verbesserte Transparenz oder automatisierte Prozesse zur Wahrnehmung der Betroffenenrechte im Rahmen der Intervenierbarkeit. [Hansen 2016]

## 3.3 STANDARDISIERUNG

Wichtige Vorgehensweisen für Informationssicherheit liefern die Standards der ISO/IEC-27000-Familie für Informationssicherheits-Managementsysteme und der IT-Grundschutz des BSI mit den IT-Grundschutz-Standards und -Katalogen. Diese beinhalten Methoden, Prozesse und Vorgehensweisen sowie Bausteine, Gefährdungen und Maßnahmen bezüglich Informationssicherheit. Datenschutzspezifische Regelungen werden jedoch nur eingeschränkt behandelt. In den IT-Grundschutz-Katalogen umfasst der Baustein B 1.5 »Datenschutz« die Rahmenbedingungen für den Datenschutz und zeigt die Verbindung zur Informationssicherheit im IT-Grundschutz auf. Der Baustein basiert allerdings noch auf der deutschen Gesetzgebung.

Die internationale Norm ISO/IEC 27001 [DIN ISO/IEC 27001 2015] legt die Anforderungen für die Einrichtung, Umsetzung und Aufrechterhaltung eines Informationssicherheits-Managementsystems (ISMS) fest. Die Norm berücksichtigt dabei die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität für alle Daten einer Organisation, nicht nur für die personenbezogenen Daten. Allerdings deckt sie nicht die datenschutzspezifischen Anforderungen aus der Sicht betroffener Personen ab.

Diverse weitere internationale Standards sind in den letzten Jahren für verschiedene Teilbereiche des Datenschutzes entstanden:

- ISO/IEC 27018: 2014 liefert einen Leitfaden zum Schutz personenbezogener Daten in öffentlichen Cloud-Diensten;
- ISO/IEC 29101 bietet ein Rahmenwerk für Datenschutzarchitekturen und listet Komponenten für die Implementierung datenschutzfreundlicher Systeme auf;
- ISO/IEC 29191 bietet ein Rahmenwerk für das Gebiet der teilweise anonymen, teilweise unverkettbaren Authentisierung, um die Verknüpfung von Identitätsinformationen zu verhindern;
- DIN EN 16571: 2014 (Deutsche Fassung) definiert Verfahrensweisen für die RFID-Datenschutzfolgenabschätzung;
- ISO/IEC 15944-8: 2012 »Information technology Business Operational View Part 8: Identification of privacy protection requirements as external constraints on business transactions« dient der Modellierung allgemeiner Anforderungen an den Schutz von persönlichen Informationen für Käufer in der Geschäftsabwicklung.

Eine Übersicht liefert der Kompass der IT-Sicherheitsstandards. [Bitkom]

## 3.4 ZERTIFIZIERUNG

Generell dienen Zertifikate und Gütesiegel dem Nachweis bestimmter Eigenschaften und sollen die Transparenz erhöhen und Vertrauen bei den Nutzern und Anwendern erzeugen.

In der DSGVO wird daher die Einführung von Datenschutzsiegeln und -prüfzeichen festgelegt, damit betroffene Personen und Auftraggeber das Datenschutzniveau von Produkten und Dienstleistungen schnell einschätzen können.

Für die IT-Sicherheit sind Zertifikate und Anerkennungen für Produkte, Managementsysteme, Personen, Stellen und Dienstleister nach festgelegten Kriterien und Verfahren schon lange etabliert. Das BSI hat nach dem BSI-Gesetz und der BSI-Zertifi-

zierungsverordnung die Aufgabe, Zertifizierungen durchzuführen und betreibt entsprechende Zertifizierungsprogramme. Jede Zertifizierung basiert auf einem Regelwerk, das die Geltungsbereiche, bedarfsgerechte Prüfkriterien, Anforderungen und Nachweise beschreibt und das Verfahren sowie das Management zur Durchführung der Zertifizierung festgelegt. Ein bekanntes Beispiel hierfür sind die Common Criteria (CC) für IT-Sicherheitszertifikate. Die CC-Zertifizierung basiert auf dem internationalen Standard ISO/IEC 15408. Anhand des Regelwerkes wird die Vertrauenswürdigkeit (Evaluation Assurance Level, EAL-Stufe) einer Sicherheitsleistung zertifiziert. Um die Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten zu vermeiden, gibt es Abkommen und Verfahren, die die gegenseitige Anerkennung regeln.

Datenschutz-Zertifikate haben noch nicht diese Qualität erreicht, da es noch kein abgestimmtes Zertifizierungsverfahren gibt. Im Gegenteil, in einer Übersicht der Stiftung Datenschutz zu in Deutschland angebotenen Datenschutzgütesiegeln und -zertifikaten sind 30 Einträge zu finden! [Stiftung Datenschutz 2017] Bekannte Beispiele sind das ULD Datenschutz-Gütesiegel, das Europäische Datenschutzsiegel (European Privacy Seal, EuroPriSe) und das ePrivacyseal. Eine einheitliche Grundlage für die verschiedenen Zertifizierungen existiert jedoch nicht. Neben eigenen Kriterien werden die Gesetze, die alte EU-Datenschutz-Richtlinie oder auch die Sicherheitsstandards der ISO/IEC-27000-Familie oder IT-Grundschutz angegeben. Ebenfalls sind die Unabhängigkeit und das Fachwissen der ausgebenden Organisationen nicht formal geregelt. Auch in anderen Ländern, beispielsweise in Frankreich und Großbritannien, wird an Datenschutzsiegeln gearbeitet.

Um eine einheitliche Bewertung im Sinne der DSGVO zu schaffen, ist eine abgestimmte gemeinsame europäische Datenschutzprüfung und -zertifizierung – analog einer Common-Criteria-Vorgehensweise – anzustreben. Bisher ist allerdings nur ein Register vorgesehen (DSGVO Art. 42 Abs. 8), in das der Europäische Datenschutzausschuss Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen aufnimmt und darüber veröffentlicht. Ob eine Vergleichbarkeit zwischen Siegeln unterstützt oder zukünftig doch ein Europäisches Datenschutzsiegel (DSGVO Art. 42 Abs. 5) eingeführt werden wird, ist allerdings noch unklar.

# 4. TECHNISCHE KONZEPTE, METHODEN UND LÖSUNGSANSÄTZE

Technischer Datenschutz, Systemdatenschutz oder datenschutzfördernde Technologien (auch bekannt als Privacy Enhancing Technologies (PET)) sind lange bekannte Konzepte, um Datenschutz durch technische Methoden, Maßnahmen und Produkte zu unterstützen. Heute werden oft die Begriffe Datenschutzbeziehungsweise Privacy-by-Design und Datenschutz- beziehungsweise Privacy-by-Default verwendet, die auch in der neuen Datenschutz-Grundverordnung genannt werden.

## 4.1 DATENSCHUTZ »BY DESIGN«

Datenschutzfördernde Technologien sind ein Sammelbegriff für Technologien zum Schutz der Privatsphäre. Dazu gehören Technologien zur Anonymisierung beziehungsweise Pseudonymisierung von Identitäten, kryptografische Ansätze zum Schutz sensitiver Daten, Techniken zur expliziten Einwilligung von Nutzern, zur Verhinderung ungewollter Nachverfolgung, zur Transparenz und Kontrolle der eigenen Daten, für das digitale Vergessenwerden, für Datenminimierung, vertrauliche Kommunikation und weitere. Die wesentlichen Ziele sind, möglichst wenig personenbezogene Daten zu sammeln und die Datensicherheit, Zweckbindung und Rechtmäßigkeit der Verarbeitung solcher Daten sicherzustellen. [Opiela et al. 2016] Datenschutz »by Design« lässt sich als »PETs plus datenschutzfördernde Prozesse« verstehen. [Rost und Bock 2011] Datenschutz soll so in die Gesamtkonzeption von Prozessen einbezogen und durch geeignete technische, aber auch organisatorische Maßnahmen realisiert werden. Dafür müssen die Hersteller geeignete Produkte bereitstellen und die Anwender diese auch einsetzen. [Hornung 2011]

Welche konkrete Technik eingesetzt werden soll, wird in der Gesetzgebung nicht vorgegeben. Meist wird hier der »Stand der Technik« referenziert (wie auch in DSGVO Artikel 25). So bleibt der Gesetzestext unabhängig von der technologischen Entwicklung und ist daher zukunftsfest. [TeleTrusT 2016]

Um den Stand der Technik im Datenschutz zu konkretisieren, hat die europäische Behörde für Netz- und Informationssicherheit ENISA eine Methode zur Analyse des Reifegrads von Datenschutz-Techniken sowie eine Bestandsaufnahme von Entwurfsstrategien, Ansätzen und Bausteinen verschiedener Reifegrade veröffentlicht. [ENISA 2015, 2014] In Deutschland erhofft man sich realistische Vorgaben vom Referenzmaßnahmen-Katalog des Standard-Datenschutzmodells (vgl. Abschnitt Standard-Datenschutzmodell).

## 4.2 DATENSCHUTZ »BY DEFAULT«

Datenschutzfreundliche Voreinstellungen sollen in Produkten, Diensten und Anwendungen sicherstellen, dass nur die für den Verarbeitungszweck erforderlichen personenbezogenen Daten erhoben und verarbeitet werden.

Bisher wurden häufig vielfältige Daten einer Person abgefragt, ob für die konkrete Anwendung notwendig oder nicht. Wollte man bestimmte Daten nicht übermitteln, musste man diese gezielt abwählen (Opt-out-Verfahren). Dies geht oftmals einher mit Ungewissheit, manchmal auch mit gewollter Verunsicherung, ob man nach Abwahl der Voreinstellungen die Anwendung oder den Dienst weiterhin mit vollem oder zumindest in verständlicher Art und Weise eingeschränktem Funktionsumfang nutzen kann.

Widersprüchlich wurde in der Vergangenheit beispielsweise der Umgang mit Cookies gehandhabt. Die sogenannte Cookie-Richtlinie der EU (2009/136/EG) hat jedoch explizit das Opt-in-Verfahren festgelegt. In der Benutzerführung auf Webseiten wird dies dem Nutzer heute meist mit Einblendungen beziehungsweise Pop-ups am oberen oder unteren Bildschirmrand kundgetan. Dabei erfolgt oftmals der Hinweis, dass man sich mit dem Cookie einverstanden erklärt, wenn man die Webseite oder den Dienst nutzt. Auch wenn dies ein erster Schritt ist, führt dieser Hinweis nicht zum datenschutzfreundlichen Umgang mit Cookies, sondern ist eher lästig, da man ja »sowieso nichts machen kann« und keine wirklichen Auswahlalternativen hat.

Ein weiteres Beispiel ist die »Do-not-track«-Einstellung in Browsern, die den Webseiten-Betreibern mitteilt, dass man nicht verfolgt werden möchte. Dies verhindert die Bildung von Nutzerprofilen. Übermittelt wird dieser Wunsch (im Header-Feld von HTTP) beim Abruf von Webseiten, die Berücksichtigung ist allerdings nicht weltweit gesetzlich verpflichtend. Die deutschen Datenschutzaufsichtsbehörden werten indes das Setzen des Do-not-track-Feldes als Widerspruch im Sinne des §15 Abs. 3

DIE GRENZE ZWISCHEN ANONYMITÄT UND PSEUDONYMITÄT IST DURCH BIG-DATA-ANALYSEN NICHT MEHR EINDEUTIG.

des Telemediengesetz (TMG). Manche Browser bieten auch einen Privacy Modus an, in diesem Fall werden alle Cookies und temporären Dateien nach Beendigung der Session wieder gelöscht.

Verbesserungen für diese Probleme soll die zukünftige EU E-Privacy-Verordnung bringen, die die geltenden EU-Richtlinien für Privacy und Cookies ablösen soll. [Vorschlag E-Privacy-Verordnung] Cookie-Regeln sollen vereinfacht werden und Do-not-track-Einstellungen verbindlich sein. Die Regeln sollen auch für Over-the-Top-Kommunikationsdienste gelten, wie beispielsweise VoIP-Telefonie, Instant-Messaging und webgestützte E-Mail-Dienste.

Kritisch ist indes festzustellen, dass sich Datenschutz »by Design und by Default« in der DSGVO nur an die für die Verarbeitung Verantwortlichen und nicht an die Hersteller von Datenverarbeitungstechnik richtet. Die für die Verarbeitung Verantwortlichen können freilich nur im Rahmen der von den Herstellern zur Verfügung gestellten Technik handeln, Hersteller müssten daher konsequenterweise ebenfalls zum Datenschutz durch Technik verpflichtet werden. [Roßnagel et al. 2016]

## 4.3 DATENSCHUTZ-ERKLÄRUNGEN UND DIE INFORMIERTE EINWILLIGUNG

Datenschutzerklärungen als Teil der AGBs und die informierte, bewusste Einwilligung sollen das Recht auf informationelle Selbstbestimmung fördern. Laut einer Studie sind diese AGBs jedoch meist zu umfangreich, unverständlich, in sich widersprüchlich und/oder unverhandelbar, daher bestätigen die meisten Menschen, diese gelesen zu haben, obwohl das nicht stimmt. [DIVSI 2014] Angeblich würde man im Durchschnitt 76 Arbeitstage im Jahr benötigen, um alle AGBs der Dienste zu lesen, die man im Internet nutzt. [Madrigal 2012]

Um die inflationäre Einwilligungsflut und die damit einhergehende Überprüfungs- und Zustimmungsmüdigkeit einzudämmen, soll durch die Stiftung Datenschutz eine vereinfachte und transparente Form der Einwilligung zur Nutzung personenbezogener Daten im Geschäftsverkehr entwickelt werden. Insbesondere sollen dabei technische Lösungswege geprüft werden. [Stiftung Datenschutz 2016] Verschiedene Möglichkeiten wurden bereits in der Vergangenheit vorgeschlagen, beispielsweise Piktogramme, Zwei-Klick-Lösungen (Aktivierung von Schaltflächen durch Anklicken) oder »Just-in-time«-Einwilligungserklärungen, die erst dann die Einwilligung eines Nutzers anfordern, wenn tatsächlich eine Übertragung beziehungsweise Verarbeitung der Daten erfolgen soll.

Zweifelhaft bleibt trotzdem, ob technische Lösungen zur Einwilligung jemals ausreichen können. Für Nutzer wäre es nämlich wichtiger, dass Datensammelei durch Regulierung beziehungsweise durch technische Systeme unterbunden wird. Visionär wäre es, wenn Daten sich selbst schützen würden und eine unerlaubte Weiterleitung und Verarbeitung so verhindert werden könnte.[5] Erste Schritte in diese Richtung sind Einschränkungen bezüglich der Lebensdauer von Daten. Bisherige Versuche, so der digitale Radiergummi mit digitalen Verfallsdaten oder digitales Rechtemanagement (DRM) zur Überwachung von Zugriffsrechten, wie schon für Musik versucht, konnten bisher allerdings nicht überzeugen.

[5] Diese Idee wird im Instant-Messaging-Dienst Snapchat beworben. Gesendete Fotos zerstören sich nach ein paar Sekunden selbst. Allerdings konnten diese in der Ordnerstruktur des genutzten Geräts wiedergefunden und hergestellt werden. Auch die Datenschutzbestimmungen werden kritisiert. [Wikipedia Snapchat].

## 4.4 IDENTITÄT, ANONYMITÄT UND PSEUDONYMITÄT

Die Identität einer Person wird durch verschiedene Merkmale charakterisiert. Mit einer bestimmten Konstellation von personenbezogenen oder personenbeziehbaren Daten lässt sich eindeutig eine Person bestimmen. Datenschutz soll die Verfügbarkeit dieser Daten rechtskonform einschränken.

Die Anonymisierung der Daten ist ein wirksames Mittel, um den Personenbezug unwiderruflich aufzulösen. Gebräuchliche Verfahren zur Anonymisierung sind die Randomisierung (Techniken zur Datenverfälschung, die die direkte Verbindung von Daten zu einer bestimmten Person unterbinden) oder Generalisierung (Techniken, die Informationen reduzieren, indem Größenskalen oder -ordnungen verändert werden). [Artikel-29-Datenschutzgruppe 2014] Anonyme Daten unterliegen nicht der Datenschutzgesetzgebung.

Zwischen vollständiger Identität und Anonymität gibt es viele Abstufungen, die man als Pseudonymität bezeichnet. Pseudonyme erlauben mehr oder weniger aufwendig die Re-Identifizierung, das heißt den Rückschluss auf eine bestimmte Person; sie unterliegen daher der Datenschutzgesetzgebung.

Problematisch ist heutzutage, dass die Grenze zwischen Anonymität und Pseudonymität nicht eindeutig ist. Durch Big-Data-Analysen einschließlich anfallender Metadaten unterschiedlicher Art kann aus Daten (auch hinsichtlich verwendeter Pseudonyme) ein Personenbezug hergestellt werden.[6] Messbar und beweisbar ist das jedoch meist nicht.

[6] Über den globalen Handel mit intimsten Nutzerdaten, die durch Ausspähen, Analyse und Zusammenführen entstanden sind, wurde unlängst berichtet. [NDR 2016].

## 4.5 SELBSTDATENSCHUTZ

Das aktive Ergreifen von technischen und organisatorischen Maßnahmen zum Schutz der eigenen Daten wird auch als Selbstdatenschutz, manchmal auch als digitale Selbstverteidigung, bezeichnet. Dies umfasst meist folgende Methoden [Karaboga et al. 2014; klicksafe.de 2016]:

- Anwenden von Verschlüsselung für die vertrauliche Speicherung und Übermittlung von Daten beispielsweise in der Cloud, bei E-Mail oder Instant Messaging;
- Verwenden von Anti-Tracking-Einstellungen von Browsern oder Plug-Ins zum Verbergen des Surfverhaltens;
- Nutzung von Anonymisierungs-Tools und -Diensten, die die Identität einer Person verbergen;[7]
- Anwenden von IT-Einstellungen, wie sichere Passwörter, Abschalten von Mobilverbindungen, Verbieten von Rechten etc.;
- Verwenden von datenschutzfreundlichen Diensten und Anwendungen, statt datenschutzignoranter Dienste (häufig solcher der globalen Technologiekonzerne).

Vielen Menschen sind diese Schutzmaßnahmen bekannt. Trotzdem werden sie, je nach Sicherheitsgefühl, eher selten gezielt eingesetzt. Dies wird auch als »Privacy-Paradox« bezeichnet, also als Gegensatz zwischen Wissen und Handeln, bei dem das Wissen nicht auf das Handeln übertragen wird. [klicksafe.de 2016] Auch wenn verschiedene Ursachen bekannt sind, wie etwa Bequemlichkeit, Boni und Gutscheine, aber auch soziale Teilhabe, so ist das sicherlich nur eine Seite. Auf der anderen Seite steht ein Gefühl der Machtlosigkeit gegenüber fremdverschuldeten Sicherheits- und Datenschutzvorfällen, die nicht durch Selbstdatenschutz verhindert werden können. Zudem

[7] Beispielsweise das Anonymisierungsnetzwerk Tor für die Anonymisierung von Verbindungsdaten [Wikipedia Tor].

DIE ELEKTRONISCHE VERARBEITUNG VON VERSCHLÜSSELTEN DATEN WIRD ERFORSCHT.

kann man sich nie sicher sein, dass ein vorhandener Selbstdatenschutz auch ausreichend ist, da eine Mess- und Überprüfbarkeit solcher Schutzmaßnahmen bisher nicht möglich ist.

## 4.6 KRYPTOGRAFISCHE ENTWICKLUNGEN

Die Verschlüsselung von Daten mit kryptografischen Verfahren unterstützt deren Integrität und Vertraulichkeit bei der Speicherung oder der Übermittlung. Bisher mussten Daten jedoch entschlüsselt werden, um sie weiterzuverarbeiten. Entschlüsselte Daten können allerdings leichter missbraucht werden. Aus diesem Grund werden verschiedene Techniken erforscht, die die Verarbeitung von verschlüsselten Daten erlauben. Beispiele hierfür sind:

- Homomorphe Kryptografie: Erlaubt (meist stark eingeschränkte) Berechnungen auf verschlüsselten Daten, ohne dass diese entschlüsselt werden müssen. Diese können beispielsweise in der Cloud verarbeitet werden, ohne sie zu entschlüsseln. Das Ergebnis wird dann verschlüsselt an den Cloud-Nutzer übermittelt. [Schwan 2010]
- Private Information Retrieval: Unterstützt Datenbankanfragen, ohne dass die Datenbank beziehungsweise der Datenbank-Administrator Kenntnis über den genauen Inhalt der Anfrage erhält. So wird die Privatheit der Anfragenden unterstützt, wenn sie öffentliche Datenbanken benutzen. Die Verknüpfung von Anfragen wird ebenfalls unterbunden und damit eine Profilbildung für den anfragenden Nutzer verhindert. [Aguilar-Melchor et al. 2016]
- Sichere Multi-Parteien-Berechnung: Bezeichnet ein privatheitsunterstützendes kryptografisches Protokoll, bei dem gemeinsame Berechnungen auf geheimen Eingaben jeder Partei durchgeführt werden können, wobei die Geheimnisse gewahrt bleiben. Sensitive Daten bleiben so geschützt. Ursprung ist das sogenannte Millionärsproblem, bei dem zwei sich gegenseitig misstrauende Millionäre herausfinden können, wer von ihnen reicher ist, ohne dass sie sich ihren Besitz gegenseitig offenlegen müssen. [Beutelspacher et al. 2005]

# 5. ZUKUNFT DES DATENSCHUTZES

Ob Datenschutz heutzutage noch sinnvoll ist, wird von der Post-Privacy-Bewegung angezweifelt. Diese geht davon aus, dass alle Daten früher oder später an die Öffentlichkeit gelangen. Daher könne man sie auch selbst offenlegen. Vielleicht ergäbe sich daraus eine Zukunft, die von einer höheren gegenseitigen Toleranz geprägt ist. Um dem Allgemeinwohl zu dienen, stellen Daten-Philanthropen heute schon freiwillig ihre Daten in Form sogenannter Datenspenden beispielsweise für Wissenschaft und Forschung bereit. [Weber 2016; Welzel 2016]

Den Schutz der eigenen Daten aufzugeben, ist jedoch nicht die von der Mehrheit gewünschte Lösung. Wie der Dreiklang zwischen Datenschutz, Sicherheit und Freiheit auch zukünftig trotz oder wegen neuer Technologien ausbalanciert werden kann, bedarf daher ständiger Diskussion. Ob Datensouveränität, das heißt der selbstbestimmte Umgang mit persönlichen Informationen, Datenminimierung ablösen kann, bleibt allerdings fragwürdig. [Krempl 2015; Beer 2017]

Sind manche Datenschutzmängel für den Einzelnen noch tragbar, so sind Datenschutz und Privatsphäre für den gesellschaftlichen Dialog, freie Meinungsäußerung und die Demokratie von großer Bedeutung. Siavoshy vergleicht diese Rechte mit dem Wahlrecht, das ebenfalls für die Gesellschaft als Ganzes bedeutender ist als für die einzelne Person. [Siavoshy 2015] Auch aus diesem Grund muss Datenschutz weiterhin gefördert und erforscht werden.

Wichtige Forschungsthemen sind unter anderem:

- Metriken, Messbarkeit und Nachweisbarkeit eines ganzheitlichen Datenschutzes über verschiedene Techniken und Verfahren hinweg;
- Kontextbezogener Datenschutz, bei dem die Einwilligung für Datennutzung nicht für einzelne Anwendungen, sondern abhängig von einem bestimmten Kontext, wie etwa Zeit, Ort, Anwendungsbereich oder einer Kombinationen davon erteilt und überprüft wird;
- Techniken für das Recht auf Vergessenwerden, damit Daten auch wieder verschwinden;
- Systemseitiger Datenschutz, der den Nutzer entlastet und möglichst wenig Selbstdatenschutz erfordert;
- Anonymisierungstechniken und Nachweisbarkeit von deren korrekter Funktionsweise, auch hinsichtlich nachträglicher Verkettungen über große Datenbestände;
- Anwendungen und Verfahren, die mit verschlüsselten Datenbeständen arbeiten können, ohne diese zu entschlüsseln;
- Datenschutz für neue Technologien und Verfahren wie Big Data, Smart Home, Cloud Computing oder das Internet der Dinge verbessern.

# 6. HANDLUNGSEMPFEHLUNGEN

**Datenschutz und Datensicherheit müssen als Einheit betrachtet werden**.
Datenschutz versagt, wenn die Datensicherheit vernachlässigt wird. Daher müssen Datenschutz und Datensicherheit als Einheit betrachtet und durch geeignete technische Mittel unterstützt werden. Einfache Lösungen sind erforderlich. Die Eignung sollte gemessen, unabhängig geprüft und beispielsweise anhand einiger weniger verständlicher Siegel oder Zertifikate bewertet werden können.

**Datenschutz soll möglichst selbstständig funktionieren und den Nutzer so wenig wie möglich belasten.**
Viele Einzellösungen für verschiedene Datenschutzaspekte sind vorhanden. Jedoch überfordert die Auswahl geeigneter Sicherheits- und Datenschutztechniken die meisten Nutzer. Diese müssen entlastet werden, indem systemischer Datenschutz gestärkt wird und die Verantwortung dafür bei datenverarbeitenden Institutionen und Organisationen verbleibt.

**Nein sagen dürfen. Fairness, Wahlfreiheit und Transparenz bei der Nutzung von Daten stärken.**
Big Data ist als wirtschaftliches Potenzial unumstritten. Fairer Datenhandel muss auch durch geeignete Technikgestaltung unterstützt werden. Derzeitige Praktiken von Diensteanbietern dienen jedoch dazu, Nutzer zur Datenabgabe mehr oder weniger direkt zu zwingen. Dieser Druck sollte durch transparente Wahlmöglichkeiten ersetzt werden. Beispielsweise sollte man die Bezahlung mit Daten statt mit Geld als Alternative gestalten und nicht verschleiern, wie es heute oft üblich ist. Auch die weitere Verwendung der Nutzerdaten sollte in verständlichen Datenschutzbestimmungen dokumentiert und durch verbraucherfreundliche Einverständniserklärungen unterstützt werden.

**Datenschutzfreundliche Vorbilder und Alternativen fördern.**
Datenschutzfreundliche Alternativen müssen stetig gefördert werden, auch wenn deren Chancen, zur Marktmacht zu reifen, oft gering sind. So werden Vorbilder geschaffen und der Markt kann im Laufe der Zeit verändert werden, wenn das Bewusstsein für Datenschutz bei Nutzern wächst.

**Datenschutztechniken erforschen.**
Unerlaubte Datenweitergabe und -nutzung sollte möglichst technisch verhindert werden können. Wünschenswert wäre eine Nachvollziehbarkeit beziehungsweise Beweisbarkeit. Eine Verbesserung der Anonymisierung, das untrennbare Verbinden von Rechten mit den Daten oder eine zeitliche Einschränkung der Datenspeicherung sind einige Ansätze.

**Opfer algorithmischer Bewertung verhindern.**
Da personenbezogene Daten zunehmend in Algorithmen für Risikoeinschätzungen und Zukunftsprognosen verwendet werden, beispielsweise für Scoring, kann es durch fehlerhafte Daten zu Fehlentscheidungen kommen. Die Betroffenen wissen weder, welche Daten verwendet wurden, noch, warum sie negativ beurteilt werden. Bisher muss jeder Einzelne bei den verschiedenen Auskunfteien separat nachfragen, was über ihn gespeichert ist. Das ist zwar einmal jährlich kostenlos, sollte aber stark vereinfacht werden, beispielsweise durch eine zuständige Institution beziehungsweise durch technische Kontroll- und Eingriffsmöglichkeiten zur Datenkorrektur.

**Europäisch denken.**
Die EU-DSGVO ist ein wichtiger Schritt, um in Europa ein einheitliches Datenschutzniveau zu erreichen. Dieses sollte nicht durch nationale Regelungen aufgeweicht, sondern durch gemeinsame Konkretisierungen auch im Hinblick auf technische Lösungen gestärkt werden. Vertrauenswürdige europäische (oder globale) Datenschutzsiegel und -prüfzeichen sollten die Auswahl geeigneter Dienste und Produkte unterstützen.

# 7. LITERATURVERZEICHNIS


Aguilar-Melchor, Carlos; Barrier, Joris; Fousse, Laurent; Killijian, Marc-Olivier (2016): XPIR: Private Information Retrieval for Everyone. In: Proceedings on Privacy Enhancing Technologies 2016 (2). DOI: 10.1515/popets-2016-0010.

Artikel-29-Datenschutzgruppe (2014): Stellungnahme 5/2014 zu Anonymisierungstechniken. 0829/14/DE. Online verfügbar unter ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf.

Beer, Kristina (2017): Verbraucherschützer warnen Merkel vor Ende der Datensparsamkeit. In: Heise Online, 03.01.2017. Online verfügbar unter https://heise.de/-3585744.

Beutelspacher, Albrecht; Neumann, Heike B.; Schwarzpaul, Thomas (2005): Multiparty-Computations. In: Albrecht Beutelspacher, Heike Neumann und Thomas Schwarzpaul (Hg.): Kryptografie in Theorie und Praxis. Mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk. Wiesbaden: Vieweg, S. 250 - 265.

BfDI (Hg.) (2016): Datenschutz-Grundverordnung. BfDI Informationsbroschüre. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI – Info 6). Online verfügbar unter www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.html.

Bitkom (Hg.): Kompass der IT-Sicherheitsstandards. Online verfügbar unter www.kompass-sicherheitsstandards.de/Default.aspx.

Bock, Kirsten; Meissner, Sebastian (2012): Datenschutz-Schutzziele im Recht. In: Datenschutz und Datensicherheit - DuD 36 (6), S. 425 - 431. DOI: 10.1007/s11623-012-0152-0.

BSI IT-Grundschutz. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html.

BSI IT-Grundschutz Baustein B 1.5. Datenschutz. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01005.html.

BSI-Standard 100 - 2. IT-Grundschutz-Vorgehensweise (2008). Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html.

Bundesverfassungsgericht, Urteil vom 15.12.1983, Aktenzeichen 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83. In: openJur 2012, 616.

DIN ISO/IEC 27001. Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (2015).

DIVSI (Hg.) (2014): DIVSI Studie Daten – Ware und Währung. Eine repräsentative Bevölkerungsbefragung des Instituts für Markt- und Politikforschung (dimap) im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI). Online verfügbar unter https://www.divsi.de/publikationen/studien/divsi-studie-daten-ware-und-waehrung/.

DSK (Hg.) (1997): Erforderlichkeit datenschutzfreundlicher Technologien. Entschließung. Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Bamberg. Online verfügbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/54DSK-ErforderlichkeitDatenschutzfreundlicherTechnologien.html.

DSK (Hg.) (2016): Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen. Entschließung. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. Schwerin. Online verfügbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/91DSK_EntschliessungDSStaerken.html.

ENISA (Hg.) (2014): Privacy and Data Protection by Design – from policy to engineering. Online verfügbar unter https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

ENISA (Hg.) (2015): Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies. Methodology, Pilot Assessment, and Continuity Plan (Version 1.0). Online verfügbar unter https://www.enisa.europa.eu/publications/pets.

EU-Datenschutz-Grundverordnung (2016): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/ EG (Datenschutz-Grundverordnung). Online verfügbar unter eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679.


Friedewald, Michael; Obersteller, Hannah; Nebel, Maxi; Bieker, Felix; Rost, Martin (2016): Datenschutz-Folgenabschätzung. Ein Werkzeug für einen besseren Datenschutz. White Paper. 2. Auflage. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Online verfügbar unter www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums.php.

Gilbert, Francoise (2014): Privacy v. Data Protection. What is the Difference? Online verfügbar unter https://www.francoisegilbert.com/?p=937.

Hansen, Marit (2016): Datenschutz-Folgenabschätzung – gerüstet für Datenschutzvorsorge? In: Datenschutz und Datensicherheit – DuD 40 (9), S. 587–591. DOI: 10.1007/s11623-016-0663-1.

Hoepner, Petra; Weber, Mike; Tiemann, Jens; Welzel, Christian; Goldacker, Gabriele; Stemmer, Michael et al. (2016): Digitalisierung des Öffentlichen. Hg. v. Jens Fromm. Kompetenzzentrum Öffentliche IT (ÖFIT); Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS. Berlin. Online verfügbar unter www.oeffentliche-it.de/documents/10181/14412/Digitalisierung+des+%C3%96ffentlichen.

Hornung, Gerrit (2011): Datenschutz durch Technik in Europa. In: ZD Zeitschrift für Datenschutz (02). Online verfügbar unter www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Hornung/Hornung_Datenschutz_durch_Technik_in_Europa_ZD_2011_51.pdf.

Karaboga, Murat; Masur, Philipp; Matzner, Tobias; Mothes, Cornelia; Nebel, Maxi; Ochs, Carsten et al. (2014): Selbstdatenschutz. White Paper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Online verfügbar unter www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums.php.

Karaboga, Murat; Matzner, Tobias; Morlok, Tina; Pittroff, Fabian; Nebel, Maxi; Ochs, Carsten et al. (2015): Das versteckte Internet. Zu Hause - Im Auto - Am Körper. White Paper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Online verfügbar unter www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums.php.

klicksafe.de (2016): Tipps zur digitalen Selbstverteidigung. klicksafe.de. Hg. v. Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz. Online verfügbar unter www.klicksafe.de/themen/datenschutz/privatsphaere/tipps-zur-digitalen-selbstverteidigung/.

Krempl, Stefan (2015): IT-Gipfel: Gabriel plädiert für Datensouveränität statt Datenschutz. In: Heise Online, 19.11.2015. Online verfügbar unter https://heise.de/-2966141.

Madrigal, Alexis C. (2012): Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days. The Atlantic. Online verfügbar unter www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

NDR (2016): Nackt im Netz: Millionen Nutzer ausgespäht, 01.11.2016. Online verfügbar unter www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaeht,nacktimnetz100.html.

Opiela, Nicole; Hoepner, Petra; Weber, Mike (2016): Das ÖFIT-Trendsonar der IT-Sicherheit. Hg. v. Kompetenzzentrum Öffentliche IT und Fraunhofer Institut FOKUS. Online verfügbar unter www.oeffentliche-it.de/publikationen?doc=42256&title=Trendsonar.

Probst, Thomas (2012): Generische Schutzmaßnahmen für Datenschutz-Schutzziele. In: Datenschutz und Datensicherheit – DuD 36 (6), S. 439 - 444. DOI: 10.1007/s11623-012-0154-y.

Roßnagel, Alexander (2016): Wie zukunftsfähig ist die Datenschutz-Grundverordnung? In: Datenschutz und Datensicherheit – DuD 40 (9), S. 561 - 565. DOI: 10.1007/s11623-016-0658-y.

Roßnagel, Alexander; Geminn, Christian L.; Jandt, Silke; Richter, Philipp (2016): Datenschutzrecht 2016 »Smart« genug für die Zukunft? Kassel: Kassel University Press. Online verfügbar unter www.uni-kassel.de/upress/online/OpenAccess/978-3-7376-0154-2.OpenAccess.pdf.


Roßnagel, Alexander; Nebel, Maxi (2016): Die neue Datenschutz-Grundverordnung. Ist das Datenschutzrecht nun für heutige Herausforderungen gerüstet? Policy Paper. 1. Auflage. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Online verfügbar unter www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums.php.

Rost, Martin (2012): Standardisierte Datenschutzmodellierung. In: Datenschutz und Datensicherheit – DuD 36 (6), S. 433 - 438. DOI: 10.1007/s11623-012-0153-z.

Rost, Martin (2015): Datenschutz, Privacy und das Standard-Datenschutzmodell. Forum Privatheit. Berlin, 27.11.2015. Online verfügbar unter https://www.forum-privatheit.de/forum-privatheit-de/aktuelles/veranstaltungen/veranstaltungsdokumente/2015-11-26u27_dokumentation_zukunft-der-informationellen-selbstbestimmung/1.3.c-2015-1127_Rost_DSTheorieSDM.pdf.

Rost, Martin; Bock, Kirsten (2011): Privacy By Design und die Neuen Schutzziele. In: Datenschutz und Datensicherheit – DuD 35 (1), S. 30 - 35. DOI: 10.1007/s11623-011-0009-y.

Rost, Martin; Pfitzmann, Andreas (2009): Datenschutz-Schutzziele – revisited. In: Datenschutz und Datensicherheit – DuD 33 (6), S. 353 - 358. DOI: 10.1007/s11623-009-0072-9.

Schwan, Ben (2010): Voll homomorphe Verschlüsselung in der Cloud. In: Heise Online, 16.06.2010. Online verfügbar unter https://heise.de/-1021361.

SDM (2016): Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. V.1.0 Erprobungsfassung. Hg. v. AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. Online verfügbar unter https://www.datenschutzzentrum.de/sdm/.

Siavoshy, Babak (2015): Why privacy matters even if you don't care about it (or, privacy as a collective good). Online verfügbar unter https://concurringopinions.com/archives/2015/06/privacy-as-a-collective-good.html.

Stiftung Datenschutz (Hg.) (2016): Projekt Einwilligung und Transparenz. Online verfügbar unter https://stiftungdatenschutz.org/themen/pims-studie/.

Stiftung Datenschutz (Hg.) (2017): Übersicht zu Zertifizierungen und Gütesiegeln im Datenschutz. Stand Februar 2017. Online verfügbar unter https://stiftungdatenschutz.org/fileadmin/Redaktion/PDF/Zertifizierungsuebersicht/SDS-Zertifizierungsuebersicht_02_2017.pdf.

TeleTrusT (Hg.) (2016): Handreichung zum »Stand der Technik« im Sinne des IT-Sicherheitsgesetzes (ITSiG). TeleTrusT – Bundesverband IT-Sicherheit e.V. Online verfügbar unter https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/TeleTrusT-Handreichung_Stand_der_Technik.pdf.

Vorschlag E-Privacy-Verordnung: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), vom 10.01.2017. Online verfügbar unter ec.europa.eu/transparency/regdoc/rep/1/2017/DE/COM-2017-10-F1-DE-MAIN-PART-1.PDF.

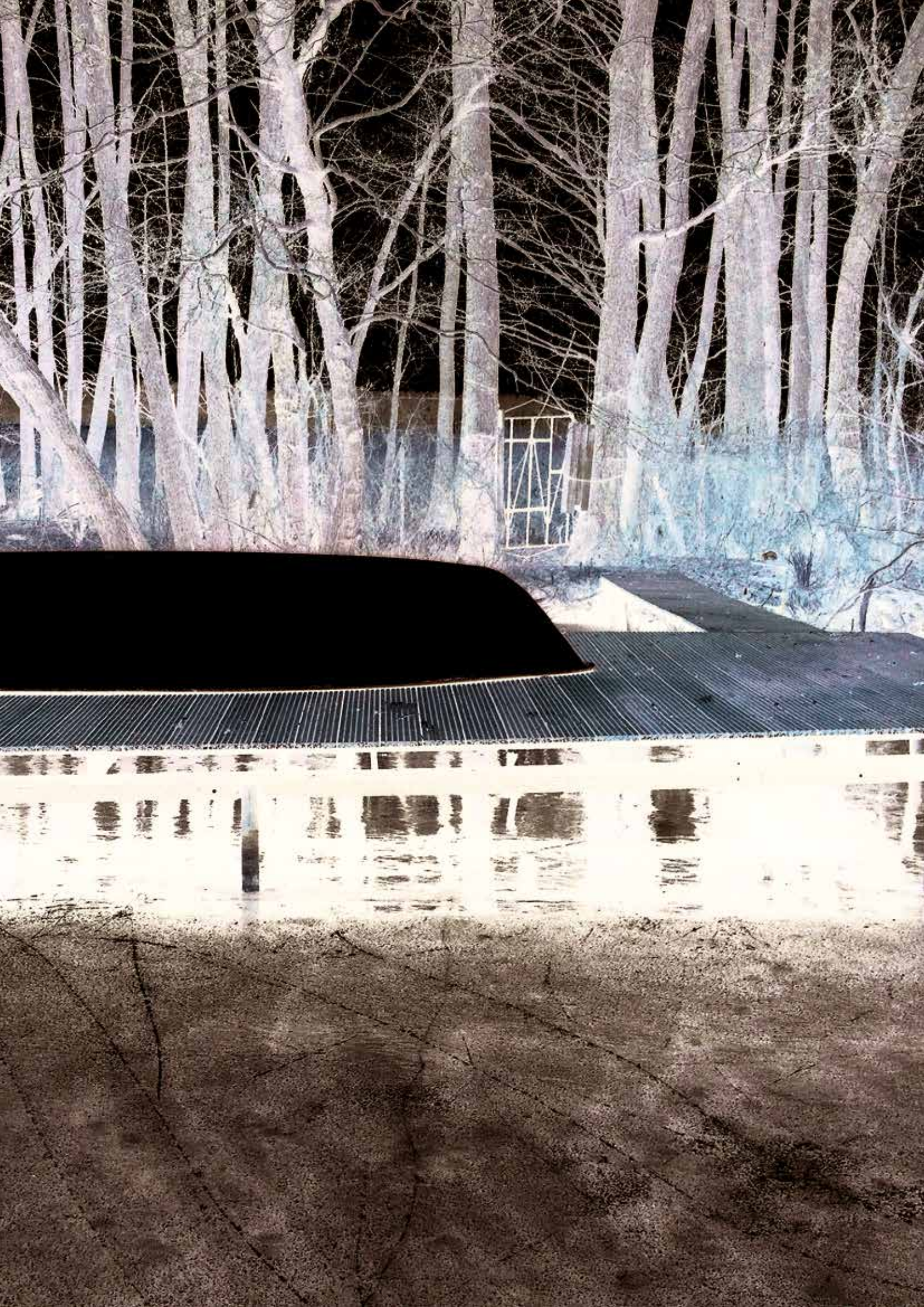
Weber, Mike et. al. (2016): Trendthema Post-Privacy. Online verfügbar unter www.oeffentliche-it.de/-/post-privacy.

Welzel, Christian et al. (2016): Trendthema Daten-Philanthrop. Online verfügbar unter www.oeffentliche-it.de/-/daten-philanthrop.

Wikipedia Snapchat. Online verfügbar unter https://de.wikipedia.org/w/index.php?title=Snapchat.

Wikipedia Tor. Online verfügbar unter https://de.wikipedia.org/wiki/Tor_(Netzwerk).

Witt, Bernhard C. (2012): Informationstechnik & Datenschutz – Ein spannendes Verhältnis. Ringvorlesung zur Technikfolgenabschätzung. Universität Stuttgart, 08.05.2012. Online verfügbar unter www.uni-ulm.de/fileadmin/website_uni_ulm/iui/datenschutz/IT_DS_2012-05-08.pdf.



GEFÖRDERT VOM

Bundesministerium
des Innern

## KONTAKT

Petra Hoepner
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de
Twitter: @OeffentlicheIT

ISBN: 978-3-9816025-5-5



kre | 1704 (Fotos: Fraunhofer FOKUS)