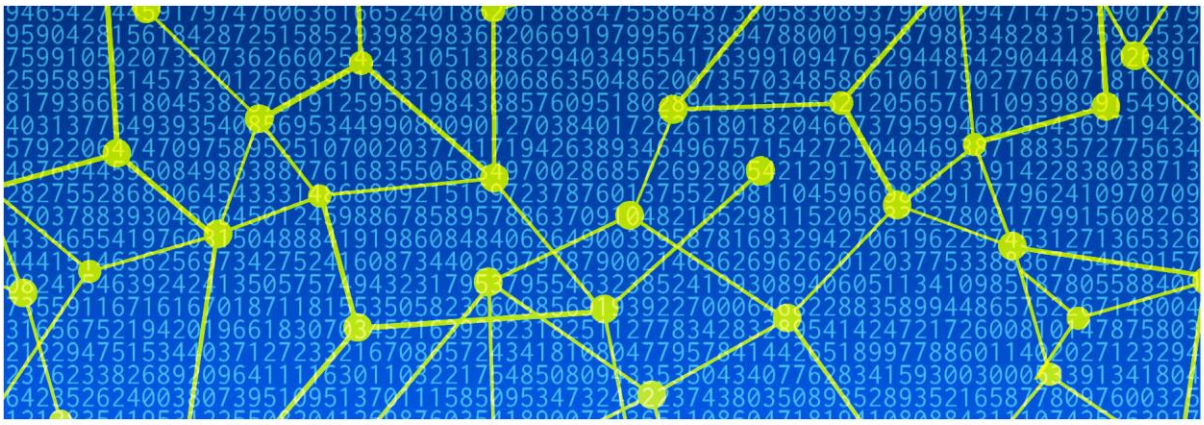

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 5/2018

Vorläufige Stellungnahme zu Schutz der Privatsphäre durch Technikgestaltung

EDPS

31. Mai 2018

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten (...) sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden"; er ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten" zuständig. Gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 ist die Kommission zur Konsultation des EDSB verpflichtet, „wenn [sie] einen Vorschlag für Rechtsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten annimmt".

Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und speziell mit einem konstruktiven und proaktiven Vorgehen beauftragt. In seiner im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag auf verantwortungsvolle Weise zu erfüllen gedenkt.

Mit dieser Stellungnahme soll ein Beitrag zu einer erfolgreichen Auswirkung der neuen Verpflichtung zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen leisten, die in Artikel 25 der Datenschutz-Grundverordnung niedergelegt ist, und zwar durch Sensibilisierung, Förderung einer sachdienlichen Debatte und Vorschläge für denkbare Vorgehensweisen.

Die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen werden im Hinblick auf ihre historische Entwicklung und auf ihre Umsetzung in Privacy Engineering-Methoden und Technologien zur Erhöhung des Datenschutzes (Privacy Enhancing Technologies) beleuchtet.

Diese Analyse ist vor dem Hintergrund des wachsenden und sich ausbreitenden Bedarfs an einer auf menschlichen Werten und auf Ethik beruhenden technologischen Entwicklung zu sehen. Eine wirksame Umsetzung des Grundsatzes des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen kann einen herausragenden Meilenstein auf dem Weg zu einer auf menschlichen Werten fußenden Technologiegestaltung bilden.

Zusammenfassung

In unser aller Leben und in unseren Gesellschaften spielen die Möglichkeiten und Grenzen von Technologie eine immer wichtigere Rolle. Das Maß, in dem Menschen ihre Grundrechte wahrnehmen können, hängt nicht nur von Rechtsrahmen und gesellschaftlichen Normen ab, sondern auch von den Merkmalen der ihnen zur Verfügung stehenden Technologie. Enthüllungen in jüngerer Zeit von unangemessenen Verwendungen personenbezogener Daten haben der öffentlichen Debatte über den Datenschutz einen bis dato unerreichten Schub verliehen. Es ist erforderlich, dass bei der Gestaltung und Nutzung von Technologie der Notwendigkeit, die Rechte natürlicher Personen zu wahren, Rechnung getragen wird, und nicht ausschließlich wirtschaftliche Interessen einiger Unternehmen den Ausschlag geben.

Mit der umfassenden Anwendbarkeit der Datenschutz-Grundverordnung seit dem 25. Mai 2018 ist Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen eine einklagbare rechtliche Verpflichtung geworden. Wir müssen die entstandene Dynamik erhalten, damit diese neue Verpflichtung die Wirksamkeit des von der DSGVO versprochenen Schutzes erhöhen kann. Dies wird zum Erreichen dieses Ziels beitragen, und zwar durch Sensibilisierung, Förderung der Schaffung öffentlichen Werts und gesellschaftlichen Wohlstands und durch eine Aufforderung an alle Stakeholder, sich mit Blick auf angemessene Maßnahmen in eine verantwortungsvolle Debatte einzubringen.

In dieser Stellungnahme wird zwischen dem allgemeinen Grundsatz des „Schutzes der Privatsphäre durch Technikgestaltung“ (Privacy by Design), der eine ethische Dimension umfasst, die sich an die in der EU-Charta der Grundrechte verankerten Grundsätze und Werte anlehnt, und den spezifischen rechtlichen Verpflichtungen in Artikel 25 DSGVO unterschieden, die wir als „Datenschutz durch Technikgestaltung“ (Data Protection by Design) und „Datenschutz durch datenschutzfreundliche Voreinstellungen“ (Data Protection by Default) bezeichnen.

Die Stellungnahme vermittelt einen kurzen historischen Abriss des Grundsatzes des Schutzes der Privatsphäre durch Technikgestaltung, beginnend mit ersten Forschungsarbeiten im Bereich entsprechender Technologien, bis hin zur DSGVO. Danach analysiert sie den Inhalt von Artikel 25 und dessen Beziehung zu anderen Artikeln. Ferner betrachtet sie weitere EU-Rechtsvorschriften, die sich mit Schutz der Privatsphäre durch Technikgestaltung befassen. Auch einige Beispiele aus Ländern außerhalb der EU werden vorgestellt.

In einem Überblick über den Stand der Technik schildert die Stellungnahme Beispiele von Methoden für die Identifizierung von Vorgaben für den Schutz der Privatsphäre und den Datenschutz und für deren Integration in Privacy Engineering-Verfahren zu Anwendung geeigneter technologischer und organisatorischer Garantien. Einige dieser Methoden legen Datenschutzziele unmittelbar anhand der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes fest, wie die der DSGVO, oder leiten sie aus operationellen Zwischenzielen ab. Andere Methoden hingegen stützen sich auf Risikomanagement. Im Gestaltungs- und Betriebsprozess ist der gesamte Lebenszyklus eines Dienstes oder eines Produkts zu berücksichtigen, von den Anfängen der Planung bis hin zum Ende des Dienstes bzw. der Entsorgung des Produkts. Der Überblick über die Technologie beschäftigt sich auch mit Normungsbemühungen zur Integration von Datenschutzvorgaben in das Systemdesign und mit dem Stand der Technik bei Technologien zur Erhöhung des Datenschutzes.

Es müssen Fortschritte beim Stand der Technik und beim Einsatz von Lösungen zur Erhöhung des Datenschutzes erzielt werden. Zwar wird immer intensiver geforscht und gibt es

zunehmend Initiativen zur Weiterentwicklung der Fachrichtung „Privacy Engineering“, doch reicht dies noch nicht aus, um den Schutz natürlicher Personen und ihrer personenbezogenen Daten tatsächlich wirksamer zu machen. Entscheiden sich Organisationen für den Ansatz des Schutzes der Privatsphäre durch Technikgestaltung, ergeben sich für sie nur Vorteile. Politische Maßnahmen zur Förderung von Technologien und Strategien zum Schutz der Privatsphäre sollten auf der Agenda der EU ganz oben stehen, und öffentliche Verwaltungen müssen hier mit gutem Beispiel vorangehen. Die IPEN-Initiative bietet eine gute Gelegenheit, bei Stakeholdern auf internationaler Ebene Werbung für Technologien zum Schutz der Privatsphäre zu machen.

Initiativen für den Schutz der Privatsphäre durch Technikgestaltung sollten im größeren Zusammenhang der Integration ethischer Erwägungen in technisches Design gesehen werden, wie es in den Schlussfolgerungen des jüngst vorgelegten Berichts des Ethik-Beirats des EDSB heißt.

In der vorliegenden Stellungnahme formuliert der EDSB eine Reihe von Empfehlungen für EU-Organe:

- Gewährleistung eines starken Schutzes der Privatsphäre, auch durch Technikgestaltung, in der E-Privacy-Verordnung,
- Unterstützung des Schutzes des Privatsphäre in allen Regelwerken, die Einfluss auf das Design von Technologie haben, durch verstärkte Anreize und entsprechende Pflichten, einschließlich angemessener Haftungsvorschriften,
- Förderung der Einführung und Anwendung von Konzepten für den Schutz der Privatsphäre durch Technikgestaltung und von Technologien zum Schutz der Privatsphäre in der EU und auf Ebene der Mitgliedstaaten durch angemessene Durchführungsmaßnahmen und politische Initiativen,
- Gewährleistung von Sachverstand und Ressourcen für Forschung und Analysen im Bereich Privacy Engineering und Technologien zum Schutz der Privatsphäre auf EU-Ebene durch ENISA oder andere Einrichtungen,
- Unterstützung der Entwicklung neuer Vorgehensweisen und Geschäftsmodelle mit Hilfe der EU-Instrumente für Forschung und technologische Entwicklung,
- Unterstützung der EU-Verwaltung und nationaler öffentlicher Verwaltungen bei der Integration angemessener Vorgaben für den Schutz der Privatsphäre durch Technikgestaltung in das öffentliche Beschaffungswesen,
- Unterstützung einer Bestandsaufnahme und einer Beobachtungsstelle des „Stands der Technik“ bei Privacy Engineering und PET sowie ihrer Fortschritte.

Der EDSB wird

- sich weiterhin für eingebauten Datenschutz einsetzen, gegebenenfalls in Zusammenarbeit mit anderen Datenschutzbehörden im Europäischen Datenschutzausschuss (EDSA),
- die koordinierte und wirksame Durchsetzung von Artikel 25 DSGVO und damit zusammenhängender Bestimmungen unterstützen,

- für die Verarbeitung Verantwortlichen Hilfestellung bei der korrekten Umsetzung des in der Rechtsgrundlage niedergelegten Grundsatzes anbieten und

- zusammen mit den Datenschutzbehörden von Österreich, Irland und Schleswig-Holstein einen Wettbewerb für datenschutzfreundliche mobile Apps im Gesundheitsbereich ins Leben rufen.

Koordinierung und gemeinsame Anstrengungen des technologischen Sachverstands der Datenschutzbehörden sind für die Förderung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen wesentlich. Erforderlich ist ferner die Zusammenarbeit innerhalb des EDSA sowie in der International Working Group on Data Protection and Telecommunications (IWGDPT, „Berlin-Gruppe“).

Wir freuen uns auf Rückmeldungen zu dieser vorläufigen Stellungnahme.

Die Internationale Konferenz der Datenschutzbeauftragten 2018 wird ein Meilenstein in der Debatte über digitale Ethik im Allgemeinen sein und die Möglichkeit bieten, den weiteren Weg für den Schutz der Privatsphäre durch Technikgestaltung besser abzustecken.

INHALTSVERZEICHNIS

1. Schutz der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen - eine Chance für einen wirksameren Schutz natürlicher Personen

1.1 Warum eine Stellungnahme zu „Schutz der Privatsphäre durch Technikgestaltung“

1. Zu Beginn des Jahres 2018 erreicht die öffentliche Debatte über die Verarbeitung personenbezogener Daten mit ausgefeilter Informations- und Kommunikationstechnologie ein bis dato nie gekanntes Maß an Aufmerksamkeit. Parlamentsausschüsse führen Untersuchungen durch oder erwägen sie, und zwar im Europäischen Parlament[1], im US-Kongress[2] und in nationalen Parlamenten von EU-Mitgliedstaaten wie dem Vereinigten Königreich[3], Deutschland[4] und Frankreich[5]. Abgeordnete dieser Parlamente sowie die breite Öffentlichkeit [6] wollen Klarheit darüber, wie ihre personenbezogenen Daten verarbeitet und bei der Verfolgung der Webaktivitäten der Bürger und der Verarbeitung der erhobenen personenbezogenen Daten verwendet werden. Bei diesen Untersuchungen spielen Anhörungen von Vorstandsvorsitzenden von Technologieunternehmen eine Hauptrolle.

2. Trotz des gewaltigen Medieninteresses nimmt die Öffentlichkeit im Hinblick auf Tracking und Targeting noch immer nur die „Spitze des Eisbergs“[7] wahr. Der EDSB hat in einer jüngst vorgelegten Stellungnahme[8] die Nutzung personenbezogener Daten für Online-Manipulation analysiert und Empfehlungen zur Durchsetzung des Datenschutzrechts, zu gemeinsamen Analysen und zur Zusammenarbeit zwischen Regulierern über die Branchengrenzen hinweg, zu Selbstregulierung und zur Stärkung der Eigenverantwortung des Einzelnen formuliert. In der Stellungnahme heißt es ferner, durch die jüngsten Enthüllungen wird die Bedeutung der Tatsache unterstrichen, dass Technologien so zu gestalten sind, dass die praxistaugliche und wirksame Wahrnehmung von Grundrechten gefördert und nicht ausschließlich auf die wirtschaftlichen Interessen von Unternehmen Rücksicht genommen wird.

3. Die vorliegende Stellungnahme baut auf vielen Jahren der Arbeit von Experten für Privatsphäre und Technologie zu der Rolle technologischen Designs auf, durch das das Grundrecht auf Schutz der Privatsphäre garantiert wird. Sie nimmt eine Bestandsaufnahme der rechtlichen und technologischen Entwicklungen weltweit vor und formuliert Empfehlungen für Maßnahmen, die Fortschritte beim Schutz der Privatsphäre und beim Datenschutz durch Technikgestaltung bringen sollen. Auch wenn die Beobachtungen zu Online-Manipulation die Dringlichkeit eines neuen Ansatzes bei der Gestaltung von Technologie deutlich vor Augen führen, und auch wenn die im Internet eingesetzten Systeme eine zentrale Rolle spielen, gilt doch für alle Instrumente der Datenverarbeitung, dass die Grundrechte bei der technologischen Entwicklung berücksichtigt werden müssen, und dies unabhängig von den verwendeten Plattformen und Anwendungsbereichen.

„Schutz der Privatsphäre durch Technikgestaltung“ oder „Datenschutz durch Technikgestaltung“

4. Für die Zwecke dieser Stellungnahme verwenden wir den Begriff „Schutz der Privatsphäre durch Technikgestaltung“ zur Bezeichnung des breit angelegten Konzepts technologischer

Maßnahmen zur Gewährleistung der Privatsphäre, wie es sich im Verlauf der letzten Jahrzehnte in der internationalen Debatte herausgebildet hat. Die Begriffe „Datenschutz durch Technikgestaltung“ und „Datenschutz durch datenschutzfreundliche Voreinstellungen“ verwenden wir hingegen für die konkreten rechtlichen Verpflichtungen, festgelegt in Artikel 25 DSGVO [9]. Zwar dürften auch aufgrund dieser Verpflichtungen ergriffene Maßnahmen dazu beitragen, dass das eher allgemeine Ziel des „Schutzes der Privatsphäre durch Technikgestaltung“ erreicht wird, doch sind wir der Auffassung, dass bezüglich des Ziels „Schutz der Privatsphäre durch Technikgestaltung“ ein breiteres Spektrum von Ansätzen berücksichtigt werden könnte, denn es umfasst ja, im Einklang mit den in der Charta der Grundrechte der EU verankerten Grundsätzen und Werten, auch eine visionäre und ethische Dimension.

Formt die Technologie die Gesellschaft oder formt die Gesellschaft die Technologie?

5. Seitdem der Mensch die ersten Werkzeuge erfunden hat, ist Technologie mit der Entwicklung der Menschheit verknüpft. Technologischer Fortschritt hat sich stets stark auf die Entwicklung von Gesellschaften ausgewirkt, häufig zu deren Vorteil, mitunter zu deren Nachteil. Auch die Regeln, nach denen unsere Gesellschaften leben, und zwar sowohl verbindliche Gesetze als auch gesellschaftliche Normen, werden stark durch die Technologie beeinflusst. Der Datenschutz ist ein gutes Beispiel für diese Wechselwirkung, da die Geburt dieses Rechtsbegriffs zunächst auf die Entwicklung und wachsende Beliebtheit von Computern und in jüngerer Zeit des Internets zurückzuführen ist. Die geradezu programmatischen Worte in Erwägungsgrund 2 der Datenschutzrichtlinie[10] (*„Die Datenverarbeitungssysteme stehen im Dienste des Menschen“*) und in Erwägungsgrund 4 der DSGVO (*„Die Verarbeitung personenbezogene Daten sollte im Dienste der Menschheit stehen“*) verdeutlichen diesen Aspekt ganz klar. Das Beispiel Datenschutz zeigt, wie komplex die Interaktion zwischen Technologie und Vorschriften ist: Das Konzept des Datenschutzes wurde als Reaktion auf den zunehmenden Einsatz von Computern in Behörden und Unternehmen entwickelt; es bedurfte mehrerer Jahrzehnte, bis die Verpflichtung zur Integration von Datenschutzgarantien in die Gestaltung von Technologie ausdrücklich im Gesetz verankert wurde.

6. Im Jahr 1989 setzten zwei Entwicklungen einen Wandel in Gang, an dessen Ende das Internet zu der dominanten Kommunikationsinfrastruktur wurde, die es heute ist. In den ersten 20 Jahren seiner Existenz war das Internet hauptsächlich von zivilen und militärischen Forschungs- und Wissenschaftseinrichtungen eingesetzt worden; für die öffentliche kommerzielle Nutzung wurde es durch seinen Anschluss an bestehende E-Mail-Dienste geöffnet. Im gleichen Jahr wurde mit dem Vorschlag von Sir Tim Berners-Lee für ein verteiltes Hypertext-System, das Links und Universal Resource Locators (URL) verwendet, das Fundament für das World Wide Web mit seinem anscheinend unbegrenzten Potenzial gelegt, Informationen zu organisieren und sie weltweit zur Verfügung zu stellen.

7. In den vergangenen 29 Jahren wurden sowohl das Internet als auch das World Wide Web ständig weiterentwickelt und geändert, und beide wachsen nach wie vor bei Größe, Kapazität und Fähigkeiten. Cookies, Skript-Sprachen, komprimierte audio-visuelle Formate, Suchmaschinen, Streaming-Protokolle, Social Media-Plattformen, intelligente mobile Geräte, Tracking-, Analyse- und Profiling-Tools haben neue Möglichkeiten der Verwendung und der Unternehmensführung ermöglicht. Zwar liegen viele Vorteile auf der Hand, doch werden zunehmend Bedenken bezüglich ihrer Auswirkung auf Grundrechte und auf das eigentliche Fundament und die Funktionsweise demokratischer Gesellschaften geäußert. Der Verlust der Kontrolle über personenbezogene Daten, die Verbreitung von

Fake News und gezielter politischer Werbung auf der Grundlage der Analyse und Auswertung personenbezogener Daten sind nur einige der jüngst identifizierten Herausforderungen.[11] 2018 stellte Sir Tim Berners-Lee in seiner Ansprache zum Jahrestag der Gründung des WWW fest, dass mehr als die Hälfte der Weltbevölkerung Zugang zum WWW hat, dass aber das Web derzeit von einigen wenigen mächtigen Plattform-Unternehmen kontrolliert wird, die aufgrund ihrer Macht entscheiden können, welche Ideen und Innovationen weiterverfolgt werden, und dabei einem Großteil der Weltbevölkerung ein Mitspracherecht bei seiner weiteren Entwicklung verweigern, und gleichzeitig Werbung für die Hauptantriebskraft des Web machen.[12]

8. Derweilen sich unsere Parlamente und unsere Gesellschaften noch überlegen, wie sie mit diesen Herausforderungen umgehen sollen, dürften neue technologische Entwicklungen noch größere und tiefer greifende Veränderungen in der Kommunikation zwischen Menschen und in der sozialen Interaktion hervorrufen. Bei der Verarbeitung riesiger Informationsmengen, Big Data, ist ein kontinuierliches Wachstum zu beobachten. Das Internet der Dinge steckt noch in den Kinderschuhen, und die Zahl verbundener Geräte dürfte sich zumindest um ein Vielfaches erhöhen, die nicht nur in Wohnungen und Städten, sondern auch im menschlichen Körper immer weiter um sich greifen.[13] Die Entwicklung der künstlichen Intelligenz fängt gerade an, sich von kleinen spezialisierten Bereichen hin zur Anwendung in größerem Umfang zu bewegen. Die Blockchain-Technologie soll in großem Maßstab eingesetzt werden, auch für die Verarbeitung personenbezogener Daten. Unternehmerische und technische Entscheidungen über die künftige Entwicklung dieser Technologien, die heute getroffen werden, dürften sich noch lange auf uns und unsere Nachkommen auswirken.

9. Wir haben ein Beispiel einer erfolgreichen Bemühung gefunden, Technologie im Einklang mit gesellschaftlichen Zielsetzungen bezüglich der Nachhaltigkeitsgrundsätze zu gestalten, die in den vergangenen Jahrzehnten für den Erhalt der natürlichen Ressourcen formuliert wurden.[14] Denn im Umweltrecht muss Technologie während ihres gesamten Lebenszyklus auf eine Weise gestaltet und eingesetzt werden, die mit den Grundrechten und Werten vereinbar ist, die unsere demokratischen Gesellschaften prägen. Diese Erfahrung schafft Zuversicht dahingehend, dass es möglich ist, Technologie zum Vorteil der Menschen zu kontrollieren. Nachforschungen in der Geschichte der Technologie haben ergeben, dass *„Technologie weder gut noch schlecht noch neutral ist“*[15], dass ihre Entwicklung keinem inhärenten Determinismus unterworfen ist und dass sie gestaltet werden kann: *„Auch wenn Technologie in vielen öffentlichen Angelegenheiten vielleicht ein wichtiges Element ist, haben in technologiepolitischen Entscheidungen doch nicht technische Faktoren Vorrang“*.[16] Der EDSB hat sich in den vergangenen Jahren im Rahmen der Arbeiten des 2015 eingerichteten Ethik-Beirats[17] intensiv mit einer Analyse weiterreichender ethischer Forderungen befasst.

10. Die EU hat spezifische Vorschriften bezüglich der Gestaltung technologischer Lösungen erlassen, wenn eine Verarbeitung personenbezogener Daten stattfindet. Seit dem 25. Mai 2018, seit also die DSGVO[18] vollumfänglich anzuwenden ist, sind Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen nicht länger lediglich ein Wunsch oder eine empfohlene bewährte Vorgehensweise, sondern eine gesetzliche und durchsetzbare Verpflichtung, der alle, die nach EU-Recht personenbezogenen Daten verarbeiten, nachzukommen haben. Wir müssen die entstandene Dynamik erhalten, damit diese neue Verpflichtung Gestalt annehmen und die Wirksamkeit des von der DSGVO verheißenen Schutzes erhöhen kann und nicht zu eng ausgelegt wird.

11. Der EDSB möchte mit dieser Stellungnahme zu diesem Prozess beitragen, und zwar durch Sensibilisierung und Förderung der Schaffung öffentlichen Werts und gesellschaftlichen Wohlstands, und er fordert die einschlägigen Stakeholder (politische Entscheidungsträger der EU und auf nationaler Ebene, Datenschutz- und andere Regulierer, die Wissenschaft, Technologieanbieter, private und öffentliche für die Verarbeitung personenbezogener Daten verantwortliche Organisationen und natürliche Personen, deren Daten verarbeitet werden) auf, sich in eine verantwortungsvolle Debatte einzubringen, damit die richtigen Entscheidungen getroffen werden, bei denen nicht nur Fortschritte der Technologie und deren endlose Fähigkeiten berücksichtigt werden, sondern auch die betroffenen Grundrechte, darunter das Recht auf Privatsphäre und auf den Schutz personenbezogener Daten.

12. Auch wenn Artikel 25 DSGVO einen wichtigen Meilenstein in dem Bemühen darstellt, eine verantwortungsbewusste Gestaltung und Nutzung von Technologie zu erreichen, und auch wenn die Art der Umsetzung und Durchsetzung dieses neuen Rechtsgrundsatzes entscheidend für den Erfolg des gesamten neuen Datenschutzregelwerks sein wird, wird in dieser Stellungnahme weder eine umfassende rechtliche Analyse von Artikel 25 DSGVO[19] vorgenommen noch enthält sie eine schrittweise Anleitung[20] für Organisationen für die Einhaltung von Artikel 25. Sie hebt vielmehr auf die Herausarbeitung wesentlicher Elemente ab, die das Verständnis des Hauptgrundsatzes und seiner Folgen für alle betroffenen Stakeholder erleichtern und möchte in verständlicher Sprache klare Botschaften vermitteln und so eine ergiebige Diskussion fördern. Es kann davon ausgegangen werden, dass Aufsichtsbehörden und EDSA detaillierte Leitlinien zu Artikel 25 herausgeben werden.

1.2 Geschichtedes Schutzes der Privatsphäre durch Technikgestaltung

13. In der Vergangenheit wurden Privatsphäre und Datenschutz von vielen Organisationen als ein Thema wahrgenommen, das hauptsächlich mit der Einhaltung von Rechtsvorschriften zu tun hatte, häufig begrenzt auf den rein formalen Prozess der Veröffentlichung langer Datenschutzerklärungen, in denen auf alle denkbaren Eventualitäten eingegangen und auf Zwischenfälle reagiert wurde, um den Schaden für die eigenen Interessen möglichst klein zu halten. Anders ausgedrückt: Für viele Organisationen war Datenschutz reine Augenwischerei mit sehr geringen Auswirkungen auf die Zielsetzungen oder Vorgehensweisen der Organisationen beim Schutz der betroffenen natürlichen Personen.

14. Die **Schwierigkeit, Rechtsgrundsätze in einklagbare Anforderungen zu übersetzen**, und die Notwendigkeit eines wirklich interdisziplinären Ansatzes[21] für den Umgang mit Fragen des Schutzes der Privatsphäre haben dazu beigetragen, die Kluft zwischen einer von Anwälten beherrschten Fachrichtung der Einhaltung von Rechtsvorschriften einerseits und einem von Unternehmensmanagern und Ingenieuren getragenen dynamischen Innovationsprozess andererseits, die letztendlich für die Gestaltung und Umsetzung von Prozessen und Systemen verantwortlich sind, die das eigentliche Funktionieren der Organisation lenken, zu vergrößern.

15. Vor diesem Hintergrund kam der Gedanke, dass die Entwicklung der Technologie nicht nur die Ursache für wachsende Bedenken hinsichtlich des Schutzes der Privatsphäre, sondern auch Teil der Lösung ist, erst im Zuge der Kodifizierung von Grundsätzen des Schutzes der Privatsphäre in Form von Best Practices und Gesetzen auf, also Ende der 1970er Jahre. Im Rahmen ihrer Arbeiten führten David Chaum und andere[22] erste Technologieforschungen

durch, die mit Beiträgen zu Datenminimierung, anonymen Transaktionen und Kommunikationsvorgängen sowie Technologien für den Schutz der Privatsphäre in Statistiken eindeutig auf das Ausräumen von Bedenken hinsichtlich des Schutzes der Privatsphäre abhoben. Verbesserungen in Kommunikationstechnologie, IT-Sicherheit (einschließlich konzeptioneller Rahmen, die dem Endnutzer von IKT-Systemen mehr Selbstbestimmung in Fragen von Privatsphäre und Sicherheit verleihen sollen[23]), anonymer Kommunikation und Kryptographie bereiteten der Entwicklung der so genannten Technologien zum Schutz der Privatsphäre (Privacy Enhancing Technologies (PET))[24] den Weg, einer Familie technologischer Lösungen, mit denen die Risiken für die Privatsphäre natürlicher Personen klein gehalten werden sollen.

16. Allerdings gehörten weder Sicherheit noch Schutz der Privatsphäre wirklich zu den primären Vorgaben bei der Entwicklung und Expansion von Internet und WWW; Vorrang hatten vielmehr Funktionalität, Skalierbarkeit und Offenheit. Nach den Enthüllungen über Programme zur Massenüberwachung durch nationale Sicherheitsbehörden im Jahr 2013[25] gab die Internet Engineering Task Force (IETF)[26] eine Erklärung ab[27] , in der es heißt: *„Es überrascht das Ausmaß der kürzlich ans Licht gekommenen Überwachung. Bei der Gestaltung vieler Internetprotokolle war ein solches Ausmaß nicht geplant...".* Den Anstoß zu Arbeiten in Richtung stärkerer Integration des Schutzes der Privatsphäre in Internetprotokolle gab dann die Tagung der IETF in Vancouver im Jahr 2013.

17. Der Begriff „Schutz der Privatsphäre durch Technikgestaltung" geht ursprünglich auf Ann Cavoukian in ihrer Zeit als Datenschutzbeauftragte von Ontario, Kanada, zurück. Ihr Konzept besagt, dass sich der Schutz der Privatsphäre durch Technikgestaltung in „sieben Grundprinzipien "[28] unterteilen lässt, und es unterstreicht die Notwendigkeit, bei der Prüfung der Anforderungen an den Schutz der Privatsphäre vom Beginn der Designphase an während des gesamten Lebenszyklus der Daten proaktiv vorzugehen, damit *„er in das Design und die Architektur von IT-Systemen und Geschäftspraktiken eingebettet ist, ...ohne dass die Funktionalität beeinträchtigt wird ..."*, wobei datenschutzfreundliche Voreinstellungen gewählt werden sollten, End-to-End-Sicherheit einschließlich sichererer Datenvernichtung und ausgeprägte Transparenz, die von unabhängiger Seite überprüft wird. Der Grundsatz des Schutzes der Privatsphäre durch datenschutzfreundliche Voreinstellungen ging ein als das zweite der Grundprinzipien; er besagt, dass Schutz der Privatsphäre durch Technikgestaltung *„dafür sorgt, dass personenbezogene Daten automatisch in allen IT-Systemen oder Geschäftspraktiken geschützt werden. Tut eine Person nichts, bleibt ihre Privatsphäre weiterhin geschützt. Die Person muss nichts unternehmen, damit ihre Privatsphäre geschützt wird - dieser Schutz ist als Voreinstellung in das System eingebaut"*. Diese Erklärung ist eine kraftvolle operationelle Definition des Grundsatzes des Schutzes der Privatsphäre durch datenschutzfreundliche Voreinstellungen, bei der die Person nicht damit belastet wird, sich bei der Nutzung eines Dienstes oder Produkts um Schutz zu bemühen, sondern „automatisch" (ohne eigenes Aktivwerden) das Grundrecht auf Privatsphäre und den Schutz personenbezogener Daten genießen kann.

18. Einige Elemente des Schutzes der Privatsphäre durch Technikgestaltung sind bereits in der Datenschutzrichtlinie 95/46/EG[29] (nachstehend „die Richtlinie") zu finden, die durch die DSGVO aufgehoben wurde. In Erwägungsgrund 46 der Richtlinie wird unterstrichen, wie die für den Schutz der Rechte und Freiheiten der Personen, deren Daten verarbeitet werden, zu ergreifenden technischen und organisatorischen Maßnahmen zu gelten haben, *nämlich„sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung ...".*

19. Die „Resolution on Privacy by Design“, angenommen von der 32. Konferenz der Datenschutzbeauftragten im Oktober 2010[30], stellt einen Meilenstein bei der Anerkennung des Grundsatzes als *„wesentlichem Bestandteil des grundlegenden Schutzes der Privatsphäre dar“*. Die Konferenz forderte Datenschutzbehörden auf, sich für Schutz der Privatsphäre durch Technikgestaltung in der *„Formulierung von politischen Maßnahmen und Rechtsvorschriften in ihren jeweiligen Zuständigkeitsbereichen“* einzusetzen.

20. In ihrer Antwort auf die öffentliche Konsultation der Europäischen Kommission zur Datenschutzreform forderte die Artikel 29-Datenschutzgruppe[31] mit folgenden Ausführungen die Einführung des Grundsatzes des Schutzes der Privatsphäre durch Technikgestaltung in den neuen Rechtsrahmen: *„Die vorstehend genannten Bestimmungen der Richtlinie helfen zwar bei der Förderung des Schutzes der Privatsphäre durch Technikgestaltung, doch haben sie in der Praxis nicht ausgereicht, um dafür zu sorgen, dass der Schutz der Privatsphäre in die IKT eingebettet wird“*; ferner forderte sie *„Schutz der Privatsphäre durch Standardeinstellungen“*. Weiter empfahl die Artikel 29-Datenschutzgruppe Folgendes: *„Dieser Grundsatz sollte für Designer und Hersteller von Technologie sowie für die für die Verarbeitung Verantwortlichen verbindlich sein... Sie sollten dazu verpflichtet sein, einen technologischen Datenschutz bereits in der Phase der Planung von informationstechnologischen Verfahren und Systemen zu berücksichtigen“.*

21. In seiner „Stellungnahme zur Stärkung des Vertrauens in die Informationsgesellschaft durch die Förderung des Schutzes von Daten und Privatsphäre vom März 2010“[32] befürwortete der EDSB ganz und gar den Grundsatz des Schutzes der Privatsphäre durch Technikgestaltung als Schlüsselinstrument für eine Stärkung des Vertrauens in Informationstechnologie und nahm eine umfassende Analyse vor, an deren Ende konkrete Empfehlungen standen. Wir gingen darauf ein, wie der Grundsatz in das allgemeine und sektorielle Recht zum Schutz personenbezogener Daten (darunter soziale Netzwerke, Internet der Dinge, RFID-Geräte und Browser) hätte eingebettet werden sollen. Des Weiteren formulierten wir Empfehlungen zur Förderung der Umsetzung des Grundsatzes in IT-Produkten und -Dienstleistungen, nachdem wir eingeräumt hatten, dass PET sich auf dem Markt nicht hatten durchsetzen können, und die in Frage kommenden Gründe hierfür analysiert hatten, darunter fehlende wirtschaftliche Anreize, fehlende institutionelle Unterstützung und unzureichende Nachfrage seitens der Nutzer.

22. Zwar hat der Schutz der Privatsphäre durch Technikgestaltung erhebliche Fortschritte in rechtlicher, technologischer und konzeptioneller Hinsicht gemacht, doch ist er noch weit davon entfernt, sein Potenzial für den Schutz der Grundrechte natürlicher Personen voll ausschöpfen zu können. Die folgenden Abschnitt dieser Stellungnahme bieten einen Überblick über die relevanten Entwicklungen und empfehlen weitere Anstrengungen.

2. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen im EU-Recht

2.1 Artikel 25 DSGVO

23. Artikel 25[33] DSGVO mit dem Titel „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ [34] sieht vor, dass der Verantwortliche[35] sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen trifft, um die Datenschutzgarantien wirksam aufzunehmen, um der Verordnung Genüge zu tun und

die Rechte der natürlichen Personen zu schützen, deren Daten verarbeitet werden. Diese Maßnahmen werden unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen ermittelt. In dem Artikel heißt es, dass nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden dürfen. Abschließend besagt der Artikel, dass ein genehmigtes Zertifizierungsverfahren herangezogen werden kann, um die Erfüllung der Anforderungen nachzuweisen.[36].

24. Das Erfordernis des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen von Artikel 25 ist eine Ergänzung der in Artikel 24, einer Kernbestimmung der DSGVO, geregelten Verantwortung des für die Verarbeitung Verantwortlichen. In diesem Artikel ist festgelegt, „wer was macht", um natürliche Personen und ihre personenbezogenen Daten zu schützen, und besagt, dass mit einem risikobasierten Ansatz ermittelt werden muss, was zu diesem Zweck unternommen werden muss. Genauer gesagt verlangt er von den Verantwortlichen *„die Umsetzung technischer und organisatorischer Maßnahmen zur Gewährleistung und zum Nachweis, dass die Verarbeitung in Übereinstimmung mit dem Gesetz erfolgt"*. Diese Maßnahmen werden *„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 Risiken für die Rechte und Freiheiten natürlicher Personen"* konzipiert..

25. Diese umfassen auch die Vorschriften von Artikel 32, dem zufolge ein IT-Sicherheitsmanagementrahmen sowie Maßnahmen erforderlich sind, um durch eine angemessene Datensicherung die Risiken für die natürlichen Personen zu mindern, deren Daten verarbeitet werden. Es sei an dieser Stelle nochmals darauf hingewiesen, dass die in Artikel 32 aufgeführten Maßnahmen auf gerade mal einen der in Artikel 5[37] genannten Grundsätze des Datenschutzes abheben, nämlich „Integrität und Vertraulichkeit", Artikel 24 aber von der Umsetzung aller Datenschutzgrundsätze und der Einhaltung der DSGVO insgesamt spricht.

26. Vor dem Hintergrund der Verantwortung des für die Verarbeitung Verantwortlichen, die Einhaltung der Verordnung sicherzustellen und nachzuweisen, zielt Artikel 25 auf die in Artikel 24 erwähnten technischen und organisatorischen Maßnahmen ab, unterstreicht einige Dimensionen ihrer Durchführung, die implizit bereits in Artikel 24 vorhanden sind, fügt weitere hinzu und macht sie alle verbindlich. Auf diese Dimensionen gehen wir in den folgenden Abschnitten ein.

Die verschiedenen Dimensionen der Verpflichtung zum Datenschutz durch Technikgestaltung

27. Die erste Dimension ist die Anerkennung der Tatsache, dass die Verarbeitung personenbezogener Daten, teilweise oder ganz durch IT-Systeme gestützt, stets das **Ergebnis eines Gestaltungsprojekts** sein sollte. Artikel 25 verlangt Garantien[38] sowohl in der Gestaltungs- als auch in der operationellen Phase, **zielt damit auf den gesamten Lebenszyklus des Projekts ab**[39] und zählt eindeutig den **Schutz natürlicher Personen und ihrer personenbezogenen Daten zu den Vorgaben des Projekts**.

28. Die zweite Dimension ist der **Risikomanagementansatz** zur Auswahl und Umsetzung von **Maßnahmen** für einen wirksamen Schutz. Die **Werte, die es zu schützen gilt, sind die**

natürlichen Personen, deren Daten verarbeitet werden, und hier insbesondere ihre Grundrechte und Grundfreiheiten.[40] Diesbezüglich werden keine obligatorischen Maßnahmen erwähnt.[41] Der Gesetzgeber nennt jedoch Anhaltspunkte zu diesen Faktoren (Art, Umfang, Umstände und Zwecke der Verarbeitung), die die Organisation bei der Wahl der geeigneten Maßnahmen zu berücksichtigen hat.

29. Gleichzeitig ist die Organisation dafür verantwortlich, unter den verfügbaren Garantien ihre auszuwählen (unter Berücksichtigung des „Stands der Technik") und ihre Implementierungskosten unter den Elementen zu berücksichtigen, die letztendlich zur Entscheidung führen, die mit den Risiken für natürliche Personen abgewogen werden müssen. Diese beiden Faktoren, also der Stand der Technik der verfügbaren Technologie und die Implementierungskosten der Maßnahmen, dürfen nicht so gedeutet werden, dass die ausgewählten Maßnahmen bestehende Risiken nicht in ausreichendem Maße mindern und der aus ihnen resultierende Schutz nicht angemessen ist.

30. Die dritte Dimension ist die Notwendigkeit, dass diese **Maßnahmen geeignet und wirksam sein müssen**. Die Wirksamkeit ist am Zweck dieser Maßnahmen zu messen: Es muss sichergestellt und nachgewiesen werden, dass der Verordnung Genüge getan wird; es müssen die Grundsätze des Datenschutzes angewandt und die Rechte natürlicher Personen geschützt werden, deren Daten verarbeitet werden. Artikel 25 bestimmt für diese Maßnahmen insbesondere, dass sie dafür ausgelegt sein müssen, *„die Datenschutzgrundsätze ... wirksam umzusetzen"*. Diese in Artikel 5 aufgeführten Grundsätze des Datenschutzes können als die **zu erreichenden Ziele** gelten. Sie wurden vom Gesetzgeber als Grundpfeiler des Schutzes natürlicher Personen bei der Verarbeitung ihrer Daten ausgewählt und werden in der DSGVO ergänzt, entweder durch detailliertere Vorschriften (also die Informationspflicht gegenüber natürlichen Personen und deren Rechte als „betroffene Personen"[42], die im Zusammenhang mit dem Grundsatz der „Transparenz" näher ausgeführt werden, oder die Verpflichtungen betreffend die Sicherheit in Artikel 32), oder durch andere der Rechenschaft dienenden Instrumente, wie die Dokumentationspflichten von Artikel 30, die diesen Grundsätzen dienlich sind. Das bedeutet, dass eine wirksame Wahrung dieser Grundsätze/Ziele, wie im Rechtstext mit anderen Bestimmungen ausgeführt, den erwarteten Schutz personenbezogener Daten gewährleisten würde.

31. Die vierte Dimension ist die Verpflichtung zur **Integration der ermittelten Garantien in die Verarbeitung.** In der DSGVO finden sich einige Garantien für den Schutz natürlicher Personen, deren Daten verarbeitet werden, durch Mittel, die „außerhalb" der eigentlichen Verarbeitung stehen, wie beispielsweise Datenschutzhinweise. Bei dieser Dimension geht es jedoch eher um die Notwendigkeit, die natürlichen Personen direkt durch den Schutz ihrer Daten und den Umgang mit ihnen zu schützen.

32. Alle vier Dimensionen sind gleichermaßen wichtig und werden Bestandteil der Rechenschaftspflicht und unterliegen gegebenenfalls der Aufsicht durch die zuständige Datenschutzbehörde.

Die Verpflichtung zum Datenschutz durch datenschutzfreundliche Voreinstellungen

33. In Anwendung des Grundsatzes des Datenschutzes durch Technikgestaltung dürfen Organisationen standardmäßig nur personenbezogene Daten verarbeiten, die für den jeweils im Einklang mit dem Gesetz festgelegten konkreten Zweck erforderlich sind und den betreffenden Personen auf transparente Weise kommuniziert werden. Zwar könnte hier das

Argument angebracht werden, dass diese Verpflichtung implizit bereits in den Grundsätzen der „Zweckbindung“ und der „Datenminimierung“[43] sowohl in der Gestaltungs- als auch in der Betriebsphase[44] enthalten ist, doch betont die Vorschrift ausdrücklich, wie wichtig es ist, dass technische Maßnahmen ergriffen werden, damit die Erwartungen der natürlichen Personen erfüllt werden, deren Daten verarbeitet werden, dass ihre Daten nicht für andere Zwecke verarbeitet werden, als für das Produkt oder die Dienstleistung unbedingt erforderlich ist, wobei standardmäßig die Möglichkeit besteht, jede weitere Verwendung zu unterbinden, beispielsweise über Einstellungen bei der Konfiguration.[45]

34. Ein gewisser Mehrwert der Bestimmung über Datenschutz durch datenschutzfreundliche Voreinstellungen liegt ferner in der Tatsache, dass näher auf den Grundsatz der Datenminimierung eingegangen wird, und in der Erweiterung auf den Grundsatz der Speicherbegrenzung. In Artikel 25 Absatz 2 wird erklärt, wie die Verpflichtung, standardmäßig nur personenbezogene Daten zu verarbeiten, die erforderlich sind, *„für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit...“* gilt. Dann sieht der Artikel eine präzise Verpflichtung vor, indem er den allgemeinen Grundsatz in einem bestimmten Nutzungsfall instanziiert: Organisationen treffen Maßnahmen, mit denen verhindert wird, dass personenbezogene Daten standardmäßig öffentlich zugänglich gemacht werden.

Die Rolle von „Auftragsverarbeitern“ und einschlägige Pflichten von für die Verarbeitung Verantwortlichen

35. Anbieter von Diensten für eine Organisation, die personenbezogene Daten im Auftrag der Organisation verarbeiten, gelten in der DSGVO als „Auftragsverarbeiter“.[46] Die Organisation/der Verantwortliche ist verpflichtet, Auftragnehmer/Auftragsverarbeiter auszuwählen, die in der Lage sind, sie/ihn bei der Einhaltung des Gesetzes[47] und somit auch bei der Erfüllung ihrer/seiner Pflichten beim Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu unterstützen.

36. Damit sind diese Auftragsverarbeiter indirekt verpflichtet, Prozesse und Technologie so zu gestalten und zu nutzen, dass die verantwortliche Organisation in der Lage ist, die natürlichen Personen und ihre Daten nach dem Ansatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu schützen.

Artikel 25 und Entwickler von Produkten und Technologie

37. Eine schwerwiegende Einschränkung der Pflichten gemäß Artikel 25 ist darin zu sehen, dass diese nur für die für die Verarbeitung Verantwortlichen gelten, nicht hingegen für die Entwickler dieser Produkte und Technologien, die zur Verarbeitung personenbezogener eingesetzt werden. Im verfügenden Teil der DSGVO findet sich keine Verpflichtung für Anbieter von Produkten und Technologie. In Erwägungsgrund[48] 78 heißt es jedoch: *„Mit Blick auf die Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die auf der Verarbeitung personenbezogener Daten beruhen oder die zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller bzw. Anbieter dieser Produkte, Anwendungen und Dienste dazu ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung von Produkten, Diensten 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...“*. Die Anwendung von Artikel 25 würde also vom Anbieter verlangen, seine Produkte so zu gestalten, dass der Verantwortliche in der

Lage ist, alle erforderlichen Maßnahmen zu ergreifen, die erforderlich sind, um die Personen und ihre Daten zu schützen, und sie so zu konfigurieren, dass standardmäßig, ohne jegliches Eingreifen des Nutzers, gar keine personenbezogenen Daten oder zumindest nur die erhoben werden, die unbedingt erforderlich sind, um das vornehmen zu können, was von der Grundnutzung dieses Produkts erwartet werden kann.

Artikel 25 und öffentliche Verwaltungen

38. Artikel 25 gilt für alle Arten von Organisationen, die als für die Verarbeitung Verantwortliche auftreten, darunter öffentliche Verwaltungen, die in Anbetracht ihrer Aufgabe, dem öffentlichen Wohl zu dienen, beim Schutz der Grundrechte und Grundfreiheiten der Menschen mit gutem Beispiel vorangehen sollten. Die DSGVO unterstreicht die Rolle des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in Fällen, in denen öffentliche Verwaltungen ihre Lieferanten von Produkten und Dienstleistungen auswählen, in Erwägungsgrund 78, wo es heißt: *„Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden“*. Öffentliche Verwaltungen sind aufgerufen, bei der Anwendung dieser Grundsätze an vorderster Front zu stehen, bereit, bei Bedarf ihre Umsetzung der zuständigen Aufsichtsbehörde nachzuweisen.

Datenschutz-Folgenabschätzung

39. Artikel 35 DSGVO sieht eine obligatorische Datenschutz-Folgenabschätzung (DSFA) vor, sobald eine Verarbeitung *„voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat ....“* Diese Verpflichtung ergänzt den **vorgeschriebenen Risikomanagementansatz** von Artikel 24, wenn nach Auffassung der Organisation für natürliche Personen, deren Daten verarbeitet werden, ein hohes Risiko besteht.[49] Die DSFA ist ein herausragendes Instrument der Rechenschaftspflicht, und Organisationen können von diesem Ansatz auch in Fällen profitieren, in denen er nicht vorgeschrieben ist.[50]

40. In ihren Leitlinien zur DSFA[51] stellte die Artikel 29-Datenschutzgruppe fest, sie diene als Garantie des Datenschutzes durch Technikgestaltung, da sie *„vor der fraglichen Verarbeitung durchgeführt werden sollte...“*. Dies steht im Einklang mit den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.[52] Der Umgang mit Datenschutzrisiken steht im Zentrum des Konzepts des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

2.2 Schutz der Privatsphäre durch Technikgestaltung und Datenschutz durch Technikgestaltung in sektoralen Vorschriften der EU

41. Neben der DSGVO gibt es mehrere Bestimmungen im sektoralen Recht der EU, in denen es um die Grundsätze des Schutzes der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen geht.

Die Richtlinie über Privatsphäre und elektronische Kommunikation und die Richtlinie über Funkanlagen und Telekommunikationsendeinrichtungen (RTTE)

42. Die Grundsätze des Schutzes der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen werden im verfügenden Teil der Datenschutzrichtlinie für elektronische Kommunikation[53] nicht ausdrücklich erwähnt. Doch

heißt es jedoch in Erwägungsgrund 30: *„Die Systeme für die Bereitstellung elektronischer Kommunikationsnetze und -dienste sollten so konzipiert werden, dass so wenig personenbezogene Daten wie möglich benötigt werden“*. Dies ist eine Empfehlung an die Anbieter öffentlicher Kommunikationsdienste **und -produkte**, diese Dienste so zu gestalten, dass der Grundsatz der Datenminimierung gewahrt wird.

43. In Erwägungsgrund 46 heißt es: *„Der Schutz personenbezogener Daten und der Privatsphäre des Nutzers öffentlich zugänglicher elektronischer Kommunikationsdienste sollte nicht von der Konfiguration der für die Bereitstellung des Dienstes notwendigen Komponenten (...) abhängen“*, womit an die Notwendigkeit eines allumfassenden Schutzes erinnert wird. Und weiter heißt es dort: *„Daher könnten sich Maßnahmen als notwendig erweisen, mit denen die Hersteller bestimmter Arten von Geräten, die für elektronische Kommunikationsdienste genutzt werden, verpflichtet werden, in ihren Produkten von vornherein Sicherheitsfunktionen vorzusehen, die den Schutz personenbezogener Daten und der Privatsphäre des Nutzers und Teilnehmers gewährleisten“.* Im Anschluss wird ausdrücklich auf den Erlass der Maßnahmen verwiesen, die in Einklang mit der Richtlinie 1999/5/EG[54] über Funkanlagen und Telekommunikationsendeinrichtungen zu erlassen sind. Die Richtlinie 2014/53/EU[55], die sie aufhebt und relevante Vorschriften für Funkanlagen ersetzt, sieht in Artikel 3 Absatz 3 Buchstabe e ausdrücklich vor, dass bestimmte Funkanlagen *„so konstruiert sein müssen...“*, dass sie folgende Anforderung erfüllen: *„Sie verfügen über Sicherheitsvorrichtungen, die sicherstellen, dass personenbezogene Daten und die Privatsphäre des Nutzers und des Teilnehmers geschützt werden“.* Auch bei dieser Verpflichtung ist ein Hinweis auf die **Entwicklungsphase von Produkten** festzustellen.

44. Die Stellungnahme[56] des EDSB zur dem Vorschlag der Kommission, die Datenschutzrichtlinie für elektronische Kommunikation[57] zu ersetzen durch die neue Verordnung über Privatsphäre und elektronische Kommunikation steht in Einklang mit Erwägungsgrund 78 der DSGVO und schlägt für den Sektor folgendes vor: *„(...) eine Verpflichtung für Hardware- und Software-Anbieter, Voreinstellungen umzusetzen, die Endnutzer gegen unerlaubten Zugriff auf Informationen in ihren Geräten und gegen die Speicherung von Informationen in ihren Geräten schützen.“* Diese Verpflichtung würde für **Anbieter von Hardware und Software für alle Arten von Kommunikationsdiensten** gelten, einschließlich Instant Messaging, Voice-over-IP und Mitteilungen personenbezogener Daten zwischen „Objekten“ im Internet der Dinge und Website-Betreibern. Diese Bestimmung würde das Schutzniveau deutlich anheben und allen Anbietern elektronischer Kommunikationsdienste eine echte Möglichkeit bieten, dem Gesetz Genüge zu tun und den Vorwurf eines geringen Schutzes zurückzuweisen, indem sie mit den Fingern auf das Fehlen geeigneter Lieferanten weisen. Ferner wäre sie ein Verweis, der möglicherweise auf eine ähnliche Bestimmung in anderen Sektoren ausgedehnt werden könnte.

eIDAS-Verordnung

45. Die eIDAS-Verordnung[58] bietet den Rahmen für elektronische Identifizierung und Vertrauensdienste im digitalen Binnenmarkt der EU. Da die Erbringung solcher Dienste die Verarbeitung personenbezogener Daten durch den Dienstanbieter erfordert, wird in der Verordnung mehrfach auf die Datenschutzrichtlinie verwiesen. Neben der Wahrung der Datenschutzgrundsätze erwähnt die Verordnung noch ausdrücklich den „eingebauten Datenschutz“ als Grundsatz, der vom eIDAS-Interoperabilitätsrahmen unterstützt werden muss. Die technische Implementierung von eIDAS-Diensten sollte in Anlehnung an einen gemeinsamen Interoperabilitätsrahmen erfolgen, der den Grundsatz des Schutzes der Privatsphäre durch Technikgestaltung umsetzt.[59] Allerdings wäre eine Anpassung der nach

der eIDAS-Verordnung durchgeführten Maßnahmen erforderlich, damit dieses Potenzial ausgeschöpft werden kann.

Intelligente Messsysteme und intelligente Netze für Energie und Gas: ein Fall für die Ko-Regulierung

46. Für den Energiesektor, genauer gesagt für die Einführung intelligenter Messsysteme in der EU, wurde der Grundsatz des Datenschutzes durch Technikgestaltung noch umfassender substantiiert. Im Jahr 2012 gab die Kommission eine Empfehlung[60] zu Vorbereitungen für die Einführung intelligenter Messsysteme in den Strom- und Gasmärkten als Hilfestellung für die Mitgliedstaaten beim Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen und bei der Anwendung der Datenschutzgrundsätze heraus. Die Empfehlung besagte, dass die Mitgliedstaaten ein Muster für die Datenschutz-Folgenabschätzung („DSFA-Muster“) annehmen und anwenden und dann dafür Sorge tragen sollten, dass Netzbetreiber und Betreiber intelligenter Messsysteme geeignete technische und organisatorische Maßnahmen zur Gewährleistung des Schutzes personenbezogener Daten ergreifen. Das Muster wurde von der Industrie mit der Hilfe und Koordinierung der Kommission erarbeitet und der Artikel 29-Datenschutzgruppe zweimal zur Stellungnahme vorgelegt. Es wurde einer im Oktober 2014 angenommenen Empfehlung der Kommission als Anlage beigefügt.[61]

47. Erwägungsgrund 17 der Empfehlung über das DSFA-Muster besagt: *„Ein solches Muster dürfte die Anwendung des Grundsatzes des konzeptionsgebundenen Datenschutzes erleichtern, indem es die für die Datenverarbeitung Verantwortlichen dazu anhält, Datenschutz-Folgenabschätzungen zum frühestmöglichen Zeitpunkt durchzuführen, wodurch sie in die Lage versetzt werden, mögliche Auswirkungen auf die Rechte und Freiheiten von Betroffenen rechtzeitig zu erkennen und strenge Sicherheitsvorkehrungen zu treffen. Solche Maßnahmen sollten von den für die Datenverarbeitung Verantwortlichen über den gesamten Lebenszyklus der Anwendung oder des Systems hinweg überwacht und überprüft werden.“* Dies steht in Einklang mit der **zentralen Rolle des Datenschutz-Risikomanagements**, wie in Absatz39 ausgeführt, und mit der Notwendigkeit, **Vorgaben für den Schutz der Privatsphäre schon in frühen Phasen und während des gesamtem Lebenszyklus** eines Projekts zu berücksichtigen, wie in Absatz27 erläutert.

48. Die Empfehlung 2012/148/EU war auch der Auslöser der Initiative, Beste verfügbare Techniken[62] für die Cybersicherheit und den Schutz der Privatsphäre bei intelligenten Messsystemen auf der Grundlage von zehn funktionalen Mindestanforderungen zu ermitteln. Der Begriff „Beste verfügbare Techniken“ (BAT) [63] bezeichnet *das effektivste und am weitesten fortgeschrittene Stadium der Entwicklung von Aktivitäten und ihrer Arbeitsmethoden; der Begriff bringt zum Ausdruck, dass bestimmte Techniken in der Praxis prinzipiell dafür geeignet sind, die Grundlage für die Einhaltung des EU-Datenschutzrahmens zu bilden. Sie sind zur Vorbeugung oder Minderung von Risiken für die Privatsphäre, für personenbezogene Daten und für die Sicherheit konzipiert“.*

49. Im Sinne von Artikel 25 DSGVO entspricht der Katalog von BAT einem Hinweis auf den Stand der Technik für technische und organisatorische Maßnahmen, bei denen die Wirksamkeit der Maßnahmen, die Ausgereiftheit der Technik und die Implementierungskosten berücksichtigt werden. Darüber hinaus können BAT im Bereich Schutz der Privatsphäre auch als PET gelten.

50. Unserer Ansicht nach könnten einige Elemente der im Bereich intelligenter Messsysteme geleisteten Arbeiten und insbesondere der Ansatz, eine Bestandsaufnahme der besten verfügbaren Techniken für den Schutz der Privatsphäre vorzunehmen, einen Beitrag zur Operationalisierung des Schutzes der Privatsphäre durch Technikgestaltung in verschiedenen Technologiesektoren leisten.

3. Die internationale Dimension des Schutzes der Privatsphäre durch Technikgestaltung

51. Die Anwendung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ist kein Konzept, das nur in der EU gilt, denn ein erheblicher Teil seiner Entwicklung wurde auf der anderen Seite des Atlantiks vorangetrieben. Die sieben Grundprinzipien[64], niedergeschrieben von Datenschutzbeauftragen in der Erklärung von Jerusalem[65], und die Forschungen an Technologien zum Schutz der Privatsphäre sowie Bemühungen, Systeme und Prozesse für Anforderungen an den Schutz der Privatsphäre zu schaffen, haben weltweit Einfluss auf Leitfäden zum Schutz der Privatsphäre und die Definition bester Vorgehensweisen und neuer Standards ausgeübt. In der letzten Zeit ist der Schutz der Privatsphäre durch Technikgestaltung als Grundsatz in das Recht auch anderer Länder eingegangen.[66]

52. Beispiele für Länder, in denen der Ansatz des Schutzes der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen weitgehend von den zuständigen Behörden vorangetrieben wurde, sind Kanada, Australien[67] und die USA, häufig parallel mit der Verwendung von Abschätzungen der Folgen auf den Schutz der Privatsphäre (Privacy Impact Assessments (PIA)), identifiziert als „der“ methodologische Schritt, der bewirkt, dass das Gesamtkonzept schon in den frühen Phasen des Projekts umgesetzt und dazu verwendet wird, Anforderungen im Wege der Beurteilung von Datenschutzrisiken herauszuarbeiten. Profitiert hat der Ansatz von dem breiteren Anwendungsbereich der PIA, der häufig über den reinen Schutz personenbezogener Daten hinausgeht und das weiter gefasste, interdisziplinäre und kontextuelle Konzept des Schutzes der Privatsphäre und sogar andere Grundrechte als Ziele umfasst.

53. In einem Bericht des Jahres 2012[68] schlug die US Federal Trade Commission (FTC) den Schutz der Privatsphäre durch Technikgestaltung als eines der drei Hauptkonzepte[69] eines neuen Rahmens vor, der *„die ganze Bandbreite der Grundsätze für faire Informationspraktiken, fit gemacht für das 21. Jahrhundert“* enthalten soll.[70] Schutz der Privatsphäre durch Technikgestaltung *„muss etwas sein, an das ein Ingenieur oder Website-Entwickler beim Schreiben eines Codes oder bei der Entwicklung eines neuen Produkts instinktiv denkt. Die Wahrung der Privatsphäre muss als fester Bestandteil des Innovationsprozesses gelten ... enthebt den Verbraucher der Last des Schutzes der Privatsphäre ... Nur zu häufig ist der Schutz der Privatsphäre davon abhängig, dass Verbraucher die Juristensprache langatmiger Datenschutzhinweise lesen und verstehen können. Mit ihrem neuen Rahmen möchte sich die FTC von dieser unrealistischen Vision des Schutzes der Privatsphäre abwenden“.*[71]

54. Zwischen dem FTC-Rahmen und der DSGVO bestehen Unterschiede bezüglich des Anwendungsbereichs[72] und der rechtlichen Natur[73], und einige erhebliche Unterschiede sind in der rechtlichen Auslegung einiger der Grundsätze für den Schutz der Privatsphäre zu finden, die umgesetzt werden sollen (z. B. die Rechtmäßigkeit in den Datenschutzgrundsätzen in Artikel 5 DSGVO, einschließlich des strengen Tests der

Notwendigkeit der Datenverarbeitung). Dessen ungeachtet kann die FTC-Definition von Schutz der Privatsphäre durch Technikgestaltung als recht (methodisch und inhaltlich weitgehend) ähnlich dem angesehen werden, was im EU-Recht in allen seinen in Abschnitt 2.1 dargestellten Dimensionen verankert ist, und wurde eindeutig mit Blick auf die Umsetzung des Grundsatzes in der Praxis formuliert.

55. Zwar haben der FTC-Rahmen und andere damit zusammenhängende Initiativen zur konzeptionellen Entwicklung des Schutzes der Privatsphäre durch Technikgestaltung und technologischer Mittel beigetragen, doch ist ein angemessenes Follow-up in Form gesetzgeberischer Entwicklungen bisher ausgeblieben, und deshalb hatten sie nicht die tiefgreifenden und weitreichenden Auswirkungen, die sie bei einem engagierten Einsatz des Gesetzgebers hätten haben können.

56. Vor Kurzem hat das National Institute of Standards and Technology (NIST), eine Einrichtung des US-Handelsministeriums, einen internen Bericht über die Einführung der Konzepte des Privacy Engineering und des Risikomanagements für föderale Systeme in den USA herausgegeben.[74] Dies wäre eine herausragende Neuerung in der Landschaft der Orientierungshilfen, die von Regierungen oder Datenschutzbehörden bereitgestellt werden, denn das Dokument umfasst ein Modell von Risiken für den Schutz der Privatsphäre und eine Methodologie für die Implementierung von Vorgaben für den Schutz der Privatsphäre beim Entwurf von Systemen, die personenbezogene Daten verarbeiten. NIST-Dokumente haben den Rang von Standards für föderale Informationssysteme in den USA und sollten von föderalen Einrichtungen eingehalten werden.[75] Das Programm des NIST zum Privacy Engineering wird fortgesetzt.[76]

4. Verfahren und Systeme gestalten und betreiben und gleichzeitig personenbezogene Daten schützen

4.1 Operationalisierung von Schutz der Privatsphäre/Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

57. Im EU-Datenschutzrecht und anderen Rahmen für den Schutz der Privatsphäre, wie den Grundsätzen für faire Informationspraktiken (FIPP)[77] oder den OECD-Leitlinien[78], werden Ziele vorgegeben, findet sich aber in der Regel keine Hilfestellung dazu, wie diese in der Praxis erreicht werden können. Die Anwendung des Grundsatzes des Schutzes der Privatsphäre durch Technikgestaltung kann bei der Lösung dieses Problems helfen, denn sie gibt praxisbezogene Hinweise für Folgendes:

    1. Festlegung einer Methodologie für die Integration von Vorgaben für den Schutz der Privatsphäre und den Datenschutz in Projekte, mit denen ein Prozess, Verfahren oder System entwickelt werden soll, das personenbezogene Daten verarbeitet;

    2. Identifizierung und Durchführung geeigneter technischer und organisatorischer Maßnahmen, die zum Schutz natürlicher Personen und ihrer Daten in diese Prozesse, Verfahren und Systeme eingebaut werden können. Unterstützt werden können diese Maßnahmen durch technologische Innovation;

    3. Integration der Unterstützung für den Schutz der Privatsphäre in dem Management- und Governance-Rahmen der Organisation durch Identifizierung von Aufgaben und Festlegung und Zuweisung von Ressourcen und Verantwortlichkeiten.

58. Schon seit langem gibt es Methodologien für die Festlegung von Anforderungen an Geschäftsprozesse und IT-Systeme.[79] Einvernehmen besteht insbesondere in der Frage, wie Anforderungen für IT-Systeme vorbereitet werden sollten, und Wissenschaft und Industrie haben zahlreiche bewährte Vorgehensweisen vorgeschlagen und übernommen. Normalerweise wird zwischen funktionalen und nicht funktionalen Anforderungen unterschieden. Unter funktionalen Anforderungen versteht man diejenigen, die den Hauptgeschäftszweck und die Spezifizität des zu entwickelnden Systems festlegen. Nicht funktionale Anforderungen[80] gelten für alle Systeme und betreffen horizontale Fragen, wie Sicherheitsbedürfnisse und Einhaltung des geltenden Rechts. Der Schutz der Privatsphäre und der Datenschutz sollten den nicht funktionalen Anforderungen zugerechnet werden.[81]

59. Aus vielerlei Gründen wurde jedoch bei der Gestaltung von Systemen der Schutz der Privatsphäre häufig vergessen oder als Nebensache betrachtet. Zu den Gründen hierfür zählen das kontextgebundene und häufig kulturabhängige Konzept des Schutzes von Privatsphäre und die Schwierigkeit, Zielsetzungen des Schutzes der Privatsphäre in einklagbare Anforderungen zu übersetzen. Die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) hat im Dezember 2014[82] eine umfassende Analyse des Stands der Technik bei der Gestaltung des Schutzes der Privatsphäre durch Technikgestaltung vorgelegt.

4.2 Engineering von Schutz der Privatsphäre und Datenschutz

Identifizierung von Anforderungen an den Datenschutz und Auswahl geeigneter Maßnahmen, um diesen Anforderungen gerecht zu werden

60. Nach einigen der derzeitigen Methodologien des Privacy Engineering werden Datenschutzziele entweder direkt anhand der Datenschutzgrundsätze festgelegt oder werden operationelle Zwischenziele festgelegt, die es ermöglichen, die ursprünglichen Ziele zu erreichen. Andere Methodologien stützen sich recht ausdrücklich auf einen Risikomanagementansatz, indem sie das Risiko, die Datenschutzgrundsätze nicht einzuhalten, identifizieren und dagegen vorgehen, und/oder indem sie direkt mögliche nachteilige Auswirkungen auf natürliche Personen analysieren.

61. In Abschnitt 2.1 sagen wir, dass die DSGVO diese Grundsätze als zu erreichende Ziele betrachtet; sie werden als „Stellvertreter“ für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen verwendet, unabhängig vom Risikoniveau. Gleichzeitig verfolgt sie einen „Vorsorge“-Ansatz und nennt Garantien, die unter allen Umständen unter bestimmten Bedingungen implementiert werden müssen (z. B. Sicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten usw.). Was dann noch zu tun ist, um den erwarteten Schutz natürlicher Personen zu erreichen und ihnen die bestehenden Datenschutzrechte aufgrund der Umstände, der Art der Daten, der Art der Verarbeitung usw. zu gewähren, bleibt dann dem Risikomanagementansatz überlassen. Dieser Ansatz versetzt Organisationen in die Lage, neue Maßnahmen zu identifizieren, und er trägt dazu bei, dass das näher spezifiziert und integriert wird, was aufgrund des Risikos für die Personen bereits obligatorisch ist.

62. In Anlehnung an Methodologien der Software-Entwicklung verwendet der Ansatz einen Katalog spezifischer Gestaltungsmuster für die Entwicklung von Lösungen bekannter Probleme mit dem Schutz der Privatsphäre. Auf diesen Aspekt wird näher in Absatz 72 eingegangen.

Beispiele für bestehende Methodologien

63. Auf der Grundlage der Festlegung von Zielen für den Schutz der Privatsphäre und den Datenschutz ist es nunmehr möglich, Gestaltungsmethodologien zu entwickeln, in die die entsprechenden Anforderungen vollständig integriert werden können. In diesem Abschnitt finden Sie eine kurze Einführung in einige dieser Methodologien; zu einer Vertiefung seien dem interessierten Leser die Quellendokumente empfohlen.

64. Die „Six protection goals for privacy engineering“[83] bieten einen Rahmen für die Identifizierung von Garantien für IT-Systeme, die personenbezogene Daten verarbeiten. Auf den klassischen IT-Sicherheitsdreiklang[84] von „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ folgen drei weitere Ziele[85]: „Unverlinkbarkeit“, „Transparenz“ und „Interventionsfähigkeit“. In diesem Zusammenhang geht es bei IT-Sicherheit nicht um Risiken für die Organisation, sondern vielmehr um Risiken für die Rechte natürlicher Personen. Wenn klar ist, welche Werte zu schützen sind (die natürlichen Personen), kann eigentlich jeder übliche Ansatz zur Anwendung kommen, der in der Literatur zum IT-Sicherheitsrisikomanagement bekannt ist.

65. „Unverlinkbarkeit“ bezeichnet die Fähigkeit von Informationsstücken, miteinander und mit einer natürlichen Person verbunden zu sein. Dazu gehört ganz eindeutig auch die Anonymität. „Transparenz“ impliziert, dass *„alle für den Schutz der Privatsphäre relevanten Datenverarbeitungen einschließlich der rechtlichen, technischen und organisatorischen Gegebenheiten jederzeit verstanden und rekonstruiert werden können... Des Weiteren ist sie Voraussetzung für Rechenschaftspflicht. Zu den Standardmethoden, mit denen sich Transparenz erreichen oder fördern lässt, gehören Protokolle und Berichte, die Dokumentation der Datenverarbeitung oder Mitteilungen an den Nutzer.“* „Interventionsfähigkeit“ ermöglicht *„die wirksame Durchsetzung von Veränderungen und Korrekturmaßnahmen“* und ist von Bedeutung, damit natürliche Personen ihre Rechte wahrnehmen und möglicherweise zuständige Behörden eingreifen können.

66. Diese Ziele sind miteinander verbunden und machen unter anderem deutlich, dass Maßnahmen zum Schutz der Privatsphäre durchaus miteinander kollidieren könnten. So erhöht beispielsweise das Protokollieren von Vorgängen im Zusammenhang mit personenbezogenen Daten im Dienste der Interventionsfähigkeit das Risiko, das Ziel der „Unverlinkbarkeit“ zu verfehlen, weil das Risiko eines Missbrauchs der protokollierten Vorgänge entsteht. Zur Abrundung des Bildes noch der Hinweis, dass diese Ziele nach einer Methodologie verwendet werden könnten, mit der Garantien aufgetan werden, mit denen sie erreicht werden können, und dass es Bemühungen gibt, einen Katalog möglicher Maßnahmen zu erstellen, die diesen Zielen dienen.

67. Das US-amerikanische NIST[86] hat Privacy Engineering definiert als eine *„Spezialdisziplin der Systemtechnik, in deren Mittelpunkt steht, Freiheit von Bedingungen zu erlangen, die für natürliche Personen Probleme mit nicht hinnehmbaren Folgen schaffen können, die aus dem System bei der Verarbeitung von PII[87] entstehen“*. Nach Ansicht des NIST besteht Privacy Engineering aus einer Vielzahl von Komponenten, deren Grundlage ein Rahmen für das Risikomanagement und Engineering-Ziele sind. Sie identifizieren ein Modell mit Risiken für den Schutz der Privatsphäre und drei Systemziele für den Schutz der Privatsphäre zusätzlich zu den klassischen Sicherheitszielen in Gestalt von Vertraulichkeit, Integrität und Verfügbarkeit: **Vorhersehbarkeit**, **Beherrschbarkeit** und **Trennbarkeit**. Die drei Ziele helfen bei der Gestaltung von Systemen, damit diese den Grundsätzen des Schutzes der Privatsphäre entsprechen[88], wie im Referenzdokument gezeigt[89].

68. Bei der „Vorhersehbarkeit“ geht es um *„das Ermöglichen zuverlässiger Annahmen durch natürliche Personen, Eigentümer und Betreiber bezüglich PII und deren Verarbeitung durch ein Informationssystem.“* Dies bedeutet die Integration von Mechanismen, die gewährleisten und den Stakeholdern gegenüber belegen, dass das, was zum Schutz natürlicher Personen und ihrer Daten getan werden sollte, getan wurde und wirksam ist. So würde beispielsweise das Erdenken eines Mechanismus für das Management von Einwilligungen, der auch nachweist, was ausgewählt wurde, dem Ziel der Vorhersehbarkeit entsprechen. „Beherrschbarkeit“ bedeutet *„Bereitstellung der Fähigkeit zur granularen Verwaltung von PII einschließlich Änderung, Löschung und selektiver Weitergabe“,* die für ein ordnungsgemäßes Management personenbezogener Daten wesentlich sind. „Trennbarkeit“ ermöglicht *„die Verarbeitung von PII oder Ereignissen ohne Zuordnung zu natürlichen Personen oder Geräten über die operativen Anforderungen des Systems hinaus.“* Im Mittelpunkt dieses Ziels beim Schutz der Privatsphäre stehen eindeutig Datenminimierung und mögliche Anonymisierung.

69. In der Methodologie des NIST für Privacy Engineering ragt die Vorhersehbarkeit als eine Art Meta-Ziel heraus, das die Grundlage für Wirksamkeit bei der Implementierung von Maßnahmen bildet, sowie für Transparenz und Rechenschaftspflicht der vorgeschlagenen Lösungen gegenüber den Stakeholdern (natürliche Personen, zuständige Behörden, Gesellschaft usw.). Ein Beispiel aus der Praxis für die Umsetzung dieses Ziels sind Maßnahmen wie der Einsatz von Kryptographie als mathematische Nachweise von Fakten.

70. Ein weiteres Beispiel für eine Methodologie des Privacy Engineering, in diesem konkreten Fall mit Betonung auf der Dimension der Risikoanalyse, ist der LINDDUN[90]-Ansatz, der an der Universität Löwen entwickelt wurde. Er umfasst Folgendes:

    - Schaffung von Datenflussdiagrammen auf der Grundlage einer High Level-Systembeschreibung;

    - Kartierung folgender Kategorien von Bedrohungen für den Schutz der Privatsphäre: Verlinkbarkeit, Identifizierbarkeit, Nichtabstreitbarkeit, Nachweisbarkeit, Weitergabe von Informationen, fehlendes Bewusstsein, Nichtkonformität, wie in den Methodologien identifiziert, mit den Diagrammelementen;

    - Identifizierung der Elemente der Datenflussdiagramme, bei denen diese Bedrohungen ein Risiko darstellen könnten, und Durchführung einer Risikoanalyse unter Verwendung der von der Methodologie angebotenen Baummuster für Bedrohungen des Schutzes der Privatsphäre. Gestützt auf die Ergebnisse der Analyse werden die Bedrohungen dann nach ihrer Priorität geordnet. LINDDUN macht keine Aussagen dazu, wie die Risikobeurteilung vorgenommen werden soll. Das bedeutet, dass die Kriterien, anhand derer die Prioritäten bei den Risiken festgelegt werden, der Organisation überlassen bleiben, die die Methodologie umsetzt; damit verfügt die Organisation über einen gewissen Spielraum.

    - Auf der Grundlage der Prioritäten bei den Risiken werden Eindämmungsstrategien und spezifische Lösungen ausgewählt, die für die jeweiligen Bedrohungen relevant sind. Die Methodologie bietet eine Taxonomie von Eindämmungsstrategien, die nach Bedarf integriert und detailliert werden können. Sodann müssen PET für eine wirksame Implementierung dieser Strategien ausgewählt werden.

71. Im Zentrum der LINDDUN-Methodologie steht das Risikomanagement, ergänzt durch einen Katalog technologisch neutraler High Level-Strategien, die mit Maßnahmen der

Organisation und dem Stand der Technik entsprechenden technologischen Lösungen umzusetzen sind.

72. Ein anderer Ansatz für die Identifizierung von Maßnahmen zur Umsetzung von Vorgaben zum Schutz der Privatsphäre ist die Identifizierung von „Mustern“ (patterns) bei der Gestaltung von IT-Lösungen für Vorgaben zum Schutz der Privatsphäre. „Gestaltungsmuster“ (design patterns), wie sie in Methodologien für die Software-Entwicklung zur Lösung immer wiederkehrender Probleme definiert werden[91], werden als Bausteine für die Implementierung von Maßnahmen zum Schutz der Privatsphäre in Systemen[92] im Kontext einer Strategie (und einer Taktik) vorgeschlagen. Diese Muster werden dann in der Praxis in Software-Bausteinen implementiert und durch PET unterstützt. „Gestaltungsstrategien“ (design strategies) für weithin bekannte Probleme beim Schutz der Privatsphäre werden identifiziert[93] durch Beschreibung *„eines grundlegenden Ansatzes für das Erreichen eines bestimmten Gestaltungsziels“*. Für eine bessere Modellbildung können sie in eine weitere, spezifischere Abstraktionsschicht untergliedert werden (z. B in so genannt „Taktiken“, als *„Ansätze zum Schutz der Privatsphäre durch Technikgestaltung, die zu einer übergeordneten Strategie beitragen“*).

Abdeckung des gesamten Lebenszyklus von Diensten und Produkten, Governance und Management von Organisationen

73. Zwar stellen einige Methodologien für das Privacy Engineering im Wesentlichen die Phase der Anforderungen oder die durchzuführenden Maßnahmen in den Mittelpunkt, doch muss beim Privacy Engineering der gesamte Lebenszyklus eines Dienstes oder eines Produkts bedacht werden, von den allerersten Planungen bis hin zur Entsorgung des Dienstes/Produkts. Damit der Gesamtansatz angewandt werden kann, bedarf es angemessener Governance- und Managementstrukturen und -verfahren in der Organisation.

74. Ein Beispiel für eine Methodologie, die auf den gesamten Lebenszyklus des Projekts abhebt, ist eine von dem Forschungsprojekt PRIPARE[94] erarbeitete, in der umfassende Aktionen und Leistungen im Zusammenhang mit dem Schutz der Privatsphäre vorgeschlagen werden, und zwar über acht Projektphasen, von den Überlegungen bezüglich des Organisationsumfelds und der Infrastruktur bis hin zur Stilllegung des Systems. Weitere hilfreiche Hinweise sind in einer gerade erst veröffentlichten Web-Publikation der norwegischen Datenschutzbehörde zu finden.[95]

75. Unter wirksamem Schutz der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ist im Wesentlichen zu verstehen, dass der Schutz der Grundrechte einer natürlichen Person eine der Aufgaben der Organisation wird und als solche in der Governance- und Managementstruktur der Organisation erkennbar sein muss, mit einer ordnungsgemäßen Zuweisung von Aufgaben und Verantwortlichkeiten im Bereich des Schutzes der Privatsphäre und auf nachvollziehbare Weise. Die Hauptverantwortung für Anforderungen an den Schutz der Privatsphäre liegt beim Management; die Umsetzung kann an die für die Gestaltung und den Betrieb der einschlägigen Systeme zuständigen Abteilungen delegiert werden. Die IT- und Technologieabteilungen unterstützen die Geschäftsinhaber auf der Grundlage von deren Weisungen und bewährten Gestaltungspraktiken.

76. Eine wichtige Rolle spielen die Datenschutzbeauftragten, deren Einbeziehung bei einem Ansatz des Schutzes der Privatsphäre durch Technikgestaltung von entscheidender Bedeutung ist. Sie müssen ab den allerersten Phasen eingeweiht sein, wenn also

Organisationen Systeme für die Verarbeitung personenbezogener Daten planen, damit sie Manager, Geschäftsinhaber und IT- und Technologieabteilungen bei Bedarf unterstützen können. Ihr Kompetenzprofil sollte diesen Anforderungen entsprechen.

77. Der EDSB hat Leitlinien für IT-Management und IT-Governance[96] zur Unterstützung der EU-Organe bei der Berücksichtigung von Anforderungen an den Schutz der Privatsphäre und den Datenschutz in der Entwicklung und im Betrieb von IT-Systemen und in der Frage herausgegeben, wie die IT-Governance einer Organisation in Einklang mit dem Grundsatz der Rechenschaftspflicht eingerichtet werden kann. Diese Leitlinien stützen sich auf allgemein geltende Grundsätze, auch wenn sie sich an die EDSB-spezifische Zielgruppe wenden.

Standardisierungsbemühungen

78. Standardisierungsbemühungen zur Integration der Anforderungen an den Schutz der Privatsphäre in die Gestaltung des Systems hat es schon in mehreren Normungsorganisationen und -initiativen gegeben.[97] Häufig nehmen sie bestehende Ansätze für das Risikomanagement der IT-Sicherheit als Modell, das dann auf das Management von Risiken für den Schutz der Privatsphäre erweitert und abgeändert wird. So hat beispielsweise die ISO Normen für einen Rahmen für den Schutz der Privatsphäre (ISO/IEC 29100) und eine Architektur des Schutzes der Privatsphäre (ISO IEC 29101) herausgegeben, in denen es um PII in einem Informations- und Kommunikationstechnologie-Umfeld geht. Im Zuge ihrer Arbeiten wurden auch die Normen ISO/IEC 27001 und 27002 über das Management der Informationssicherheit auf das Management des Schutzes der Privatsphäre ausgedehnt. Ein andere Beispiel ist die RFC 6973[98] der IETF zu „Privacy considerations for Internet Protocols“, die sich die Aufnahme von Anforderungen an den Schutz der Privatsphäre in Internetprotokolle zum Ziel gesetzt hat.

79. Die Normungstätigkeit im Bereich Schutz der Privatsphäre dürfte auch mit Blick auf die Rolle weiter zunehmen, die möglicherweise Zertifizierungen als Nachweis der Einhaltung der DSGVO spielen werden. Zertifizierungsverfahren können zum Nachweis dafür verwendet werden, dass der Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gewahrt wurde.[99]

80. Im Jahr 2015 forderte die Europäische Kommission[100] die europäischen Normungsorganisationen (ESO)[101], die eine Kooperationsvereinbarung[102] mit der Kommission haben, auf, an einem „Ansatz für den Schutz der Privatsphäre und den Datenschutz durch Technikgestaltung“ und einem „Rahmen für das Management von Schutz der Privatsphäre und Datenschutz“ für die Sicherheitsbranche zu arbeiten. 2017, nach der Verabschiedung der DSGVO, haben die ESO die Möglichkeit eines breiter angelegten und deutlicheren Arbeitsplans geprüft, der Privatsphäre, Datenschutz und Cybersicherheit umfasst. Er umfasst: eine Norm zu „Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ mit *„Vorgaben für Hersteller und/oder Diensteanbieter“* für die Umsetzung des Grundsatzes, *„… geltend für alle Wirtschaftssektoren einschließlich der Sicherheitsbranche“*, sowie technische Berichte zu spezifischen Umsetzungen des Grundsatzes[103], Initiativen für Cybersicherheit und Schutz der Privatsphäre und Datenschutz zur Unterstützung neuerer und laufender einschlägiger politischer Entscheidungsprozesse auf EU-Ebene.[104] Diese Normungstätigkeit kann für die Industrie und alle Stakeholder der Ausgangspunkt für die Feststellung des Stands der Technik beim Schutz der Privatsphäre

sein. Daher kommt es unbedingt darauf an, dass das Ergebnis in Einklang mit den einschlägigen Rechtsvorschriften steht, damit es tatsächlich zu einer korrekten Umsetzung des Schutzes der Privatsphäre durch Technikgestaltung beiträgt.[105]

4.3 Technologien zum Schutz der Privatsphäre (Privacy enhancing technologies (PET))

81. Technologien zum Schutz der Privatsphäre, also spezifische technische Lösungen für bestimmte Probleme beim Schutz der Privatsphäre in der Systemgestaltung, waren die Vorläufer der Idee eines umfassenden Ansatzes des Privacy Engineering[106] und können heute als hochwertige Grundbausteine für die Gestaltung des Schutzes der Privatsphäre betrachtet werden. Eine umfassende Auflistung bestehender PET würde den Rahmen dieses Dokuments sprengen, aber wir können auf einige relevante Beispiele hinweisen, wie z. B. eine Gestaltungsstrategie namens „attribute-based credentials“ (attributbasierte Anmeldedaten) oder „anonymous credentials“ (anonyme Anmeldedaten), die natürlichen Personen die Möglichkeit gibt, sich gegenüber einem Dienst zu authentifizieren, ohne ihre volle Identität offenzulegen; sie geben vielmehr auf vertrauenswürdigem Übertragungsweg selektiv nur die Attribute an, die in dem betreffenden Zusammenhang unbedingt erforderlich sind. Ermöglicht wird dies durch die Verwendung spezifischer kryptographischer Konzepte wie Zero-Knowledge Proofs. Ein Beispiel: Wendet sich ein Dienst an Erwachsene, sollten natürliche Personen lediglich auf sicherem und zuverlässigem Weg angeben, dass sie älter als 18 Jahre sind, ohne dass sie dem Dienst ihr Alter oder andere Identitätsattribute verraten.[107]

82. Viele Entwickler aus kommerziellen und nicht kommerziellen Umfeldern haben in die Bereitstellung von Tools und Diensten mit verbesserten Merkmalen beim Schutz der Privatsphäre investiert. Zu den betroffenen Bereichen gehören Messaging-Dienste, die häufig vollständige End-to-End-Verschlüsselung bieten und ohne jegliche Zentralserver arbeiten, die Kommunikationsinhalte oder Metadaten verarbeiten oder speichern. Ihre insbesondere seit 2013 wachsende Beliebtheit hat mit Sicherheit dazu beigetragen, dass ähnliche Verschlüsselungsstandards jetzt auch für sehr viel häufiger benutzte Kommunikationsinstrumente gelten. Gewisse Erfolge konnten auch in Bereichen wie Suchmaschinen festgestellt werden. Beliebte Browser wurden mit mehr Kontrollen zum Schutz der Privatsphäre ausgestattet, wie z. B. Do Not Track (DNT)-Merkmalen[108] und Nutzerkontrolle über Tracking-Merkmale, und sie können durch zahlreiche Add-ons aufgerüstet werden, die Tracking-Versuche unterdrücken oder das Profiling begrenzen. Kommunikationsinfrastrukturen wie Mix-Networks[109] und auch komplette Betriebssysteme wurden ebenfalls bis zu einer umfassenden Benutzerfreundlichkeit weiterentwickelt. Die technologieorientierten Elemente der DSGVO sind Auslöser für neue, auf Technologie basierende Geschäftsideen, z. B. Unterstützung aussagekräftiger Einwilligungsmechanismen und Datenübertragbarkeit. Alle diese Entwicklungen zeigen, dass die technologische Kompetenz für die Umsetzung des Schutzes der Privatsphäre durch Technikgestaltung durchaus vorhanden ist.

83. Die Entwicklung von PET erstreckte sich über Jahre, und es hat Bemühungen gegeben, eine Bestandsaufnahme der vorliegenden Ergebnisse vorzunehmen, beispielsweise den Bericht der ENISA über den Stand der Technik zum Schutz der Privatsphäre in ihrer Publikation zum Schutz der Privatsphäre durch Technikgestaltung vom Dezember 2014.[110] Ergänzt wurde dieser Bericht durch einen weiteren über den Schutz der Privatsphäre durch Technikgestaltung für die Big Data-Analyse.[111]

84. In den letzten Jahren hat sich die ENISA weiter intensiv mit dem Stand der Technik befasst und eine Methodologie für die Analyse der Einsatzbereitschaft und Ausgereiftheit von PET erarbeitet[112], einen Ansatz für die Bewertung von Online- und mobilen Tools für den Schutz der Privatsphäre sowie Empfehlungen für alle Stakeholder, von Entwicklern bis zu zuständigen Behörden, für den Aufbau und die Pflege eines angemessenen und qualifizierten Registers zur Ausgereiftheit von PET. In der letzten Ausgabe des Berichts empfiehlt die ENISA zuständigen Behörden und Regulierern, sich einzusetzen für *„den Einsatz des Tools als Online-Register von PET-Beurteilungen vor dem Hintergrund der Umsetzung des Grundsatzes des Schutzes der Privatsphäre durch Technikgestaltung in der Praxis“,* der Forschungsgemeinschaft, ihn zu unterstützen durch *„aktive Mitwirkung als Bewerter und Nutzer der Plattform sowie durch Werbung für seine weitere Nutzung“*, und der Forschungsgemeinschaft, der Kommission und den EU-Einrichtungen im Bereich Sicherheit und Schutz der Privatsphäre, die Plattform zu verbessern.

85. Der EDSB wird auch weiterhin auf den laufenden Initiativen der ENISA aufbauen, und zwar mit seinen eigenen künftigen Aktionen zur Förderung des Privacy Engineering. Ein gut funktionierendes, auf dem neuesten Stand befindliches und qualitätsgestütztes Bewertungstool kann einen Beitrag leisten zur Überwachung und zum Benchmarking des Implementierungsniveaus des Schutzes der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, indem es mit dem Stand der Technik bei PET Schritt hält.

86. In seinen formellen Kommentaren[113] zum Cybersicherheitspaket der Kommission hat der EDSB darauf hingewiesen, dass die ENISA derzeit die einzige Einrichtung auf EU-Ebene ist, die über die Kompetenz und die Ressourcen verfügt, um gezielt Forschung zu betreiben und zu beraten in Sachen Schutz der Privatsphäre und Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen und in Sachen Technologien zum Schutz der Privatsphäre (PET). Wir wiederholen unsere Empfehlung, diese Funktion beizubehalten und auszubauen, wenn nicht bei der ENISA, dann bei einer anderen Einrichtung wie dem EDSB.

5. Technologie für Menschen: dem Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zum Durchbruch verhelfen

5.1 Fortschritte beim „Stand der Technik“ und beim Einsatz von Lösungen zur Erhöhung des Datenschutzes

Derzeitige Lage

87. Die Analyse, die wir 2010 in unserer „Stellungnahme zur Stärkung des Vertrauens in die Informationsgesellschaft durch die Förderung des Schutzes von Daten und Privatsphäre“ vorgenommen haben, ist noch heute weitgehend gültig. Es besteht nur eine begrenzte Aufnahme von kommerziellen Produkten und Diensten, die das Konzept des Schutzes der Privatsphäre durch Technikgestaltung und durch datenschutzfreundlichen Voreinstellungen vollständig umsetzen. Auf der anderen Seite haben Enthüllungen über staatliche Überwachung das Bewusstsein für die Gefahren der allgegenwärtigen und massiven Erhebung personenbezogener Daten für Profilingzwecke geschärft. Mit dem Erscheinen der DSGVO reagiert die Öffentlichkeit sensibler und verfügen Unternehmen über Anreize, Aufmerksamkeit und Ressourcen in Richtung Schutz der Privatsphäre und Datenschutz umzulenken. Dieser Trend dürfte sich fortsetzen, da die DSGVO vollumfänglich

anzuwenden ist und Durchsetzungsmaßnahmen beginnen. Die derzeitige politische Aufmerksamkeit für das kommerzielle Tracking für Profiling- und Targeting-Zwecke hat möglicherweise zur Folge, dass die Nachfrage nach überall verfügbaren Diensten und Produkten weiter steigt, die den Schutz der Privatsphäre durch Technikgestaltung unterstützen.

88. PET haben sich einen gewissen Anteil am kommerziellen Mainstream-Angebot erobert, einschließlich einer zunehmenden Verwendung der Kryptographie für die Sicherheit personenbezogener Daten (z. B. mobiles Messaging mit End-to-End-Verschlüsselung), Nutzung von Do Not Track[114] und seinen standardmäßigen No-Tracking-Einstellungen (obwohl dies häufig von den Dienstanbietern nicht honoriert und unterschiedlich ausgelegt wird) oder Anwendung von so genannten „differential privacy algorithms“[115] bei der Erhebung von Nutzungsstatistiken bei den Kunden. Datenschutzfreundliche Suchmaschinen scheinen nachhaltig zu funktionieren. Andere Dienste sind noch als Nischenangebot zu betrachten und werden nur begrenzt genutzt. Die Familie der Produkte und Dienstleistungen, die unter der Bezeichnung Personal Information Management Systems (PIMS) bekannt ist, bietet den Nutzern die Möglichkeit, mithilfe von PET und einer neuen Konfiguration der Daten-Governance ihre Daten stärker zu kontrollieren, was häufig der Anstoß zu neuen Geschäftsmodellen ist. Der EDSB hat in seiner Stellungnahme zu Systemen für das *Personal Information Management* den Sachstand dargestellt und Empfehlungen für politische Maßnahmen ausgesprochen.[116]

89. Wissenschaft und Industrie haben mit Unterstützung von Vereinigungen der Zivilgesellschaft und einigen Datenschutzbehörden relevante Forschungsarbeiten in Bereichen wie Datenwissenschaft, Kryptographie, Quantenphysik, Künstliche Intelligenz und maschinelles Lernen sowie Humanwissenschaften durchgeführt. Ingenieur- und Internetverbände haben damit begonnen, für das Privacy Engineering gezielt Ressourcen und Sichtbarkeit bereitzustellen.[117] Die EU hat zahlreiche Projekte über die Rahmenprogramme für Forschung und technologische Entwicklung und andere politische Initiativen kofinanziert. Das alles ist zwar bemerkenswert und ermutigend, reicht aber noch nicht aus.

Wie geht es weiter?

90. Von zentraler Bedeutung ist, dass weiter geforscht und gleichzeitig dafür Sorge getragen wird, dass Technologien zum Schutz der Privatsphäre ein hohes Maß an Ausgereiftheit erreichen und zu bezahlbarer Technologie, bezahlbaren Produkten und Diensten auf dem Markt weiterentwickelt werden können.

91. **Politische Maßnahmen zur Förderung von Technologien und Strategien zum Schutz der Privatsphäre** sollten auf der Agenda der EU ganz oben stehen. Der LIBE-Ausschuss des Europäischen Parlaments[118] erörtert gerade seine Stellungnahme zum Cybersicherheitspaket der Kommission. Er hat die dringliche Aufforderung des EDSB berücksichtigt, die Unterstützung der EU für Forschung und politische Beratung zum Thema PET nicht aufzugeben, und prüft dementsprechend Änderungen an dem gemeinsamen Vorschlag für die überarbeitete ENISA-Verordnung. Wir legen dem EU-Gesetzgeber nachdrücklich nahe, eine kontinuierliche Unterstützung für Technologien zum Schutz der Privatsphäre sicherzustellen, indem einer geeigneten Stelle eindeutig Aufgaben zugewiesen und angemessene Ressourcen bereitgestellt werden.

92. **Eine gemeinsame Strategie für den Schutz der Privatsphäre durch Technikgestaltung und für PET kann ein ausgezeichneter Hebel für einen konstruktiven Dialog auch auf internationaler Ebene sein.** Der EDSB hat vor einigen Jahren die Initiative IPEN[119] ins Leben gerufen, um die Lücke zwischen gesetzlichen Vorgaben und Privacy Engineering durch Vernetzung zu schließen, indem er auf bereits bestehende Initiativen für Privacy Engineering hinweist und Lösungen für den Schutz der Privatsphäre für die Öffentlichkeit durch koordinierte Aktionen fördert. Nach einer bisherigen ausschließlichen Ausrichtung auf EU-Akteure veranstalteten wir im November 2017 einen Workshop[120] gemeinsam mit dem Future of Privacy Forum, dem ULD[121], der Carnegie Mellon University und der KU Löwen, in dem wir den Stand der Technik sowie Herausforderungen für Privacy Engineering mit den Schwerpunkten EU und USA erörterten. Die akademischen Partner beschlossen, die auf dem Workshop identifizierten Fragen zu erforschen und bestehende Lücken bei verfügbaren und bezahlbaren Technologien zum Schutz der Privatsphäre in transatlantischer[122] Kooperation zu schließen. In absehbarer Zukunft könnten erste akademische Veröffentlichungen vorliegen.

93. **Öffentliche Verwaltungen sollten mit gutem Beispiel vorangehen**, wenn es um die umfassende Wahrung des Grundsatzes des Schutzes der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen geht**.** Wir sind zutiefst davon überzeugt, dass dies der richtige Weg ist, denn auf diese Weise könnte indirekt ein angemessenes Angebot der Anbieter angeregt werden. In den Schlussfolgerungen der Erklärung von Tallinn zu E-Government vom Oktober 2017[123] heißt es: *„Die Entwicklung von E-Government hat die Grundrechte der Menschen wie Meinungsfreiheit, Schutz der Privatsphäre und Recht auf den Schutz personenbezogener Daten zu achten, zu unterstützen und zu stärken und mit dem einschlägigen EU-Recht, insbesondere der Datenschutz-Grundverordnung, in Einklang zu stehen. () Wir werden dafür Sorge tragen, dass Bedürfnisse der Informationssicherheit und des Schutzes der Privatsphäre berücksichtigt werden bei der Gestaltung von Lösungen für die Informations- und Kommunikationstechnologie (IKT) öffentlicher Dienste und öffentlicher Verwaltungen, nach einem risikobasierten Ansatz und unter Verwendung von Lösungen, die dem Stand der Technik entsprechen...Wir fordern die Kommission auf, gemeinsam mit unseren Ländern an Vorschlägen dazu zu arbeiten, wie Mittel der EU für Forschung und Entwicklung verstärkt in die Entwicklung von Tools für Cybersicherheit und Schutz der Privatsphäre und ihren Einsatz in den öffentlichen Verwaltungen gelenkt werden können - im Jahr 2018."* Der EDSB schließt sich diesem Aufruf an und wird zu diesem politischen Ziel in Form spezifischer Initiativen im Rahmen seiner Beratungs- und Aufsichtsfunktion für EU-Organe beitragen, wo Pilotprojekte Vorreiter für machbare Lösungen sein könnten. Wir fordern die Kommission auf, ihre Finanzierungsprogramme wie die Programme für Forschung und Entwicklung, die Strukturfonds und die administrative Zusammenarbeit, wie ISA^2, einzusetzen und politische Initiativen zu koordinieren, mit denen die Funktion des öffentlichen Sektors als treibende Kraft dabei gestärkt wird, den Stand der Technik und den Markt voranzutreiben.

94. Ein System politischer und wirtschaftlicher Anreize (letztere vor allem für KMU) sollte auf EU- und auf nationaler Ebene koordiniert werden, damit zugunsten des Einzelnen und der Gesellschaft insgesamt die Schwelle eines wirtschaftlich tragfähigen „Stands der Technik" gesenkt werden kann. Besonders von Bedeutung ist dies in der derzeitigen datengesteuerten Landschaft der Online-Unternehmen, in der Oligopole Start-ups und KMU daran hindern, lohnende Investitionen bei PET zu planen.[124]

95. Bei der Wahl technischer und organisatorischer Maßnahmen zum Datenschutz oder bei der Bewertung der von einer Organisation ergriffenen Maßnahmen spielt der Kostenfaktor eine Rolle. Die Vorteile, die einer Organisation aus ihren Investitionen erwachsen, werden gegen die Kosten aufgewogen. Ihr Risiko, haftbar gemacht zu werden, Schaden zu erleiden oder Sanktionen auferlegt zu bekommen, sinkt nicht nur, wenn sie personenbezogene Daten schützen. In einer Gesellschaft, die immer aufmerksamer und alarmierter beobachtet, wie die Verwendung ihrer Daten sich nachteilig auf ihr Leben auswirken könnte[125], **sollte ein überzeugendes und anhaltendes Engagement für den Schutz der Privatsphäre durch Technikgestaltung als Wettbewerbsvorteil gesehen werden**. Im Bericht Global Human Capital Trend 2018 von Deloitte[126] ist die Rede von einem notwendigen Wandel von Unternehmen zu „sozialen Unternehmen", in denen die Aufrechterhaltung guter Beziehungen zu diversen Stakeholdern, darunter Regulierer und Gemeinschaften, "*von entscheidender Bedeutung für die Wahrung des Rufs einer Organisation ...und für die Pflege der Kundentreue ist*", und somit *„letztendlich ihren Erfolg oder Misserfolg beeinflusst"*. Der Schutz der Rechte und Interessen natürlicher Personen durch den Schutz der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen kann einen erheblichen Beitrag zu diesem Schlüssel zum Erfolg leisten.

96. Wir **wiederholen insbesondere unseren Aufruf an Unternehmen, ihre Ressourcen, ihre Fähigkeiten und ihre Kreativität in die Erfindung neuer Dienste und Geschäftsmodelle fließen zu lassen, bei denen der Kontrolle über seine Daten habende Mensch im Mittelpunkt steht.**[127] Wie wir in unseren Web-Blog im Rahmen unserer Kommentare zu dem laufenden Gesetzgebungsverfahren für eine E-Privacy-Verordnung[128] im Zusammenhang mit komplexen Praktiken verhaltensorientierter Werbung und der zugrunde liegenden Technologie gesagt haben: *„Der Faktor, der den Nutzer in seiner wirksamen Kontrolle einschränkt, ist nicht die Technologie. Wenn es um die Interessen von Unternehmen geht, können wir gewaltige Anstrengungen und unglaubliche Erfolge bei der Entwicklung von Technologien feststellen."* Dieser Wandel ist von essenzieller Bedeutung, damit der Implementierung des Schutzes der Privatsphäre und des Datenschutzes durch Technikgestaltung umfassend Substanz verliehen wird.

5.2 Schutz der Privatsphäre durch Technikgestaltung als Referenzpunkt für eine wertorientierte Technologieentwicklung

97. Immer mehr Akteure und Organisationen rufen Initiativen ins Leben, mit denen das Element der sozialen und ethischen Verantwortung in der Entwicklung und Einführung von Technologien gestärkt werden soll. Zwar spielt in diesen Initiativen der Schutz der Privatsphäre eine zentrale Rolle, doch wird er häufig zusammen mit anderen Grundrechten und sozialen Zielsetzungen angestrebt.

98. Wie schon auf der Konferenz 2018 der CPDP festgestellt[129], herrscht weitgehend das Gefühl, auch beim Erfinder des Web[130] und bei Insidern der Industrie[131], dass wir möglicherweise die Kontrolle über die Technologie im Dienste der Menschheit als Gesellschaft verloren haben, und dass über die Hauptströmung der technologischen Entwicklung eher die wirtschaftlichen Interessen einiger Unternehmen entscheiden. Auf dem Spiel steht nicht einfach die Einhaltung bestehender Gesetze, auf dem Spiel stehen vielmehr die Menschenwürde[132] und unsere wesentlichen Grundfreiheiten, darunter die Grundlagen unserer demokratischen Gesellschaften. Vorherrschende Geschäftsmodelle schlagen Kapital aus der Verwendung unserer personenbezogenen Daten und aus der Konstruktion einer digitalen Darstellung, die uns und unsere Persönlichkeit auf Objekte

reduziert, die Einflussnahme und Manipulation ausgesetzt sind. Dies kann schwerwiegende Auswirkungen auf unser Leben haben, auch wenn wir gar nicht online interagieren, und ändert unsere Wahrnehmung durch andere, ändert die Wahrnehmung anderer Menschen und der Welt um uns herum durch uns, und wirkt sich auf unsere Rechte und Freiheiten aus.

99. 2015 gab der EDSB eine Stellungnahme[133] zu der notwendigen Ergänzung des regulatorischen Ansatzes durch ein digitales Ethos heraus, mit dem das Design und die Verwendung neuer Technologien im Lichte gemeinsamer menschlicher Werte unterstützt werden sollen. Der Ethik-Beirat[134], der eingesetzt wurde, hat gerade seine zweijährige Amtszeit beendet und einen Abschlussbericht veröffentlicht[135], in dem die Hauptherausforderungen für die digitale Ethik analysiert und aufgezeigt wird, in welche Richtungen zu gehen ist und wo die größten Risiken in der Zukunft liegen: Bekräftigung des Gedankens, dass die Menschenwürde im digitalen Zeitalter unantastbar bleiben sollte; dass Menschen und ihre Daten zwei untrennbar miteinander verbundene Konzepte sind; dass auf automatischem Profiling von Massendaten beruhende Entscheidungsprozesse möglicherweise mit demokratischen Gesellschaften unvereinbar sind und zu Diskriminierung führen; dass die Behandlung von Daten als Ware die Gefahr birgt, dass nicht mehr der Mensch einen Wert hat, sondern seine personenbezogenen Daten.

100. Unsere Forderung nach ethischen Grundlagen in der Technologie wird von anderen Stakeholdern geteilt, darunter Akteure im Technologiebereich, insbesondere mit Blick auf die erwartete Zunahme von Anwendungen der Künstlichen Intelligenz und auf die Rolle, die sie bei der Beeinflussung unseres Lebens in vielen Bereichen spielen kann. Im April 2016 rief das Institute of Electrical and Electronics Engineers (IEEE) eine Global Initiative on Ethics of Autonomous and Intelligent Systems[136] ins Leben, ein ehrgeiziges Projekt für Leitlinien für eine *„ethische Implementierung intelligenter Technologien“*. Ziel der Initiative ist es, *„ethische Aspekte des menschlichen Wohlergehens, die vielleicht nicht automatisch Berücksichtigung finden, in die Gestaltung und Herstellung von A/IS-Technologien einzubeziehen, und den Begriff „Erfolg“ neu zu umreißen, damit menschlicher Fortschritt auch die absichtliche Priorisierung von individuellen, gemeinschaftlichen und gesellschaftlichen ethischen Werten umfassen kann.“* Mit einem Bericht, der Beiträge von Hunderten von Teilnehmern aus der ganzen Welt umfasst, soll eine öffentliche Debatte über das Thema vorangetrieben werden. Ferner wurden Arbeitsgruppen eingerichtet, die Standards für die Berücksichtigung ethischer Erwägungen in spezifischen Kontexten entwerfen sollen, darunter Schutz der Privatsphäre und die Verarbeitung personenbezogener Daten durch autonome Systeme, die Entscheidungen ohne menschliches Zutun treffen.[137]

101. Bereits im Jahr 1989 legte die IETF ein Dokument vor[138], in dem jegliche Störung der beabsichtigten Nutzung des Internets als ethisch nicht hinnehmbar bezeichnet wurde, einschließlich der Privatsphäre der Nutzer. Im Oktober 2017 legte die IETF ausführliche Leitlinien zu einem Menschenrechtsprotokoll vor[139], das betrachtet wurde als *...der erste Meilenstein in einer längerfristig angelegten Forschungsarbeit...Das Internet ist nicht wertneutral... Mit diesem Dokument soll 1) die Beziehung zwischen Protokollen und Menschenrechten dargelegt werden; sollen 2) mögliche Leitlinien für den Schutz des Internets als eines befähigenden Umfelds für Menschenrechte in der Entwicklung künftiger Protokolle vorgeschlagen werden, ähnlich wie bei den Arbeiten im Zusammenhang mit Erwägungen des Schutzes der Privatsphäre [RFC6973]; und soll 3) sowohl in der Menschenrechtsgemeinschaft als auch in der Technikgemeinschaft das Bewusstsein für die*

Bedeutung der technischen Funktionsweise des Internets und ihre Auswirkungen auf Menschenrechte geschärft werden."

102. Initiativen zur Unterstützung des Rechts auf Schutz der Privatsphäre können als Leuchtturm für die Integration ethischer Grundsätze bei der Gestaltung des Internets und der technologieorientierten Gesellschaft für die gesamte Bandbreite der Menschenrechte dienen. Nach Auffassung des EDSB stellt das Streben nach einer wirksamen Umsetzung der Grundsätze des Schutzes der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen eine bisher nie dagewesene Möglichkeit dar, die Achtung vor der Ethik in der Technologie zu erhöhen. Alle Stakeholder tragen eine schwere Verantwortung; insbesondere Unternehmen, deren Geschäft auf der Verwendung personenbezogener Daten fußt, sowie Behörden sind aufgerufen, ihre Arbeitsweisen so zu gestalten, dass sie dem Gemeinwohl dienen.

6. Empfehlungen und Selbstverpflichtungen

103. Unser Wunsch ist es, eine vernünftige und pragmatische Debatte im Kreis der Stakeholder (politische Entscheidungsträger, Regulierer, Industrie, Wissenschaft und Zivilgesellschaft) zu fördern, damit am Ende klare und umsetzbare Entscheidungen für die Gestaltung von Technologie im Dienste der Menschen stehen. Gleichzeitig bekräftigen wir die Zusage des EDSB, für eine wirksame Umsetzung der DSGVO zu sorgen, und hier insbesondere des Grundsatzes des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Vor diesem Hintergrund ruft der EDSB alle Stakeholder auf, ihre Anstrengungen noch zu steigern.

104. Der EDSB fordert das Europäisches Parlament, den Rat und die Europäische Kommission auf,

- in dem laufenden Gesetzgebungsverfahren für eine ePrivacy-Verordnung für einen starken Schutz der Privatsphäre zu sorgen, darunter Schutz der Privatsphäre durch Technikgestaltung; auf diese Weise soll ein größerer Markt für die Privatsphäre schützende Produkte und Dienste im Kommunikationsbereich gefördert und sollen neue Marktchancen für europäische Unternehmen geschaffen werden, in denen der Schutz der Privatsphäre Teil ihrer DNS ist;

- den Schutz der Privatsphäre bei der Änderung oder Erarbeitung von Rechtsrahmen, die die Gestaltung von Technologie beeinflussen, zu unterstützen, und zwar durch stärkere Anreize und begründete Verpflichtungen, darunter angemessene Haftungsvorschriften, den Schutz der Privatsphäre durch Technikgestaltung in Produkte und Dienste zu integrieren, z. B. in den Bereichen Verkehr, Energie, Finanzen, Intelligente Städte und Internet der Dinge;

- die Einführung und Anwendung von Konzepten für den Schutz der Privatsphäre durch Technikgestaltung und von Technologien zum Schutz der Privatsphäre in der EU und auf Ebene der Mitgliedstaaten durch angemessene Durchführungsmaßnahmen und politische Initiativen zu fördern;

- eine fortgesetzte Verfügbarkeit von Kompetenzen und Ressourcen für die Forschung und Analyse im Bereich des Privacy Engineering und von Technologien zum Schutz der Privatsphäre auf EU-Ebene zu gewährleisten, entweder durch Aufrechterhaltung der

derzeitigen Kapazitäten und Aufgaben für die ENISA oder durch Zuweisung angemessener Ressourcen an andere Stellen;

- die Entwicklung neuer Praktiken und Geschäftsmodelle mithilfe der EU-Instrumente für Forschung und technologische Entwicklung zu unterstützen, mit besonderem Augenmerk auf neuen Themen wie Künstliche Intelligenz, maschinelles Lernen und Blockchain;

- politische Initiativen für EU-Einrichtungen und nationale öffentliche Verwaltungen zu unterstützen, die mit gutem Beispiel vorangehen sollen, und angemessene Vorgaben für den Schutz der Privatsphäre durch Technikgestaltung in das öffentliche Beschaffungswesen zu übernehmen, unter Berufung auf Kooperationsvereinbarungen zwischen Verwaltungen; und

- eine Bestandsaufnahme und Beobachtungsstelle für den „Stand der Technik" des Privacy Engineering und der PET und ihrer Fortschritte zu unterstützen und Bürger sowie Akteure in Wirtschaft und Politik für das Thema zu sensibilisieren.

105. Der EDSB wird auch weiterhin den Schutz der Privatsphäre durch Technikgestaltung fördern, gegebenenfalls in Zusammenarbeit mit anderen Datenschutzbehörden im EDSA. und zwar

- durch Unterstützung einer koordinierten und wirksamen Durchsetzung von Artikel 25 DSGVO und damit zusammenhängender Bestimmungen, einhergehend mit entsprechenden Sensibilisierungsmaßnahmen oder anderen unterstützenden Aktionen, und

- durch Bereitstellung von Hilfestellung für die für die Verarbeitung Verantwortlichen bei der korrekten Umsetzung des in der Rechtsgrundlage niedergelegten Grundsatzes.

106. Wir glauben, dass Koordinierung und, soweit möglich, eine Zusammenführung der in den Datenschutzbehörden vorhandenen technologischen Fähigkeiten wesentlich sind für die Förderung, Festlegung und Bewertung eines anspruchsvollen „Stands der Technik" für Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Der EDSB fordert seine Kollegen auf, im Rahmen des EDSA gemeinsam sowie in der International Working Group on Data Protection and Telecommunications[140] (IWGDPT, „Berliner Gruppe") in diese Richtung zu arbeiten.

107. Der EDSB wird direkt Initiativen und Pilotprojekte unterstützen, mit denen Privacy Engineering und PET vorangebracht werden sollen, und zwar durch Steigerung der Bekanntheit bestehender Initiativen und Förderung weiterer Koordinierung auf EU-Ebene und Zusammenarbeit auf internationaler (z. B. transatlantischer) Ebene. Von besonderer Bedeutung in diesem Zusammenhang wird das IPEN-Netzwerk sein.

108. Gemeinsam mit den Datenschutzbehörden von Österreich, Irland und Schleswig-Holstein arbeitet der EDSB an einem Wettbewerb für eine mobile App im Gesundheitsbereich, die Datenschutzgrundsätze umsetzt.

109. Mit dieser Stellungnahme wollen wir einen Beitrag zur Verankerung der allgemeinen Debatte über die Integration von Anforderungen des Schutzes der Privatsphäre und Ethik in die Gestaltung von Technologien leisten. Wir freuen uns auf Rückmeldungen zu dieser

vorläufigen Stellungnahme. Die Internationale Konferenz der Datenschutzbeauftragten 2018[141], die gemeinsam vom EDSB und der bulgarischen Datenschutzbehörde veranstaltet wird, sollte ein Meilenstein in der Diskussion über eine digitale Ethik im Allgemeinen sein und eine gute Möglichkeit bieten, das weitere Vorgehen beim Datenschutz durch Technikgestaltung genauer abzustecken, als gutes Beispiel eines werteorientierten Ansatzes für technologische Entwicklung.

Brüssel, den 31. Mai 2018

Giovanni Buttarelli

Europäischer Datenschutzbeauftragter

Endnoten

[1] Der Präsident des EP, Tajani, lädt den CEO von Facebook ein: http://www.europarl.europa.eu/news/en/agenda/briefing/2018-04-16/1/facebook-meps-to-discuss-misuse-of-eu-citizens-personal-data.

[2] Anhörung des CEO von Facebook in Ausschüssen des US-Senats: https://www.judiciary.senate.gov/imo/media/doc/04-10-18%20Zuckerberg%20Testimony.pdf.

[3] Vereinigtes Königreich, House of Commons, Digital, Culture, Media and Sports Committee: Untersuchung zu Fake News: https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/inquiries/parliament-2017/fake-news-17-19/.

[4] Deutscher Bundestag, Ausschuss Digitale Agenda, Bericht https://www.bundestag.de/presse/hib/2018_03/-/548624.

[5] Entschließung des französischen Parlaments, http://www.assemblee-nationale.fr/15/pdf/propositions/pion0858.pdf.

[6] Das im Juni 2015 veröffentliche Eurobarometer Spezial 431 erbrachte, dass mehr als 80 % der Befragten das Gefühl haben, keine vollständige Kontrolle über ihre personenbezogenen Daten zu haben. 31 % von diesen glaubten, überhaupt keine Kontrolle zu haben. (http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf) Diese Wahrnehmung wurde jüngst durch Studien anderer Organisationen bestätigt. So führte beispielsweise PwC 2017 eine Erhebung bei 2 000 Amerikanern durch: https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/cybersecurity-protect-me.html. Nur 10 % der Befragten erklärten, sie hätten den Eindruck, die vollkommene Kontrolle über ihre personenbezogenen Daten zu haben.

[7] Giovanni Buttarelli auf CNN, 5. April 2018: http://transcripts.cnn.com/TRANSCRIPTS/1804/05/qmb.91.html.

[8] EDSB, Stellungnahme 3/2018 zu Online-Manipulation und personenbezogenen Daten vom 19. März 2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_de.pdf.

[9] 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), ABl. L 119 vom 4.5.2016, S. 1.

[10] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[11] Tim Berners-Lee, Three challenges for the web, according to its inventor, Web Foundation · 12. März 2017, https://webfoundation.org/2017/03/web-turns-28-letter/.

[12] Tim Berners-Lee, The web is under threat. Join us and fight for it. Web Foundation · 12. März 2018, https://webfoundation.org/2018/03/web-birthday-29/.

[13] Daten aus einem Herzschrittmacher wurden in mindestens einer Rechtssache vor Gericht zur Überprüfung der Frage herangezogen, ob die aufgezeichneten Herzschläge zur Darstellung der Ereignisse durch den Beschuldigten passten. https://www.forensicmag.com/news/2017/02/data-suspects-pacemaker-leads-arson-insurance-fraud-charges.

[14] Es liegen umfangreiche Forschungsarbeiten zur Wirksamkeit von Umweltrechtsvorschriften vor. Die Schlussfolgerung, dass *„mit fast absoluter Sicherheit (...) Umweltvorschriften die technologischen Verbesserungen angeschoben haben, einen Anstieg der Produktionsleistung mit geringeren Emissionen ermöglicht haben“*, wird von anderen mitgetragen, z. B.von Bryan C. Williamson, Do Environmental Regulations Really Work?, in: University of Pennsylvania, The Regulatory Review, 24 November 2016, https://www.theregreview.org/2016/11/24/williamson-do-environmental-regulations-really-work/.

[15] Melvin Kranzberg, Technology and History: "Kranzberg's Laws", in : Technology and Culture, Vol. 27, No. 3 (Jul., 1986), S. 544-560.

[16] Ebenda.

[17] Siehe: https://edps.europa.eu/data-protection/our-work/ethics_de

[18] 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), ABl. L 119 vom 4.5.2016, S. 1.

[19] Siehe z. B.: Lina Jasmontaite, Irene Kamara, Gabriela Zanfir-Fortuna and Stefano Leucci, “*Implementation of Data Protection by Design and by Default: Framing guiding principles into applicable rules*” EDPL Vol. 4 (2018), forthcoming.

[20] Datenschutzbehörden und ihre Organisationen (WP 29, EDSA) werden angemessene Leitlinien zur Umsetzung der Bestimmungen der DSGVO vorlegen.

[21] Siehe beispielsweise *Tsormpatzoudi, P., Berendt, B., & Coudert, F. (2016). Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity. In B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, & S. Schiffner (Eds.), Privacy Technologies and Policy. Third Annual Privacy Forum, APF 2015. Luxembourg, Luxembourg, October 7-8, 2015. Revised Selected Papers (S. 199-212). Berlin etc.: Springer. LNCS 9484. © Springer*:

https://people.cs.kuleuven.be/~bettina.berendt/Papers/tsormpatzoudi_berendt_coudert_APF2015_with_bib_metadata.pdf.

[22] Zwei Beispiele von Lösungsvorschlägen sind in folgenden Papieren zu finden: "*Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM, 24(2):84–88, 1981*" and "*Security without identification: transaction systems to make big brother obsolete. Commun. ACM, 28(10):1030–1044, October 1985. http://doi.acm.org/10.1145/4372.4373.*".

[23] Dieses Paradigma wurde als multilaterale Sicherheit bezeichnet und ist ursprünglich zu finden in Papieren wie *„Kai Rannenberg. Recent development in information technology security evaluation – the need for evaluation criteria for multilateral security. In Richard Sizer, Louise Yngström, Henrik Kaspersen, and Simone Fischer-Hübner, editors, Security and Control of Information Technology in Society – Proceedings of the IFIP TC9/WG 9.6 Working Conference. North-Holland Publishers, 1994."*

[24] Eine der am häufigsten übernommenen Definitionen des Begriffs „Privacy Enhancing Technology" erfolgte 1995 durch Borking, Blarkom und andere, die sie bezeichnen als *„ein System von IKT-Maßnahmen zum Schutz der informationellen Privatsphäre durch Entfernen oder Minimieren personenbezogener Daten, wodurch eine unnötige oder unerwünschte Verarbeitung personenbezogener Daten verhindert wird, ohne dass die Funktionalität des Informationssystems verloren geht"*.

[25] Siehe z. B. "The Guardian - Revealed: how US and UK spy agencies defeat internet privacy and security": https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (zuletzt aufgerufen am 22.02.2018).

[26] „Die Internet Engineering Task Force (IETF) ist eine große offene internationale Gemeinschaft von Netzwerk-Designern, Betreibern, Anbietern und Forschern, die sich Gedanken über die weitere Entwicklung der Internet-Architektur und den reibungslosen Betrieb des Internets machen. Sie steht allen interessierten Personen offen" (Auszug aus der Website der IETF: https://www.ietf.org/about/who/) (zuletzt aufgerufen am 22.02.2018).

[27] "IETF news- Security and Pervasive Monitoring", 7 September 2013: https://www.ietf.org/blog/security-and-pervasive-monitoring/ (zuletzt aufgerufen am 22.02.2018).

[28] Siehe: https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf (zuletzt aufgerufen am 21.02.2018). Nachstehend die „sieben Grundprinzipien": 1. Proaktiv, nicht reaktiv, präventiv, nicht abhelfend; 2. Schutz der Privatsphäre als Standardvoreinstellung; in das Design eingebetteter Schutz der Privatsphäre; 4. Volle Funktionalität - Positive Summe, keine Nullsumme; 5. End-to-End-Sicherheit — Schutz während des gesamten Lebenszyklus; 6. Sichtbarkeit und Transparenz — Offenhalten; 7. Achtung vor der Privatsphäre des Nutzers - Nutzerzentriert halten.

[29] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995.

[30] Siehe: https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf.

[31] Die Artikel 29-Datenschutzgruppe bestand aus Vertretern der Datenschutzbehörden aller EU- und EWR-Länder. Ihre Rechtsgrundlage ist Artikel 29 der Richtlinie 95/46/EG. Sie wurde in der DSGVO durch den EDSA ersetzt.

[32] Die Stellungnahme ist einsehbar unter: https://edps.europa.eu/sites/edp/files/publication/10-03-19_trust_information_society_de.pdf.

[33] ***Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen***

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 —, 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.

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 der 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.

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.

[34] Im EU-Rechtsrahmen werden zwar die Begriffe „Privatsphäre“ und „Datenschutz“ mit unterschiedlicher Bedeutung verwendet, doch werden wir den Begriff „Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“ dahingehend verwenden, dass er auch alle Verwendungen des Ausdrucks „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“ umfasst. Wenn wir ferner von „Schutz der Privatsphäre durch Technikgestaltung“ sprechen, schließt diese Formulierung den „Schutz der Privatsphäre durch datenschutzfreundlichen Voreinstellungen“ nicht aus, sondern betont einfach nur die Dimension der „Gestaltung“.

Mit Blick auf die Charta der Grundrechte der EU bezeichnet „Privatsphäre“ in der Regel das durch Artikel 7 geschützte Recht („Achtung des Privat- und Familienlebens“), wohingegen „Datenschutz“ in Artikel 8 („Schutz personenbezogener Daten“) verwendet wird.

[35] In der DSGVO ist der Verantwortliche definiert als *„eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet...“* Siehe Artikel 4.

[36] Diese Zertifizierungsverfahren müssen auf der Grundlage von Artikel 42 genehmigt werden. Eine Auslegung dieses Artikels wurde vom Europäischen Datenschutzausschuss angenommen (siehe Artikel 70 DSGVO).

[37] In Artikel 5 sind alle Grundsätze für die Verarbeitung personenbezogener Daten aufgelistet. Sie heißen: a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz; b) Zweckbindung; c) Datenminimierung; d) Richtigkeit; e) Speicherbegrenzung: f) Integrität und Vertraulichkeit. Für weitere Einzelheiten wird auf den Artikel in seiner Gesamtheit verwiesen.

[38] In diesem Dokument werden die Begriffe „Garantie“ und „Maßnahme“ austauschbar verwendet.

[39] In der Literatur zum Thema Projektmanagement werden „die Umsetzung/der Aufbau“ des Projekts/Systems nach der Gestaltung und vor dem Betrieb sowie „die Einstellung/der Übergang“ eines Projekts/Systems nach seinem Betrieb ebenfalls als erkennbare Projektphasen mit ihren eigenen spezifischen Anforderungen bezeichnet. Dessen ungeachtet besteht kein Anlass zu der Vermutung, dass der Gesetzgeber mit seiner Erwähnung lediglich der Gestaltungs- und der operationellen Phase nicht den gesamten Lebenszyklus eines Projekts meinte.

[40] Bezüglich der zu schützenden Grundrechte und Grundfreiheiten stellt Erwägungsgrund 75 der DSGVO eine wertvolle und zuverlässige Quelle dar.

[41] Tatsächlich wird ein Beispiel zur Erläuterung des Konzepts gegeben, wenn nämlich die „Pseudonymisierung“ als eine mögliche Garantie zur Wahrung des Grundsatzes der Datenminimierung erwähnt wird.

[42] Siehe die Definition des Begriffs „betroffene Person“ in Artikel 4 Absatz 1 DSGVO.

[43] Die Grundsätze der Zweckbindung und der Datenminimierung sind Gegenstand von Artikel 4 Absatz 1 Buchstaben b bzw. c.

[44] Siehe ferner die „Stellungnahme des EDSB zum Datenschutzreformpaket“ vom 7. März 2012, insbesondere Punkt 180. Gegenstand dieser Stellungnahme war natürlich der ursprüngliche Vorschlag der Europäischen Kommission, COM(2012 211 final: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012PC0011 . Der Wortlaut des Grundsatzes des Datenschutzes durch datenschutzfreundlichen Voreinstellungen im ursprünglichen Vorschlag ist dem im endgültigen Wortlaut sehr ähnlich.

[45] Wenn ich beispielsweise eine App für Car-Sharing benutze, dann erwarte ich, dass ich mithilfe meines Standorts erfahre, wo das nächste Auto geparkt ist, und dass meine Kontaktdaten dazu dienen, sich mit mir im Zusammenhang mit dieser Dienstleistung in Verbindung zu setzen. Das heißt jedoch nicht, dass mein Standort und meine Kontaktdaten an örtliche Fahrradvermietungen weitergegeben werden sollten, und diese mir dann Werbung und Angebote zuschicken.

[46] Siehe die Definition des Begriffs „Auftragsverarbeiter“ in Artikel 4 Absatz 8 DSGVO.

[47] Siehe Artikel 28 Absatz 1 DSGVO.

[48] In einem Rechtstext stehen die „Erwägungsgründe“ vor den Artikeln („verfügender Teil“). Ihr Zweck ist es, zu den Artikeln Hintergründe darzustellen und sie zu begründen und einschlägige weitere Empfehlungen und Erläuterungen zu geben. Auch wenn nur die Artikel rechtsverbindlich sind, werden Erwägungsgründe häufig zur Auslegung des Rechts herangezogen, auch von Regulierungsstellen und Gerichten.

[49] Eine Ergänzung zu den Vorschriften von Artikel 35 DSGVO liegt vor in Form einschlägiger Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) - WP248, herausgegeben von der Artikel 29-Datenschutzgruppe und abrufbar unter http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (zuletzt aufgerufen am 20.02.2018).

[50] Zur Umsetzung dieses Konzepts siehe EDSB, „Vorläufige Leitlinien zur Dokumentierung von Verarbeitungsvorgängen für Organe, Einrichtungen und sonstige Stellen der EU“: https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en, insbesondere Teil 1.

[51] Op. cit in Endnote **Error! Bookmark not defined.**.

[52] Siehe Artikel 35 Absatz 1 und Artikel 35 Absatz 10 sowie die Erwägungsgründe 90 und 93 DSGVO.

[53] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37, geändert durch die Richtlinie 2009/136/EG.

[54] Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität. ABl. L 91 vom 7.4.1999, S. 10.

[55] Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG, ABl. L 153 vom 22.5.2014, S. 62. Wird auch als Funkanlagenrichtlinie bezeichnet.

[56] EDSB, Stellungnahme zu dem Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation (E-Privacy-VO), April 2017, S. 24. https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_de.pdf (zuletzt aufgerufen am 7. März 2018).

[57] 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), COM(2017) 10 final, 2017/0003 (COD). Dieser Vorschlag durchläuft derzeit das normale Gesetzgebungsverfahren der EU.

[58] 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, ABl. L 257 vom 28.8.2014, S. 73

[59] eIDAS-Verordnung, Artikel 12 Absatz 3 Buchstabe c.

[60] Empfehlung der Kommission 2012/148/EU vom 9. März 2012 zu Vorbereitungen für die Einführung intelligenter Messsysteme (ABl. L 73 vom 13.3.2012, S. 9):

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012H0148&from=DE (zuletzt aufgerufen am 1. März 2018).

[61] Empfehlung der Kommission 2014/724/EU vom 10. Oktober 2014 über das Muster für die Datenschutz-Folgenabschätzung für intelligente Netze und intelligente Messsysteme (ABl. L 300 vom 18.10.2014, S. 63).

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014H0724&from=DE (zuletzt aufgerufen am 1. März 2018). Die Industrie testete das DSFA-Muster zwei Jahre lang, und die Kommission nahm eine Evaluierung der Testphase vor. Derzeit wird das Muster unter Berücksichtigung der Ergebnisse der Evaluierung fertiggestellt, auch im Hinblick auf die neuen Vorgaben der DSGVO.

[62]Siehe: https://ec.europa.eu/energy/sites/ener/files/documents/bat_wp4_bref_smart-metering_systems_final_deliverable.pdf (zuletzt aufgerufen am 1. März 2018).

[63] Das BAT-Konzept stammt aus der Industrie, wo es in der Politik zur Senkung von Gasemissionen verwendet wurde. https://www.eea.europa.eu/themes/air/links/guidance-and-tools/eu-best-available-technology-reference (zuletzt aufgerufen am 1. März 2018).

[64] Siehe Endnote 28.

[65] Siehe Endnote 30.

[66] Siehe beispielsweise Vorschläge in Kanada: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/news-release/9691065 (zuletzt aufgerufen am 7. März 2018) und in Brasilien: https://iapp.org/news/a/brazilian-general-bill-on-the-protection-of-personal-data/ (zuletzt aufgerufen am 7. März 2018).

[67] Siehe z. B. das Office of the Victorian Information Commissioner: https://www.cpdp.vic.gov.au/menu-privacy/privacy-organisations/privacy-organisations-privacy-by-design (zuletzt aufgerufen am 7. März 2018).

[68] "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers": https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (zuletzt aufgerufen am 7. März 2018).

[69] Die beiden anderen sind „vereinfachte Auswahl" und „Transparenz".

[70] Remarks of Commissioner Edith Ramirez, Privacy by Design Conference, Hong Kong, June 13, 2012: https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf (zuletzt aufgerufen am 7. März 2018). Die Grundsätze für faire Informationspraktiken (Fair Information Practice Principles (FIPP)) wurden von der US-Regierung für Bundesagenturen bei der Verarbeitung von PII erlassen. Sie lassen sich kurz folgendermaßen zusammenfassen: Transparenz, Nutzungsbegrenzung, Auskunft und Berichtigung, Datenqualität und Sicherheit. Viele sehen in den FIPP die Urbausteine für Gesetze und Chartas zum Schutz der Privatsphäre, auch in der EU.

[71] Siehe Endnote 70.

[72] Siehe https://www.ftc.gov/about-ftc (zuletzt aufgerufen am 7. März 2018).

[73] Aus der in Endnote 70 zitierten Quelle: *„Nach Auffassung der FTC sind diese Konzepte beste Praktiken für Unternehmen, die sie jetzt freiwillig oder im Rahmen der Selbstregulierung übernehmen sollten. Wir haben den US-Kongress aufgefordert, umfassende Rechtsvorschriften zum Schutz der Privatsphäre zu erlassen, die sich auf die Ideen im FTC-Rahmen stützen."*

[74] "NISTIR 8062 - An Introduction to Privacy Engineering and Risk Management in Federal Systems":

https:/doi.org/10.6028/NIST.IR.8062 (zuletzt aufgerufen am 7. März 2018).

[75] Aus der Quelle in Endnote 74 : *„Im Juli 2016 gab das Office of Management and Budget (OMB) eine aktualisierte Fassung des Rundschreibens Nr. A-130 heraus, in dem Agenturen aufgefordert werden, in ihren Programmen für den Schutz der Privatsphäre den Risikomanagement-Rahmen (RMF) des NIST anzuwenden. In diesem Update des OMB wird erneut betont, dass das Management von Risiken für den Schutz der Privatsphäre über die alleinige Einhaltung von Rechtsvorschriften, Verordnungen und Richtlinien zu diesem Thema hinausgeht. Auch wenn Agenturen bereits PIA zur Minderung von Risiken für den Schutz der Privatsphäre durchführen, ist es für sie doch schwieriger, dies auf kohärente Weise zu tun, wenn es kein Modell gibt, das einen wiederholbaren und messbaren Prozess für die Beurteilung von Risiken für den Schutz der Privatsphäre ermöglicht. Wiederholbarkeit ist wichtig, damit der Prozess im Zeitverlauf immer gleich durchgeführt werden kann (wobei das Ergebnis nicht jedes Mal das gleiche sein muss). Messbarkeit ist wichtig, damit Agenturen die Wirksamkeit von Kontrollen des Schutzes der Privatsphäre bei der Bekämpfung identifizierter Risiken für den Schutz der Privatsphäre nachweisen können."*

[76] https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering.

[77] Für nähere Informationen zu den Grundsätzen für faire Informationspraktiken (FIPP) siehe Endnote 70.

[78] Siehe:
http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[79] Für einen ersten Einblick in Methodologien zur Software-Entwicklung siehe:
https://en.wikipedia.org/wiki/Software_development_process.

[80] Für einen ersten Einblick in nicht funktionale Anforderungen siehe: https://en.wikipedia.org/wiki/Non-functional_requirement (zuletzt aufgerufen am 7. März 2018).

[81] Eine Ausnahme ist der Fall, wenn der Hauptzweck des Systems das Management von Merkmalen des Schutzes der Privatsphäre ist (z. B. ein Browser-Plug-in zur Vermeidung von Tracking).

[82] "Privacy and Data Protection by Design – from policy to engineering", ENISA, December 2014: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (zuletzt aufgerufen am 7. März 2018).

[83] "Protection Goals for Privacy Engineering", Marit Hansen, Meiko Jensen and Martin Rost, 2015 IEEE CS Security and Privacy Workshops.

[84] Für einen ersten Einblick in Eigenschaften der Informationssicherheit siehe: https://en.wikipedia.org/wiki/Information_security.

[85] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management", 2010.

[86] Siehe Endnote 74.

[87] PII steht für „Personally Identifiable Information“ (Persönlich identifizierbare Informationen). In “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”, NIST Special Publication 800-122, April 2010: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf (zuletzt aufgerufen am 7. März 2018), werden PII definiert als *alle Informationen, die verwendet werden können, um die Identität eines Menschen zu unterscheiden oder nachzuvollziehen, wie Name, Sozialversicherungsnummer, Geburtsdatum und Geburtsort, Mädchenname der Mutter oder biometrische Daten; und alle anderen Informationen, die mit einer natürlichen Person verknüpft sind oder mit ihr verknüpft werden können, wie Informationen über Gesundheit, Bildung, finanzielle Lage und Beschäftigung.* PII sollten nicht mit „personenbezogenen Daten“ verwechselt werden, wie sie in Artikel 4 Absatz 1 DSGVO definiert sind.

[88] In diesem Fall sind Referenzgrundsätze die Grundsätze für faire Informationspraktiken (siehe Endnote 54).

[89] Siehe Endnote 74 in Abschnitt 3.1.1.

[90] Siehe https://distrinet.cs.kuleuven.be/software/linddun/ (zuletzt aufgerufen am 7. März 2018). Die Methodologie stammt von der DistriNet-Forschungsgruppe an der Katholischen Universität Löwen.

[91] Ein Gestaltungsmuster „bietet ein Schema für die Verfeinerung der Subsysteme oder Komponenten eines Software-Systems oder der Beziehungen zwischen ihnen. Es beschreibt eine häufig wiederkehrende Struktur von miteinander kommunizierenden Komponenten, die ein allgemeines Gestaltungsproblem in einem bestimmten Kontext löst“, wie ursprünglich in den späten 1970er Jahren definiert.

[92] Ein Beispiel für einen Katalog von Mustern ist hier zu finden: https://privacypatterns.eu (zuletzt aufgerufen am 7. März 2018).

[93] Siehe z. B. Michael Colesky, Jaap-Henk Hoepman, Christiaan Hillen, “A Critical Analysis of Privacy Design Strategies”: https://www.cs.ru.nl/~jhh/publications/iwpe-privacy-strategies.pdf (zuletzt aufgerufen am 7. März 2018).

[94] PRIPARE Handbook - Privacy and Security by Design Methodology: http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf (zuletzt aufgerufen am 7. März 2018).

[95] Datatilsynet, “Software development with Data Protection by Design and by Default”: https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/ (zuletzt aufgerufen am 7. März 2018).

[96] EDSB, „Leitlinien zum Schutz personenbezogener Daten in der IT-Governance und im IT-Management von EU-Organen“, März 2018: https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf (zuletzt aufgerufen am 7. März 2018).

[97] Siehe eine (nicht vollständige) Liste von Normungsinitiativen im Bereich Schutz der Privatsphäre in IPEN wiki: https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards#Privacy_Standards (zuletzt aufgerufen am 7. März 2018).

[98] Siehe: https://tools.ietf.org/html/rfc6973.

[99] Siehe Endnote 36.

[100] Europäische Kommission (2015) M/530 Durchführungsbeschluss der Kommission C(2015) 102 final vom 20.1.2015 über einen Normungsauftrag an die europäischen Normungsorganisationen in Bezug auf europäische Normen und europäische Normungsprodukte für Privatsphärenschutz und Personendatenschutzmanagement gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates als Unterstützung für die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates und als Unterstützung der Unionspolitik für die Sicherheitsbranche: http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548.

[101] Siehe: https://ec.europa.eu/growth/single-market/european-standards/key-players_en.

[102] Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32012R1025.

[103] Präsentation auf der CEN/CENELEC Cybersecurity Conference, 12. März 2018, A. Guarino, K. Rannenberg: ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/GUARINO_RANNENBERG_CEN-CLC_JTC8.pdf.

[104] Siehe: ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/Walter-FUMY_Chair_CEN-CLC_JTC13.pdf.

[105] Siehe ferner Kamara, I., "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'", in European Journal of Law and Technology, Vol 8, No 1, 2017: http://ejlt.org/article/view/545/723#_edn20.

[106] The Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies is awarded to outstanding Research in PETs. https://petsymposium.org/award/index.php.

[107] Siehe https://privacybydesign.foundation/en/ (IRMA-Projekt): https://privacybydesign.foundation/irma-explanation/ für eine Anwendung der Technik.

[108] Das DNT-Merkmal, implementiert in Web Clients, teilt der Website über ein Signal mit, dass der Kunde kein Tracking wünscht. Die W3C hat eine Normungsinitiative mit dem Namen Tracking Preference Expression gestartet, die zu finden ist unter: http://www.w3.org/2011/tracking-protection/.

[109] Mix Networks sind Kommunikationsprotokolle, die derart gestaltet sind, dass sie die Rückverfolgung von Absendern und Empfängern von Nachrichten stark erschweren. Siehe beispielsweise "George Danezis, University of Cambridge, Technical Report n° 594, 2004 - Designing and attacking anonymous communication systems":

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-594.pdf.

Es existiert ein Eintrag bei Wikipedia, den Sie sich vielleicht anschauen möchten: https://en.wikipedia.org/wiki/Mix_network.

[110] Siehe Endnote 82.

[111] Privacy by design in big data", ENISA, December 2015: https://www.enisa.europa.eu/publications/big-data-protection (zuletzt aufgerufen am 7. März 2018).

[112] Arbeiten der ENISA zum Thema PET sind hier zu finden: https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies (zuletzt aufgerufen am 7. März 2018).

[113] Formelle Kommentare des EDSB zum Cybersicherheitspaket, 15. Dezember 2017, https://edps.europa.eu/data-protection/our-work/publications/comments/cybersecurity-package_en.

[114] Siehe Endnote 108.

[115] Differenzieller Schutz der Privatsphäre ist ein Prozess, der in die erhobenen personenbezogenen Daten ein bisschen „Lärm" hineinbringt, so dass sie nicht mehr in Bezug zu identifizierbaren natürlichen Personen gesetzt werden können, der aber gleichzeitig bei Berechnungen (z. B. Statistiken) anhand dieser Daten eine gewisse Genauigkeit gewährleistet. Siehe ein Beispiel der Anwendung in gebräuchlichen Produkten: https://images.apple.com/privacy/docs/Differential_Privacy_Overview.pdf (zuletzt aufgerufen am 9. März 2018). Die Nennung von gewerblichen Erzeugnissen bedeutet nicht, dass der EDSB sie billigt.

[116] Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), Oktober 2016: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf (zuletzt aufgerufen am 9. März 2018).

[117] Ein Beispiel hierfür: Die IEEE hat am Rande ihres Symposium on Security & Privacy einen internationalen Workshop zu Privacy Engineering abgehalten: http://www.ieee-security.org/TC/SPW2017/IWPE/program.html (zuletzt aufgerufen am 9. März 2018).

[118] Entwurf der Stellungnahme des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres für den Ausschuss für Industrie, Forschung und Energie zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die „EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit") (COM(2017)0477–C8-0310/2017(COD)): http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-615.394&format=PDF&language=DE&secondRef=02 (zuletzt aufgerufen am 9. März 2018).

[119] Siehe: https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en (zuletzt aufgerufen am 9. März 2018).

[120]See https://fpf.org/2017/08/30/privacy-engineering-research-gdpr-trans-atlantic-initiative/ (zuletzt aufgerufen am 9. März 2018).

[121] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

[122] Siehe das Panel bei CPDP 2018: https://www.youtube.com/watch?v=3S0CV2ujIVM (zuletzt aufgerufen am 9. März 2018).

[123] Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017 http://ec.europa.eu/newsroom/document.cfm?doc_id=47559 (zuletzt aufgerufen am 9. März 2018).

[124] Der EDSB leistet seinen Beitrag in dieser Richtung insbesondere in Form der Digital Clearinghouse Initiative: https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en.

[125] Vielleicht interessiert Sie diese Reaktion auf die jüngst bekanntgewordene Facebook-Cambridge Analytica - Affaire: https://www.theguardian.com/technology/2018/apr/12/facebook-how-to-quit-delete-account-addiction-what-to-do.

[126] Den Bericht finden Sie unter: https://www2.deloitte.com/content/dam/insights/us/articles/HCTrends2018/2018-HCtrends_Rise-of-the-social-enterprise.pdf.

[127] Siehe Stellungnahme des EDSB zu Systemen für das *Personal Information Management* (Endnote 116), insbesondere Abschnitt 3.9.

[128] Siehe: https://edps.europa.eu/press-publications/press-news/blog/crucial-moment-communications-privacy_en

[129] Siehe: https://edps.europa.eu/sites/edp/files/publication/18-01-25_privacy_by_design_privacy_engineering_cpdp_en_3.pdf (zuletzt aufgerufen am 9. März 2018).

[130]Siehe z. B.: http://www.wired.co.uk/article/is-the-internet-broken-how-to-fix-it (zuletzt aufgerufen am 9. März 2018).

[131] Siehe z. B.: https://www.theguardian.com/technology/2018/jan/13/mark-zuckerberg-tech-addiction-investors-speak-up (zuletzt aufgerufen am 9. März 2018).

[132] Artikel 1 der EU-Grundrechtecharta: *„Die Würde des Menschen ist unantastbar. Sie ist zu achten und zu schützen."*

[133] Stellungnahme des EDSB, Der Weg zu einem neuen digitalen Ethos - Daten, Würde und Technologie, Dezember 2015: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_de.pdf (zuletzt aufgerufen am 9. März 2018).

[134] Siehe Endnote 26.

[135] https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf.

[136] Siehe: http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html.

[137] Siehe: https://ethicsinaction.ieee.org/.

[138] IETF RFC 1087 "Ethics and the Internet": https://tools.ietf.org/html/rfc1087.

[139] IETF RFC 8280 "Research into Human Rights Protocol Considerations": https://trac.tools.ietf.org/html/rfc8280.

[140] Arbeitsunterlagen der IWGDPT können eingesehen werden unter https://www.datenschutz-berlin.de/working-paper.html.

[141] Siehe: https://edps.europa.eu/press-publications/press-news/press-releases/2017/2018-international-conference-data-protection-0_en.