Kirsten Bock, Sebastian Meissner

Datenschutz-Schutzziele im Recht

Zum normativen Gehalt der Datenschutz-Schutzziele

Die neuen Datenschutz-Schutzziele finden zunehmend Eingang in die Datenschutzgesetze und ergänzen damit ausdrücklich und systematisch die klassischen technischen Schutzziele um die Gewährleistung des Rechts auf informationelle Selbstbestimmung. Die Autoren legen dar, wo die neuen Schutzziele bereits im Recht verankert sind und wie sie im Rahmen von Gesetzgebung, Rechtsanwendung und der Gestaltung informationstechnischer Verfahren (Privacy by Design) nutzbar gemacht werden können.

1 Einleitung

Die im Datenschutz „neuen" und elementaren Schutzziele[1] – Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit – versprechen eine systematische Verortung datenschutzrechtlicher Anforderungen im Hinblick auf technische und organisatorische Maßnahmen für Verfahren (Daten, Systeme, Prozesse)[2].[3] Dabei bleiben sie nicht bei den Datensicherheitsaspekten der Verfügbarkeit, Integrität und Vertraulichkeit stehen, sondern integrieren die spezifischen datenschutzrechtlichen Schutzziele der Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit. Sie erheben einen Vollständigkeitsanspruch, der es sowohl Entwicklern von Informationstechnologien (IT-Verfahren und Applikationen) wie auch Rechtsanwendern und dem Gesetzgeber ermöglichen soll, einen Sachverhalt datenschutzrechtlich vollständig zu erfassen *und* zu bewerten. Insoweit bilden die Schutzziele und die sie umsetzenden Maßnahmen ein verlässliches Gerüst, anhand dessen begründete Abwägungsentscheidungen in Konfliktsituationen getroffen werden können.

2 Gegenstand und Aufgabe der Schutzziele

Im Datenschutzrecht steht der Schutz des Betroffenen, nicht der einer Organisation, im Fokus. Gegenstand der Schutzziele ist daher die Umsetzung des Grundrechts auf informationelle Selbstbestimmung der natürlichen Person.[4] In dieser Aufgabe unterscheiden sie sich maßgeblich von den Schutzzielen der Datensicherheit (Verfügbarkeit, Integrität und Vertraulichkeit).[5]

Ihre Aufgabe erfüllen die Schutzziele durch eine systematische Abdeckung aller für die Umsetzung des Grundrechts auf informationelle Selbstbestimmung relevanten Aspekte. Die Umsetzung des Grundrechts leidet bislang an einer eher unsystematischen Gesetzgebung, die zudem mit der rasanten Entwicklung in der Informationsgesellschaft nicht Schritt zu halten vermag. Daraus resultieren Verunsicherungen in der Rechtsanwendung, die dazu führen, dass datenschutzrechtliche Normen weder hinreichend befolgt und durchgesetzt noch in der Verfahrensgestaltung und Softwareentwicklung berücksichtigt werden (können). Aufgabe und Versprechen der Schutzziele ist es, durch eine systematische Abdeckung aller für die Umsetzung des Grundrechts rele-

1 Grundsätzliche Ausführungen hierzu finden sich bei Rost/Pfitzmann, DuD (2009) 353-358.

2 Unter Verfahren sollen hier Daten, Systeme und Prozesse verstanden werden. Eine Legaldefinition für den Begriff des Verfahrens gibt es bislang nicht.

3 Dieser Artikel ist in engem Kontakt zu den Artikeln von Rost und Probst (beide in diesem Heft) entstanden. Rost stellt die Schutzziele im Rahmen eines generischen Datenschutzprüfmodells vor. Probst beschäftigt sich mit den Maßnahmen zur konkreten Umsetzung der Schutzziele.

4 S. dazu grundlegend Rost in diesem Heft.

5 Diese Sichtweise ist gerade in Bezug auf die Ausgestaltung informationstechnischer Verfahren und deren Risikobewertungen nicht selbstverständlich. So stellen insbesondere Verfahren zur Technikfolgenabschätzung (PIA) oder der Bewertung informationstechnischer Systeme bei der Risikobestimmung häufig nicht auf den Betroffenen, sondern auf die Sicherheit der verarbeitenden Organisation ab. Vgl. dazu z. B. ICO 2009: Privacy Impact Assessment Handbook, version 2.0 – http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/1-Chap2-2.html sowie im „Privacy Impact Assessment Guideline", der 2011 vom BSI, in Zusammenarbeit mit WU-Wien/ Spiekermann herausgegeben wurde. Beide leisten vornehmlich ein auf die Belange der jeweiligen Organisation fokussiertes Security-Impact-Assessment.

Ass. iur. Kirsten Bock

leitet das Referat EuroPriSe – Europäisches Datenschutz Gütesiegel beim Unabhängigen Landeszentrum für Datenschutz (ULD) in Kiel.

E-Mail: kbock@datenschutzzentrum.de

Ass. iur. Sebastian Meissner

ist stellvertretender Referatsleiter des EuroPriSe-Referats beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

E-Mail: smeissner@datenschutzzentrum.de

vanten Aspekte verlässliche Parameter zu schaffen, anhand derer begründete Abwägungsentscheidungen für die datenschutzkonforme Gestaltung von Verfahren und für die Auswahl von Schutzmaßnahmen getroffen werden können. Sie erlauben eine Zuspitzung und Differenzierung normativer Anforderungen und ermöglichen aufgrund ihrer höheren Spezifität die verlustfreie Thematisierung datenschutzrechtlicher Anforderungen durch Juristen und Techniker. Die Schutzziele erreichen damit eine Interoperabilität, die Recht und Technik begrifflich verbindet, ohne dass die Akteure ihre jeweilige Domäne verlassen müssen.

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten (im Folgenden „DV") steht unter einem Verbot mit Erlaubnisvorbehalt.[6] Eine DV ist daher nur zulässig, wenn sie auf einer Rechtsgrundlage beruht und deren Anforderungen erfüllt sind. Jede DV ist damit, wie auch alle anderen juristischen Entscheidungen,[7] rational zu begründen. In der Praxis ist der dabei entstehende Begründungsaufwand für die verantwortliche Stelle erheblich, weil einerseits der Gesetzgeber vielfach Regelungsgegenstände nur unzureichend und unsystematisch erfasst und Schutzbedarfe nicht hinreichend festgelegt hat und andererseits technische und organisatorische Ist-Zustände zu erfassen und zu bewerten sind. Rechtsanwender stehen vor der Aufgabe, 1. das Datenschutzrecht auf existierende oder geplante Verfahren anzuwenden und 2. die Auswahl der getroffenen Schutzmaßnahmen zu begründen. Voraussetzung dafür ist die Herstellung der Prüffähigkeit eines Verfahrens durch vollständige Erfassung aller relevanten Aspekte.

2.1 Vollständigkeitsanspruch

Die Schutzziele erheben den Anspruch, die Anforderungen des Grundrechts auf informationelle Selbstbestimmung vollständig abzubilden. Im Bereich der IT-Sicherheit sind die Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit seit langem anerkannt. Sie adressieren die Anforderungen an die Sicherheit der DV und deren Risiken primär aus der Sicht der Organisation.[8] Diese Anforderungen und Risiken sind im Datenschutzrecht, das das informationelle Ungleichgewicht zwischen dem Betroffenen und einer Organisation adressiert, aus der Sicht der Betroffenen zu bestimmen.

Das Bundesverfassungsgericht hat sich im Volkszählungsurteil grundlegend mit dem Recht auf informationelle Selbstbestimmung auseinandergesetzt und im Kern die Schutzziele beschrieben.[9] Das Schutzziel auf *Transparenz* ergibt sich aus dem Recht auf Wissen. Er wird durch das Gericht an vielen Stellen adressiert. Am bekanntesten ist der Satz: Die Betroffenen sollen „wissen können, wer was wann und bei welcher Gelegenheit über sie weiß".[10]

Die Problematik der *Nicht-Verkettbarkeit* hat das Gericht erkannt: „Entscheidend sind […] Nutzbarkeit und Verwendungsmöglichkeit [personenbezogener Daten]. Diese hängen […] von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich genommen belangloses Datum einen neuen Stellenwert bekommen."[11] „Schon angesichts der Gefahren der automatisierten Datenverarbeitung ist ein – amthilfefester – Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote erforderlich."[12] Das Gericht erkennt in diesem Zusammenhang den Grundsatz der Zweckbindung ausdrücklich an und leitet den Grundsatz der Datensparsamkeit aus der Erforderlichkeit ab.[13]

Auch das Schutzziel der *Intervenierbarkeit* wird im Volkszählungsurteil erfasst, indem das Bundesverfassungsgericht dem Einzelnen die Befugnis zuspricht „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" („informationelle Selbstbestimmung")[14]. Als Maßnahmen nennt das Gericht ausdrücklich Aufklärung, Auskunft und Löschung.[15]

Auch die Schutzrichtung der klassischen Schutzziele der Datensicherheit wird um die Betroffenenperspektive erweitert. *Verfügbarkeit* ist (auch) gegenüber den Betroffenen sicherzustellen. Nur dann können die Betroffenen von ihrem Recht Gebrauch machen. *Vertraulichkeit* ist durch „wirksame Abschottungsregelungen nach außen"[16] sicherzustellen. *Integrität* eines Verfahrens bedeutet, dass ein Verfahren so abläuft, wie es versprochen wurde. Versprochenes und Geliefertes müssen identisch sein. Betroffene müssen sich auf die ihnen zugesicherten Eigenschaften eines Verfahrens verlassen können (Vertrauenswürdigkeit): Sie haben ein Interesse daran, sich auf ein Verfahren einstellen zu können, damit sie die Nachteile und Risiken für sich vollständig überblicken können.[17]

2.2 Schutzziele als Optimierungsgebote

Als normative Gebote zeigen die Schutzziele Zielbestimmungen auf und haben insoweit Prinzipiencharakter. Sie besagen, dass etwas (z. B. Transparenz) relativ zu den rechtlichen und tatsächlichen Möglichkeiten in einem möglichst hohen Maße realisiert werden soll (Optimierungsgebot)[18]. Dabei weisen die Schutzziele als solche zwar einen hohen Grad an Generalität auf, durch ihren Bezug auf Daten, Systeme und Prozesse mit jeweils drei Schutzbedarfsgraden (normal, hoch und sehr hoch)[19] liefern sie jedoch einen gut umrissenen Kanon an Schutzmaßnahmen, die zudem, über die Prozesseigentümerschaft bzw. Rolle rechtlich an bestimmte Akteure anbindbar sind.[20] Dadurch können die konkret in Frage kommenden Maßnahmen, die sich aus den bestehenden Pflichten ergeben, unmittelbar bestimmt werden.

3 Schutzziele im geltenden Recht

Analysiert man die Vorschriften des geltenden Rechts, so lässt sich feststellen, dass die „klassischen" Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit, insbesondere aber auch die „neuen"

6 S. § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG); Art. 7 Europäische Datenschutzrichtlinie 95/46/EU (DSRL).

7 Vgl. BVerfGE 34, 269 (287), Rechtsfortbildungsbeschluß.

8 Siehe ausführlicher bei Rost in diesem Heft.

9 Freilich ohne die Schutzziele explizit zu nennen.

10 BVerfGE 65, 1, (43), Volkszählungsurteil.

11 Ibid. (45).

12 Ibid. (46).

13 Ibid. (46): „Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen."

14 Ibid. (42).

15 Ibid. (46).

16 Ibid. (49).

17 Diese Anforderung ergibt sich im Umkehrschluss auch aus der Argumentation des BVerfG. „Wer unsicher ist, ob […]", „Wer nicht mit hinreichender Sicherheit überschauen kann, welche […]" Vgl. BVerfGE 65, 1 (42f.), (45).

18 Alexy, Robert: Theorie der Grundrechte, Frankfurt a.M. 1986, S. 75.

19 Vgl. dazu Rost in diesem Heft.

20 Ausführlicher zu den Maßnahmen s. bei Probst in diesem Heft.

Schutzziele Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit (bereits) Eingang in eine Vielzahl der Bestimmungen des Datenschutzrechts gefunden haben. Dies soll nachfolgend am Beispiel der Vorschriften des Bundesdatenschutzgesetzes (BDSG) sowie der EU-Datenschutzrichtlinie 95/46/EG (DSRL) verdeutlicht werden.[21] Sofern aus Sicht des hier behandelten Themas relevant, wird auch auf einzelne Vorschriften des Entwurfs für eine Datenschutz-Grundverordnung (DS-GVO-E)[22] eingegangen.[23] Die nachfolgend verwendeten Definitionen der einzelnen Schutzziele entsprechen den einschlägigen Legaldefinitionen, wie sie erstmalig im kürzlich novellierten Landesdatenschutzgesetz Schleswig-Holstein (LDSG-SH) vollständig aufgenommen wurden.[24]

3.1 Verfügbarkeit

Verfügbarkeit ist gewährleistet, wenn Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (§ 5 Abs. 1 S. 2 N. 1 LDSG-SH).

Explizit adressiert wird das Schutzziel der Verfügbarkeit in Nr. 7 der Anlage zu § 9 Abs. 1 BDSG (Verfügbarkeitskontrolle). Danach sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Analog hierzu heißt es in Artikel 17 S. 1 DSRL, dass geeignete Maßnahmen durchzuführen sind, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung oder den zufälligen Verlust personenbezogener Daten erforderlich sind.[25]

Vergleicht man die Definition der Verfügbarkeit mit den soeben genannten Regelungen, so fällt zunächst auf, dass nur ersterer ausdrücklich auch die Verfügbarkeit von Verfahren[26] anspricht.[27] Idealerweise sollte das Recht die Verfügbarkeit von Verfahren im oben erläuterten Sinne, also von Daten, Systemen und Prozessen adressieren. Gleiches gilt für die weiteren Schutzziele, auf die im Folgenden näher eingegangen wird.

3.2 Integrität

Die Integrität von Daten ist dann sichergestellt, wenn diese unversehrt, vollständig, zurechenbar und aktuell bleiben (§ 5 Abs. 1 S. 1 Nr. 2 LDSG-SH).

Durch die Ableitung eines Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus dem allgemeinen Persönlichkeitsrecht hat das Bundesverfassungsgericht eindrucksvoll zum Ausdruck gebracht, dass die Integrität eines informationstechnischen Systems und damit auch die Integrität der hierauf gespeicherten personenbezogenen Daten ein schützenswertes (Rechts)Gut darstellt.[28]

Das Schutzziel der Integrität hat seinen Niederschlag insbesondere in Artikel 6(d) DSRL gefunden. Hiernach ist sicherzustellen, dass personenbezogene Daten sachlich richtig und, wenn nötig auf den neuesten Stand gebracht sind. Es sind zudem alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die personenbezogene Daten erhoben oder weiterverarbeitet werden, nichtzutreffende oder unvollständige Daten gelöscht oder berichtigt werden. Flankiert wird diese Bestimmung durch Artikel 17 S. 1 DSRL, wonach geeignete Maßnahmen durchzuführen sind, die für den Schutz gegen eine unberechtigte Änderung personenbezogener Daten erforderlich sind, sowie durch das in Artikel 12(b) DSRL normierte Berichtigungsrecht[29] des Betroffenen und die Pflicht zur Mitteilung einer durchgeführten Berichtigung an Dritte, denen die Daten übermittelt wurden (Art. 12(c) DSRL).[30]

Das BDSG adressiert das Schutzziel der Integrität in mehreren Nummern der Anlage zu § 9 Abs. 1. Insbesondere wird der Schutz vor Veränderung personenbezogener Daten in Nr. 3 – 5 (Zugriffs-, Weitergabe- und Eingabekontrolle) ausdrücklich angesprochen. Auch die Nr. 1 und 2 (Zutritts- und Zugangskontrolle) dienen letztlich auch dem Schutz vor unbefugter Veränderung von Daten. Das Recht des Betroffenen auf Berichtigung sowie die diesem korrespondierende Berichtigungspflicht der verantwortlichen Stelle sind in §§ 20 Abs. 1 bzw. 35 Abs. 1 BDSG geregelt, die Pflicht zur Mitteilung einer durchgeführten Berichtigung ist in §§ 20 Abs. 8 bzw. 35 Abs 7 BDSG normiert.

3.3 Vertraulichkeit

Vertraulichkeit setzt voraus, dass nur befugt auf Verfahren und Daten zugegriffen werden kann (§ 5 Abs. 1 S. 1 Nr. 3 LDSG-SH).

Die EU-Datenschutzrichtlinie enthält eine Vorschrift, die ausdrücklich mit „Vertraulichkeit der Verarbeitung" betitelt ist: Nach Artikel 16 DSRL[31] dürfen Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind und Zugang zu personenbezogenen Daten haben, sowie der Auftragsverarbeiter selbst personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten, es sei denn, es bestehen gesetzliche Verpflichtungen.

Artikel 17 S. 1 DSRL[32] schreibt hingegen vor, dass geeignete Maßnahmen zu treffen sind, die für den Schutz gegen den zufälligen Verlust, die unberechtigte Weitergabe oder den unberechtigten Zugang zu personenbezogenen Daten erforderlich sind und betrifft somit ebenfalls das Schutzziel der Vertraulichkeit.

Das Gegenstück hierzu im BDSG findet sich in den Nummern 3 – 5 (Zugriffs-, Weitergabe und Eingabekontrolle) der Anlage zu § 9 Abs. 1, welche unter anderem auch dem Schutz vor un-

21 Vereinzelt wird auch auf Vorschriften des bereichsspezifischen Datenschutzrechts eingegangen, wenn deren Regelungsinhalt ein bestimmtes Schutzziel besonders deutlich widerspiegelt.

22 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (KOM(2012) 11 endgültig).

23 Grundlegend hierzu Hornung, ZD (2012) 99-106

24 Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen vom 9. Februar 2000, zuletzt geändert durch Art. 1 G zur Änd. des LandesdatenschutzGs und des LandesverfassungsschutzG vom 11. 1. 2012 (GVOBl. Schl.-H. S. 78). Teilweise aufgenommen wurden die Schutzziele in den Landesdatenschutzgesetzen von Berlin, Hamburg und Nordrhein-Westfalen.

25 Inhaltlich deckungsgleich hierzu ist Art. 30 Abs. 2 DS-GVO-E.

26 Im LDSG-SH fehlt eine Legaldefinition.

27 Ansonsten sind die unterschiedlichen Formulierungen dem Umstand geschuldet, dass § 5 LDSG-SH das Schutzziel Verfügbarkeit und damit einen zu gewährleistenden Zustand betrifft, wohingegen Nr. 7 der Anlage zu § 9 BDSG und Artikel 17 S. 1 DSRL Maßnahmen skizzieren, die die Aufrechterhaltung dieses Zustands sicherstellen sollen. Gleiches gilt für das Verhältnis von § 5 LDSG-SH zu Vorschriften in BDSG und DSRL, die Maßnahmen zur Gewährleistung der anderen Schutzziele zum Gegenstand haben.

28 BVerfGE 120, 274.

29 Von besonderer Relevanz ist das Berichtigungsrecht im Hinblick auf das Schutzziel Intervenierbarkeit, weshalb es in diesem Zusammenhang noch näher betrachtet werden wird.

30 Inhaltlich nahezu deckungsgleiche Vorschriften zu Art. 6(d), 12(b)+(c) und 17 S. 1 DSRL finden sich in Art. 5 (d), 13, 16 und 30 Abs. 2 DS-GVO-E.

31 Eine entsprechende Vorschrift findet sich mit Artikel 27 auch in der DS-GVO-E.

32 Das Pendant hierzu findet sich in Art. 30 Abs. 2 DS-GVO-E.

befugtem Lesen, Kopieren und Entfernen dienen sollen. Auch hier gilt wieder – wie schon hinsichtlich des Schutzziels Integrität –, dass auch die Nr. 1 und 2 (Zutritts- und Zugangskontrolle) letztlich auch dem Schutz vor unbefugtem Lesen, Kopieren und Entfernen dienen sollen.

Das Bundesdatenschutzgesetz geht insofern über die Regelungen der EU-Datenschutzrichtlinie hinaus, als es explizit eine Maßnahme zur Sicherstellung der Vertraulichkeit personenbezogener Daten benennt: Gemäß S. 2 der Anlage zu § 9 BDSG kommt als eine solche (technische) Maßnahme insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren in Betracht.

§ 5 BDSG, der über die EU-rechtlichen Vorgaben des Artikels 16 DSRL hinausgeht[33], regelt das sogenannte Datengeheimnis: Danach ist es den bei der Datenverarbeitung beschäftigten Personen untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Sind diese Personen bei nicht-öffentlichen Stellen beschäftigt, so sind sie bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis[34] zu verpflichten.

Hinzuweisen ist an dieser Stelle noch auf die in Artikel 5 der EU-Daten-schutzrichtlinie für elektronische Kommunikation 2002/58/EG (DSRLeK) geregelte Vertraulichkeit der Kommunikation[35], die strafrechtliche Sanktionierung der Verletzung von Privatgeheimnissen (§ 203 StGB) sowie auf das bereits im Zusammenhang mit dem Schutzziel Integrität erwähnte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[36]

3.4 Transparenz

Transparenz ist gegeben, wenn die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann (§ 5 Abs. 1 S. 2 Nr. 4 LDSG-SH).[37]

Art. 10 f. DSRL[38] erlegen der verantwortlichen Stelle Informationspflichten gegenüber der betroffenen Person auf. Diesen entsprechen die durch den Direkterhebungsgrundsatz (§ 4 Abs. 2 BDSG) flankierte Unterrichtungspflicht des § 4 Abs. 3 BDSG sowie die Benachrichtigungspflicht der §§ 19 a Abs. 1 bzw. 33 Abs. 1 BDSG.

Die Wirksamkeit einer Einwilligung hängt davon ab, dass der Betroffene alle Informationen erhält, die notwendig sind, um Anlass, Ziel und Folgen der Verarbeitung korrekt abzuschätzen[39]: Gem. § 4a S. 2 BDSG ist er auf den vorgesehenen Zweck der Verarbeitung sowie – soweit erforderlich oder auf Verlangen – auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Art. 2(h) DSRL schreibt vor, dass eine Einwilligung[40] stets in Kenntnis der Sachlage[41] zu erfolgen hat.

Ein weiteres wichtiges Instrument zur Verwirklichung des Schutzziels Transparenz ist der Auskunftsanspruch des Betroffenen: Gem. § 34 Abs. 1 S. 1 BDSG hat die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über die zu seiner Person gespeicherten Daten und deren Herkunft, den Empfänger oder die Kategorien von Empfängern sowie den Zweck der Speicherung.[42] Das Pendant hierzu auf EU-Ebene findet sich in Art. 12(a) DSRL.[43]

Zusätzliche Beispiele für Vorschriften, die auf die Herstellung von Transparenz abzielen, sind die Regelungen zur Meldepflicht (§ 4d f. BDSG bzw. Art. 18 f. DSRL[44]) beziehungsweise zur Pflicht zur Führung eines – auf Antrag jedermann in geeigneter Weise verfügbar zu machenden – Verfahrensverzeichnisses (§ 4g Abs. 2 i. V. m. § 4e S. 1 BDSG) sowie § 6b Abs. 2 BDSG, wonach der Umstand der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (z. B. Videoüberwachung) und die verantwortliche Stelle durch geeignete Maßnahmen (z. B. Piktogramme) erkennbar zu machen sind. Schließlich ist in diesem Zusammenhang noch die Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten (engl.: personal data breach notification) zu erwähnen, die im BDSG in § 42 a geregelt ist.[45]

3.5 Nicht-Verkettbarkeit

Nicht-Verkettbarkeit[46] ist dann gewährleistet, wenn personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (§ 5 Abs. 1 S. 2 Nr. 5 LDSG-SH).

Das Bundesverfassungsgericht hat sich bereits im Volkszählungsurteil mit der Thematik der Verkettung/Verkettbarkeit verschiedener personenbezogener Daten bzw. Datensätze auseinandergesetzt.[47]

Eng verwandt mit dem Schutzziel der Nicht-Verkettbarkeit ist der sogenannte Zweckbindungsgrundsatz[48]: Nach Artikel 6(b) DSRL[49] dürfen Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweck-

33 Trotz der jeweiligen Titel „Vertraulichkeit" und „Datengeheimnis" betreffen sowohl Art. 16 als auch § 5 inhaltlich nicht nur das Schutzziel der Vertraulichkeit, sondern auch die Schutzziele Integrität (keine unbefugte Änderung), Verfügbarkeit (keine unbefugte Löschung) und Nicht-Verkettbarkeit (kein unbefugtes Verketten).

34 Dieses besteht nach § 5 S. 3 BDSG auch nach Beendigung der Tätigkeit fort.

35 Das Pendant hierzu findet sich in § 88 TKG. Grundrechtlicher Schutz wird insoweit durch Art. 10 GG bzw. Art. 7 der Charta der Grundrechte der Europäischen Union gewährleistet.

36 Siehe obige Fn. 30. Eine besondere Ausprägung des Schutzziels der Vertraulichkeit stellt das in § 203 StGB bzw. in den ärztlichen Berufsordnungen normierte Patientengeheimnis da.

37 An dieser Stelle sei darauf hingewiesen, dass die Schleswig-Holsteinische Datenschutzverordnung (DSVO-SH) detaillierte Dokumentationsanforderungen aufstellt (vgl. §§ 3 ff. DSVO-SH), durch welche das Schutzziel Transparenz gewährleistet werden soll.

38 Die Informationspflichten der verantwortlichen Stelle finden sich in Art. 14 DS-GVO-E. Sie sind gegenüber Art. 10 f. DSRL ausgeweitet worden (so muss der Betroffene bspw. über die Speicherdauer und die beabsichtigte Übermittlung von Daten in ein Drittland außerhalb der EU und des EWR informiert werden).

39 Simitis, in: Simitis, BDSG, 7. Aufl., § 4a Rn. 70.

40 Ausführlich hierzu Artikel-29-Datenschutzgruppe, Stellungnahme 15/2011 zur Definition von Einwilligung (WP 187), S. 22 ff.

41 Dieselbe Formulierung findet sich in Art. 4 Abs. 8 DS-GVO-E.

42 Relevant ist der Auskunftsanspruch auch für das Schutzziel der Intervenierbarkeit, auf das noch näher einzugehen sein wird.

43 Vgl. auch Art. 15 DS-GVO-E

44 Art. 28 DS-GVO-E führt anstelle der allgemeinen Meldepflicht gegenüber der Aufsichtsbehörde sowohl für die verantwortliche Stelle als auch für den Auftragsverarbeiter die Pflicht ein, die unter ihrer Verantwortung vollzogenen Verarbeitungsvorgänge zu dokumentieren.

45 Auf EU-Ebene findet sich eine entsprechende Vorschrift bislang lediglich in Art. 4 Abs. 3 DSRLeK. Die Informationspflicht ist bislang also auf den Telekommunikationssektor beschränkt. Art. 31 f. DS-GVO-E zufolge würde eine Informationspflicht hingegen bei jeder Verletzung des Schutzes personenbezogener Daten bestehen.

46 Grundlegend hierzu Hansen/Meissner (Hrsg.), Verkettung digitaler Identitäten, S. 19 ff.

47 Im Einzelnen s. o. unter Vollständigkeitsanspruch.

48 Gleiches gilt für den Grundsatz der Erforderlichkeit: Werden Daten erhoben, die für den jeweiligen Zweck der DV nicht erforderlich sind, so bedeutet dies regelmäßig eine Verkettung dieser Daten mit den Informationen, die zur Zweckerreichung tatsächlich benötigt werden.

49 Eine entsprechende Regelung findet sich in Art. 5(b) DS-GVO-E.

bestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Der Zweck der Verarbeitung personenbezogener Daten muss vor Beginn der Verarbeitung festgelegt und dem Betroffenen gemäß Artikel 10 f. DSRL[50] kommuniziert werden. Relevante Vorschriften im BDSG sind insoweit §§ 4 Abs. 3 S. 1 Nr. 2, 14 Abs. 2-5, 28 Abs. 2-3, 5 und 8 sowie die §§ 31 und 39. Nach Nr. 8 der Anlage zu § 9 Abs. 1 BDSG müssen geeignete Maßnahmen getroffen werden, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Darüber hinaus ist an dieser Stelle ausnahmsweise auch auf Normen des bereichsspezifischen deutschen Datenschutzrechts hinzuweisen, da sich in ihnen das Schutzziel der Nicht-Verkettbarkeit besonders deutlich widerspiegelt: Nach § 15 Abs. 3 Telemediengesetz (TMG)[51] darf der Anbieter eines Telemediendienstes für bestimmte, abschließend aufgezählte Zwecke Nutzungsprofile bei Verwendung von Pseudonymen (z. B. ID-Cookies) erstellen, jedoch dürfen die Nutzungsprofile nicht mit Daten über den Träger des Pseudonyms – wie insbesondere Name und Adresse – zusammengeführt werden.

Gemäß § 13 Abs. 4 Nr. 6 TMG hat der Diensteanbieter durch technische und organisatorische Vorkehrungen sicherzustellen, dass Nutzungsprofile nach § 15 Abs. 3 TMG nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können. Mit anderen Worten muss der Diensteanbieter also gewährleisten, dass Nutzungsprofile und identifizierende Daten über den Träger des Pseudonyms nicht miteinander verkettet werden können. Das Schutzziel der Nicht-Verkettbarkeit ist dem deutschen Recht also durchaus bereits bekannt.[52] Korrespondierende Vorschriften auf EU-Ebene gibt es bislang allerdings nicht.[53]

Maßnahmen, die auf die Gewährleistung des Schutzziels Nicht-Verkettbarkeit abzielen, sind insbesondere Vorkehrungen zur Trennung von Prozessen und IT-Systemen sowie bei Daten deren Anonymisierung und Pseudonymisierung. Nach § 3 a BDSG sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren[54], soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.[55]

Bislang finden sich im EU-Recht keine vergleichbaren Vorschriften: Zwar regelt Art. 6(e) DSRL[56], dass personenbezogene Daten nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden dürfen, die die Identifizierung der betroffenen Personen ermöglicht. In der Datenschutzrichtlinie 95/46/EG wird jedoch der Begriff des Anonymisierens lediglich in Erwägungsgrund 26, nicht aber im eigentlichen Rechtstext verwendet – den Begriff des Pseudonymisierens sucht man gar in der gesamten Richtlinie (einschließlich Erwägungsgründe) vergeblich.

Konzeptionell etwas weiter ist die aus dem Jahr 2002 datierende Datenschutzrichtlinie für elektronische Kommunikation: Ihr Erwägungsgrund 9 besagt hinsichtlich der „Einführung und Weiterentwicklung der entsprechenden Technologien", dass insoweit als Ziele insbesondere die Beschränkung der Verarbeitung personenbezogener Daten auf das erforderliche Mindestmaß und die Verwendung anonymer oder pseudonymer Daten zu berücksichtigen sind. Der Begriff des Anonymisierens wird dann auch in den Regelungen zu Verkehrs- und Standortdaten (Artikel 6 und 9 DSRLeK) verwendet, wird allerdings in der DSRLeK nicht definiert.

Leider bringt der Vorschlag der EU-Kommission für eine Datenschutz-Grundverordnung insoweit keine Verbesserung gegenüber der Datenschutzrichtlinie 95/46/EG. Es hätte nahe gelegen, in Artikel 23 Abs. 2 DS-GVO-E eine Verpflichtung zur Anonymisierung bzw. Pseudonymisierung personenbezogener Daten aufzunehmen[57] und unmissverständlich klarzustellen, dass Datenschutz durch Technik auch die Auswahl und Gestaltung von Datenverarbeitungssystemen betrifft. Zudem wäre es sinnvoll gewesen, die Begriffsbestimmungen des Artikel 4 DS-GVO-E um Legaldefinitionen der Begriffe anonymisieren und pseudonymisieren zu ergänzen. Beides ist jedoch nicht erfolgt.

3.6 Intervenierbarkeit

Das Schutzziel der Intervenierbarkeit erfordert die Gestaltung von Verfahren in einer Art und Weise, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte wirksam ermöglichen (§ 5 Abs. 1 S. 2 Nr. 6 LDSG-SH) und betrifft folglich die Operationalisierung der Ausübung von Betroffenenrechten.

Das Bundesverfassungsgericht hat wiederum in seinem Volkszählungsurteil festgestellt, dass der Gesetzgeber zur Sicherung des Rechts auf informationelle Selbstbestimmung organisatorische und verfahrensrechtliche Vorkehrungen treffen muss, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.[58] In diesem Zusammenhang hat es ausdrücklich festgestellt, dass als verfahrensrechtliche Schutzvorkehrungen (unter anderem auch) Aufklärungs-, Auskunfts- und Löschungspflichten wesentlich sind.[59] Für die anderen, insbesondere in Artikel 12 und 14 DSRL bzw. §§ 20 und 35 BDSG[60] geregelten Betroffenenrechte auf Berichtigung, Sperrung und Widerspruch kann insoweit nichts anderes gelten.[61]

Artikel 12(a) der DSRL[62] garantiert jeder betroffenen Person gegenüber der verantwortlichen Stelle ein Recht auf Auskunft über

50 Vgl. Art. 14 Abs. 1 (b) DS-GVO-E.

51 Hier sei am Rande erwähnt, dass Artikel 5 Abs. 3 DSRLeK nach Ansicht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) unmittelbar anwendbar ist, sobald Informationen im Endgerät eines Nutzers gespeichert werden bzw. auf solche Informationen zugegriffen wird (Paradebeispiel ist insoweit das Setzen bzw. Auslesen von http-Cookies). Dies ist nunmehr regelmäßig nur noch dann rechtlich zulässig, wenn der Nutzer hierin eingewilligt hat. Grund für die unmittelbare Anwendung ist, dass Artikel 5 Abs. 3 DSRLeK nicht rechtzeitig in vollem Umfang in deutsches Recht umgesetzt worden ist (insbesondere bleibt § 15 Abs. 3 TMG inhaltlich hinter den Anforderungen von Art. 5 Abs. 3 zurück). Vgl. insoweit das entsprechende Positionspapier des ULD, das abrufbar ist unter www.european-privacy-seal.eu/results/Position-Papers/ (letzter Abruf: 22.03.2012).

52 Weitere Beispiele für Regelungen, in denen sich das Schutzziel der Nicht-Verkettbarkeit niedergeschlagen hat, sind § 13 Abs. 4 Nr. 4 und 5 TMG.

53 Auch in dem Vorschlag für eine Datenschutz-Grundverordnung finden sich keine vergleichbaren Regelungen.

54 Die entsprechenden Legaldefinitionen finden sich in § 3 Abs. 6 und 6a BDSG.

55 Des Weiteren sieht § 13 Abs. 6 S. 1 TMG vor, dass der Anbieter eines Telemediendienstes dessen Nutzung und Bezahlung anonym oder unter Pseudonym ermöglichen muss, soweit dies technisch möglich und zumutbar ist.

56 Eine Art. 6(e) DSRL korrespondierende Regelung enthält Art. 5(e) DS-GVO-E.

57 Es bleibt abzuwarten, ob dies im weiteren Verlauf des Gesetzgebungsverfahrens noch in Art. 23 aufgenommen werden oder zumindest Gegenstand eines delegierten Rechtsakts der EU-Kommission sein wird.

58 BVerfGE 65, 1 (44).

59 BVerfGE 65, 1 (46).

60 Hierzu sogleich.

61 Dix, in: Simitis, BDSG, 7. Aufl., § 35 Rn. 2

62 Siehe obige Fn. 21.

die zu ihr gespeicherten Daten[63], die Zwecke, zu denen diese verarbeitet werden und die Empfänger oder Kategorien der Empfänger, an die die Daten übermittelt werden. Hierzu korrespondierende Normen finden sich im BDSG in §§ 19 und 34.

Bereits erwähnt wurden Artikel 12(b) und (c) DSRL[64]: Ersterer gibt der betroffenen Person das Recht, je nach Fall die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen der DSRL entspricht, zu verlangen. Dies gilt insbesondere für den Fall, dass die Daten unvollständig oder unrichtig sind. Ergänzend hierzu schreibt Artikel 12(c) vor, dass jede vorgenommene Berichtigung, Löschung oder Sperrung allen Dritten, denen diese Daten übermittelt wurden, mitzuteilen ist (sog. Nachberichtspflicht).[65] Die Pendants hierzu finden sich in §§ 20 und 35 BDSG. Gemäß § 6 Abs. 1 BDSG dürfen die Rechte des Betroffenen auf Auskunft, Berichtigung, Löschung oder Sperrung nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.[66]

Schließlich sei noch kurz auf das Widerspruchsrecht der betroffenen Person gemäß Artikel 14 (a) und (b) DSRL[67] bzw. §§ 20 Abs. 5, 28 Abs. 4 und 35 Abs. 5 BDSG hingewiesen.

Auch an dieser Stelle soll nochmals eine Vorschrift des bereichsspezifischen deutschen Datenschutzrechts thematisiert werden, da diese das Schutzziel der Intervenierbarkeit besonders deutlich widerspiegelt: Gem. § 13 Abs. 4 Nr. 1 TMG muss der Anbieter eines Telemediendienstes durch technische und organisatorische Vorkehrungen sicherstellen, dass der Nutzer die Nutzung des Dienstes jederzeit beenden kann.

Auf EU-Ebene finden sich bereichsspezifische Vorschriften, die zur Realisierung des Schutzziels der Intervenierbarkeit beitragen, in der Datenschutzrichtlinie für elektronische Kommunikation: So muss etwa dem Nutzer eines Telekommunikationsdienstes die Möglichkeit gegeben werden, die Rufnummernanzeige für jeden Anruf einzeln auf einfache Weise und gebührenfrei zu unterdrücken. Dies gilt unabhängig davon, ob der Nutzer selbst anruft oder angerufen wird (Artikel 8 Abs. 1 und 2 DSRLeK). Ein weiteres Beispiel ist Artikel 11 der DSRLeK, wonach jeder Teilnehmer eines Telekommunikationsdienstes die Möglichkeit haben muss, auf einfache Weise und gebührenfrei die von einer dritten Partei veranlasste automatische Anrufweiterschaltung zu seinem Endgerät abzustellen. Korrespondierende Regelungen finden sich in §§ 102 f. des deutschen Telekommunikationsgesetzes (TKG).

Ein hervorragendes Beispiel dafür, wie die Operationalisierung von Betroffenenrechten im Sinne des Schutzziels der Intervenierbarkeit rechtlich verbindlich eingefordert werden kann, stellt schließlich Artikel 12 DS-GVO-E dar: Gemäß Abs. 1 dieser Vorschrift muss die verantwortliche Stelle festlegen, mittels welcher Verfahren sie ihren Informationspflichten gegenüber dem Betroffenen nachkommt und diesem die Ausübung der ihm zustehenden Rechte (insbesondere auf Auskunft, Berichtigung, Löschung, Sperrung und Widerspruch) ermöglicht. Sie hat insbesondere Vorkehrungen zu treffen, um die Beantragung der soeben genannten Maßnahmen zu erleichtern. Im Falle der automatischen Verarbeitung personenbezogener Daten muss die verantwortliche Stelle zudem dafür sorgen, dass die jeweilige Maßnahme elektronisch beantragt werden kann.

4 Anwendung der Schutzziele

Der Vorteil der Schutzziele liegt in ihrer Anwendbarkeit sowohl für Rechtsetzungsverfahren, die Rechtsanwendung als auch für die Entwicklung informationstechnischer Verfahren und Applikationen. Bedeutung erlangen sie dabei nicht nur für den Bereich technisch-organisatorischer Maßnahmen, sondern für den gesamten Bereich der Ausgestaltung und Organisation von informationstechnischen Verfahren und Applikationen in Organisationen.

4.1 Rechtsetzung

Der Gesetzgeber ist aufgefordert insbesondere im Rahmen bereichsspezifischer Regelungen die Verwendungszwecke der zu erhebenden personenbezogenen Daten präzise zu bestimmen und nachzuweisen, dass diese Angaben für den Gesetzeszweck geeignet, erforderlich und verhältnismäßig sind.[68] Zudem sollen datenschutzrechtliche Regelungen grundsätzlich präventiv wirken.[69]

Ein Regelungsentwurf wird sich daher zwangsläufig mit den Geboten aller sechs Schutzziele auseinandersetzen müssen, um verfassungsmäßig zu sein.[70] Eine Regelung, die z. B. das Schutzziel auf Intervenierbarkeit außer Acht lässt, verschließt dem Einzelnen die Mitwirkungsmöglichkeit und Kontrolle und entspräche nicht den aus dem Volkszählungsurteil entwickelten Grundsätzen der informationellen Selbstbestimmung. Insoweit präzisiert das Schutzziel der Intervenierbarkeit für den Gesetzgeber den Auftrag, eine funktionale Steuerungsfähigkeit insbesondere auch für den Betroffenen, und nicht nur für die Organisation und ihre Prüfungsinstanz sicherzustellen.

4.2 Rechtsanwendung

Die Schwierigkeit in der datenschutzrechtlichen Beurteilung von informationstechnischen Technologien besteht in der Übersetzungsarbeit, die der Jurist zu leisten hat. Ohne weitreichendes technisches Verständnis wird es ihm kaum gelingen einen Sachverhalt zu erfassen und zu bewerten. So erfordert beispielsweise die Festlegung des jeweiligen datenschutzrechtlich Verantwortlichen im Bereich altersgerechter Assistenzsysteme (Patienten, Ärzte, Krankenkassen, Pflegedienste, Systembetreiber, etc.) eine Analyse der zugrundeliegenden technischen Verfahren und ist von der Ausgestaltung derselben abhängig.[71] Die Schutzziele ermöglichen es, einen solchen Sachverhalt über die Differenzierung an Anforderungen bzw. Beschreibungen von Verfahren (Daten, Systeme, Prozesse) zu erfassen. Die technische Verfahrensbeschreibung kann insoweit durch die Entwickler erfolgen. Der Jurist kann auf dieser Grundlage die Rollen der Beteiligten und die Schutzbedarfe festlegen. Ebenso kann der Jurist mit Hil-

63 Art. 12(b) umfasst ausdrücklich auch die sogenannte Negativauskunft, also die Bestätigung, dass es keine Verarbeitungen von personenbezogenen Daten über die den Auskunftsanspruch geltend machende Person gibt.

64 Vgl. auch obige Fn. 9.

65 Hierzu ist die verantwortliche Stelle nur dann nicht verpflichtet, wenn sich diese Mitteilung als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden ist.

66 Diese Norm geht über die Vorgaben der DSRL, die keine Regelung entsprechenden Inhalts enthält, hinaus.

67 Vgl. auch Art. 19 DS-GVO-E.

68 Vgl. BVerfGE 65, 1 (46).

69 Simitis in: Simitis Einl. Rn 16.

70 Vgl. dazu Simitis in: Simitis § 1 RN 48.

71 Vgl dazu im Detail Rost, Martin 2011: Datenschutz in 3D – Daten, Prozesse und Schutzziele in einem Modell; in: DuD – Datenschutz und Datensicherheit, 35. Jahrgang, Heft 5: 351-355.

fe der Schutzziele abstrakt Rechtmäßigkeitsanforderungen erstellen, die über die den Schutzzielen entsprechenden Maßnahmen durch den Entwickler umgesetzt werden können. Letztlich erlaubt der mit Hilfe der Schutzziele erstellte Anforderungskatalog die technisch-organisatorische Spezifikation einer Anwendung systematisch zu prüfen und zu gestalten. Audits werden so ohne größeren Aufwand ermöglicht.

4.3 Abwägungsentscheidungen

Das Recht auf informationelle Selbstbestimmung ist kein absolutes Recht. Es steht in einem Spannungsverhältnis zwischen dem Individuum und der Gemeinschaft und macht insoweit Abwägungsentscheidungen erforderlich. Art. 7(f) DS-RL sieht als Verarbeitungsgrund das berechtigte Interesse des für die Verarbeitung Verantwortlichen oder eines Dritten vor, soweit nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Eine Entsprechung findet sich im Bundesdatenschutzgesetz in § 28 Abs. 1 S. 1 Nr. 2.

Eine Norm lässt sich nur soweit erfüllen, also optimieren, wie ihr keine, ihrem Ziel widersprechenden Normen entgegenstehen. Die Feststellung und Begründung des Erfüllungsgrades einer Norm, d.h. der rechtlichen Möglichkeiten, wird im Rahmen einer Abwägungsentscheidung getroffen.[72]

Der mit einer Abwägungsentscheidung konfrontierte Rechtsanwender sollte seine Entscheidung unter Berücksichtigung der Schutzziele treffen: Sieht etwa eine Rechtsnorm vor, dass die Interessen des Betroffenen und der verantwortlichen Stelle gegeneinander abzuwägen sind, so sollte sich der Rechtsanwender die Frage stellen, welche Risiken im konkreten Fall für jedes der sechs Schutzziele bestehen und ob die identifizierten Risiken gegebenenfalls bereits durch implementierte technische oder organisatorische Maßnahmen kompensiert worden sind. Zumindest wenn erhebliche Risiken für eines oder mehrere Schutzziele verbleiben, muss die Abwägung zugunsten der Interessen des Betroffenen ausfallen (z. B. immer dann, wenn die jeweilige DV für den Betroffenen nicht hinreichend transparent ist).

5 Verfahrensentwicklung – Privacy by (Re-)Design

Bei der Entwicklung informationstechnischer Verfahren finden Datenschutzanforderungen bislang geringe oder gar keine Beachtung. Dies liegt an der Sperrigkeit datenschutzrechtlicher Normen, mit denen Entwickler wenig anzufangen wissen. Die Datenschutz-Schutzziele greifen eine für Entwickler vertraute Systematik und Sprache auf. Anders als rein juristisch entwickelte Ansätze, wie die Grundsätze des Privacy by Design,[73] sind die Datenschutz-Schutzziele über die Maßnahmen- und Schutzbedarfsanbindung für Entwickler direkt umsetzbar.[74] Schutzziele vermitteln einerseits Rechtsnormen für Verfahren mit Personenbezug und die technischen und organisatorischen Eigenschaften und Schutzmaßnahmen andererseits.

In der Praxis werden die rechtlich relevanten Merkmale eines Verfahrens und die Verfahrensbeteiligten erfasst. Maßgeblich sind dabei die zugrundeliegenden gesetzlichen oder vertraglichen Regelungen (z. B. ein Auftragsdatenverarbeitungsvertrag, Standardvertragsklauseln oder Binding Corporate Rules). Zudem ist die geplante oder bestehende Organisationsstruktur zu erfassen, die Rollen der Beteiligten zu identifizieren und Verantwortlichkeiten zu bestimmen. Neben dem Verfahrenszweck ist die Erforderlichkeit der DV zu prüfen und sind die zu verarbeitenden Datentypen einschließlich der für die Verarbeitung erforderlichen Prozesse, Applikationen und möglichen Schnittstellen zu identifizieren.

Die Abschätzung des Verfahrenszwecks und der Erforderlichkeit, sowie Möglichkeiten zur Datensparsamkeit, zur Bestimmung von Löschterminen oder zur Einholung von Einwilligungen ergeben sich nicht allein aus juristischer oder technischer Perspektive. Sie müssen immer auch fachlich beurteilt werden. Nach Klärung der rechtlich relevanten Eigenschaften können normative Abwägungen und Entscheidungen mit Hilfe der Schutzziele getroffen werden. In einer Schutzziele-Darstellung entsteht dann eine Modellierung des Verfahrens, aus dem der Betrieb sowie die theoretisch erwartbaren Schutzmaßnahmen hervorgehen.

Aus technischer Sicht ist der geplante oder Ist-Zustand des Verfahrensbetriebs für die drei Verfahrenskomponenten darzustellen. Dabei wird auch die durch die vorgefundenen Maßnahmen erzielte Intensität der Schutzwirkungen festgestellt. Dieser Ist-Zustand der Schutzmaßnahmen kann dann mit dem aus dem rechtlichen Modell ermittelten Soll-Schutzmaßnahmen abgeglichen und Mängel können identifiziert werden. Dies erlaubt eine transparente Begründung und Bewertung der Gesetzmäßigkeit eines Verfahrens, aber auch die Benennung konkreter Verbesserungsmaßnahmen.

6 Ergebnis

Das Bundesverfassungsgericht gibt mit seiner Entscheidung zum Volkszählungsurteil die Schutzziele für den Bereich des Datenschutzes vor, ohne sie jedoch begrifflich zu nennen. Mit Ausnahme einiger weniger Landesdatenschutzgesetze finden sich Aspekte der Schutzziele bislang nur verstreut in den Datenschutzgesetzen. Den Schutzzielen gelingt eine vollständige Bündelung und Systematisierung dieser Ziele, die es erlauben einen Sachverhalt datenschutzrechtlich vollständig zu erfassen und zu bewerten. Der Vorteil der Datenschutz-Schutzziele liegt zudem in ihrer universellen Anwendbarkeit sowohl aus der Perspektive der Rechtsetzung, Rechtsanwendung als auch aus Sicht der Entwicklung. Durch das von den Schutzzielen vermittelte Zusammenwirken von Recht und Technik werden Verfahren kontrollierbar.

Der Europäische Gesetzgeber bleibt aufgefordert die Schutzziele als Vorgaben für technisch-organisatorische Maßnahmen ausdrücklich aufzunehmen und für Abwägungsentscheidungen und für das Design von Informationstechnologien verbindlich zu machen.

72 Vgl. Alexy, Robert: Theorie der Grundrechte, Frankfurt a.M. 1986, S. 76.

73 The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices – http://www.privacybydesign.ca/content/uploads/2010/05/pbd-implement-7found-principles.pdf.

74 Vgl. dazu ausführlich Rost, Martin / Bock, Kirsten, 2011 Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen; in: DuD – Datenschutz und Datensicherheit, 35. Jahrgang, Heft 1: 30-34.