GERRIT HORNUNG / KORBINIAN HARTL

Datenschutz durch Marktanreize – auch in Europa?

Stand der Diskussion zu Datenschutzzertifizierung und Datenschutzaudit

Datenschutzsiegel
Prüfungsmaßstäbe
Produktzertifizierung
Garantie
Risikoanalyse

■ Im Anschluss an frühe Konzeptionen und erste gesetzliche Vorbilder u.a. in Deutschland findet sich nunmehr auch in Art. 39 des Entwurfs der EU-Kommission zu einer Datenschutzgrundverordnung (DS-GVO-E) eine Grundlage für „datenschutzspezifische Zertifizierungsverfahren" sowie zu „Datenschutzsiegeln und -zeichen". Allerdings wirft die Norm selbst eine Reihe von Fragen auf und ist im Gesetzgebungsverfahren entsprechend umstritten. Welchen Weg die Diskussion nimmt, ist sowohl für die Betroffenen als auch für die datenverarbeitende Wirtschaft von erheblicher Bedeutung. Es ist deshalb sinnvoll, sich den aktuellen Stand der Diskussion zu vergegenwärtigen; vor diesem Hintergrund ergeben sich Vorschläge insbesondere für einen höheren Detaillierungsgrad des bisherigen Entwurfs.

■ Subsequent to early conceptions and first statutory examples, among others in Germany, Art. 39 of the Draft by the EU Commission on a Data Protection Basic Regulation, there is a basis for "data specific certification procedures", as well as "data protection seals and signs". However, many questions arise from the provision itself and, thus, it is quite disputed in the legislative procedure. The path which the discussion will take is of great importance to both the parties involved, as well as the economy processing data. Thus, it makes sense to realize the discussion's current status; in view of this, suggestions arise, in particular for a more detailed version of the hitherto draft.

I. Hintergrund

Der Datenschutz des 21. Jahrhunderts ist mit Herausforderungen konfrontiert, denen das tradierte System nicht adäquat gewachsen ist. Die Fokussierung auf Abwehrmechanismen und überschaubare Datenverarbeitungsvorgänge wird Anwendungsszenarien wie dem Ubiquitous Computing[1] nicht gerecht. Ein zeitgemäßer Datenschutz kann nur durch Integration von Datenschutzkonzepten in die Technik selbst und durch entsprechende organisatorische Strategien erfolgreich sein.[2] Dabei bedarf es – i.S.e. Datenschutzes mit und nicht gegen verarbeitende Stellen – marktgestützter Verhaltensanreize zu datenschutzfreundlichem Verhalten.

Eine Möglichkeit zur Bewirkung derartiger Anreize stellen Konzepte des Audits und der Zertifizierung dar. Im Anschluss an Untersuchungen in den 1990er-Jahren[3] haben sich in Deutschland vor allem Schleswig-Holstein und Bremen zur Verabschiedung gesetzlicher Grundlagen entschieden.[4] In Schleswig-Holstein trug das *Unabhängige Landeszentrum für Datenschutz* (*ULD*) die Idee überdies mittels europäischer Verbundforschungsprojekte nach Europa.[5] Neben diesen Beispielen gibt es gerade im Online-Bereich eine Reihe sehr heterogener Datenschutz- und Datensicherheitsgütesiegel. Diesen mangelt es häufig an Bekanntheit, allgemeinen Standards, Validität, Nutzbarkeit und Anreizen für die Durchführung.[6]

Diese und andere Bestrebungen haben dazu geführt, dass die *EU-Kommission* mit Art. 39 DS-GVO-E[7] eine Norm vorschlägt, die erstmals auf europäischer Ebene eine normative Basis für entsprechende Vorhaben bieten würde. Angesichts der aktuellen Diskussion um den Entwurf insgesamt[8] und Art. 39 DS-GVO-E im Speziellen[9] bleibt allerdings abzuwarten, ob dem Vorschlag mehr Erfolg beschieden sein wird als dem 2009 in Deutschland gescheiterten Ausführungsgesetz zum Datenschutzaudit i.R.d. BDSG-Novelle.

II. Begriff und Leitziele

Mit den Begriffen des Datenschutzaudits und der Datenschutzzertifizierung werden – in wechselnder Terminologie – unterschiedliche Prozesse bezeichnet, denen die Tatsache einer Prüfung anhand datenschutzrechtlicher Kriterien gemein ist. Diese kann intern oder extern ablaufen, sich auf Produkte, Dienstleistungen, Systeme, Organisationen oder Ergebnisse von Datenverarbeitungsprozessen beziehen. Zur besseren Systematisierung sollte man unter dem Oberbegriff der „Prüfung" das Datenschutzaudit von der -zertifizierung unterscheiden. Ersteres bezieht sich auf ein Verfahren, das eine Organisation oder Organisationseinheit verwendet, und richtet sich auf die Prüfung eines Datenschutzmanagementsystems sowie die Bestätigung, dass dieses zu einer kontinuierlichen Verbesserung des Datenschutzes beiträgt.[10] Eine Zertifi-

1 Vgl. *Roßnagel/Sommerlate/Winand*, Digitale Visionen, 2008; zu den datenschutzrechtlichen Fragen s. *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007; *Kühling*, Die Verwaltung 40 (2007), 153.
2 S. mit Blick auf die Reform *Hornung*, ZD 2011, 51 ff.
3 S. zum Konzept *Roßnagel*, Datenschutzaudit. Konzeption, Durchführung, gesetzliche Regelung, 2000; s.a. *ders.*, DuD 1997, 505 ff.; jeweils auch zu Vorbildern im Ausland und in anderen Rechtsordnungen.
4 S. unter IV.3.; zu den positiven Erfahrungen s. *Bäumler*, DuD 2002, 325; *ders.*, DuD 2004, 80; *Schläger*, DuD 2004, 459.
5 Durch das Projekt „*European Privacy Seal*" (*EuroPriSe*), s. *Meissner*, DuD 2008, 525.
6 S. die Bestandsaufnahme der *ENISA*, On the security, privacy and usability of online seals, 2013; Übersicht zum existierenden Markt bei *Feik/v. Lewinski*, ZD 2014, 59.
7 KOM(2012) 11 endg.
8 Zu Stand, Kontroversen und Entwicklung *Hornung*, in: Scholz/Funk, DGRI Jahrbuch 2012, S. 1 ff.
9 *Kinast/Schröder*, ZD 2012, 207, 209; *Hornung*, Innovation 2013, 181 ff.; *Roßnagel/Richter/Nebel*, ZD 2013, 103, 106.
10 So die grundlegende Konzeption von *Roßnagel* (o. Fußn. 3), S. 65 ff.

zierung ist demgegenüber auf ein IT-Produkt oder eine Dienstleistung gerichtet.[11]

Alle Ansätze der Auditierung und Zertifizierung zielen auf die Schaffung von Marktanreizen. Eine erfolgreiche Prüfung berechtigt die datenverarbeitende Stelle, mit diesem Erfolg zu werben (Auditzeichen, Gütesiegel o.Ä.). Marktmechanismen und Wettbewerb sollen zu einer kontinuierlichen Verbesserung des Datenschutzes führen. Der ordnungsrechtliche Ansatz des Datenschutzrechts wird so um Elemente des Wettbewerbs und der Selbstregulierung ergänzt.

Im Einzelnen lassen sich dabei unterschiedliche Leitziele identifizieren.[12] Das Bewusstsein der Datenverarbeiter für ihre Selbstverantwortung wird gestärkt, wenn ihnen durch eine Zertifizierung die Eigenschaften ihres Produkt vor Augen geführt werden und sie i.R.e. Audits gezwungen werden, ein effektives Datenmanagementsystem einzurichten. Die Durchführung der Prüfungen führt zu mehr Transparenz, erleichtert so die interne und externe Datenschutzkontrolle und stärkt insbesondere betriebliche und behördliche Datenschutzbeauftragte.[13] Überdies werden interne Lernprozesse angestoßen, weil sich im Idealfall auf jeder Stufe der Organisationshierarchie die jeweils Verantwortlichen des vollen Umfangs der Datenverarbeitung und ihrer Auswirkungen bewusst werden. Durch diese Wirkungen sind Audits und Zertifizierungen (als „materielles Hauptziel")[14] auf eine Verbesserung des Datenschutzes in der konkreten Anwendungspraxis gerichtet.

III. Konzepte

Während über die Leitziele und die Grundidee „Wettbewerb als Mittel zum Zweck" Einigkeit besteht, sind Verfahren, Gegenstand, Rechtsgrundlage und Maßstab der Prüfungen unklar und umstritten.

1. Prüfungsgegenstand und -modus

Die Differenzierung zwischen der Zertifizierung (eines IT-Produkts) und der Auditierung (eines Verfahrens einer verantwortlichen Stelle) ist nicht nur terminologisch, sondern wirkt sich auch auf den Modus der Prüfung aus.

a) Zertifizierung

Die Zertifizierung hat einen statischen und objektbezogenen Charakter,[15] weil sie sich immer auf ein konkretes IT-Produkt mit seinen konkreten Eigenschaften bezieht. Schon mit einer neuen Version des Produkts kann die Zertifizierung hinfällig sein, weil zumindest geprüft werden muss, ob sich relevante Eigenschaften verändert haben. Eine Zertifizierung ist folglich nur bei Produkten sinnvoll, die eine gewisse Stabilität aufweisen. Dies gibt es auch im IT-Bereich; in bestimmten Branchen (man denke an Angebote wie soziale Netzwerke mit extrem volatilen Detailstrukturen) wird eine Durchführung aber nur um den Preis der Re-Zertifizierung in Permanenz zu haben sein. Eine zusätzliche Herausforderung ergibt sich oftmals daraus, dass die Datenschutzfreundlichkeit eines IT-Produkts auch (oder sogar maßgeblich) von seiner Einsatzumgebung abhängig ist.[16] Während Stand Alone-Systeme wie Aktenvernichter unproblematisch als solche zertifizierbar sind, wird es bei Softwarekomponenten meist auch auf die verwendete Hardware, das eingesetzte Betriebssystem und die Konfiguration der Software ankommen. Dies erfordert eine differenzierende Berücksichtigung der Unterschiede von Produkt und Einsatzumgebung in der Prüfmethodik[17] sowie die Offenlegung entsprechender Einschränkungen nach Abschluss der Zertifizierung.

Bei erfolgreicher Zertifizierung erhält der Anbieter die Möglichkeit, mit einem entsprechenden Gütesiegel für sein IT-Produkt zu werben. Dies kann sowohl auf dem Endkundenmarkt erfolgen als auch auf einem vorgelagerten Markt, wenn sich ein Endanbieter über die Datenschutzkonformität der von ihm verwendeten Komponenten vergewissern möchte.

b) Audit

Ein Datenschutzaudit i.S.e. Verfahrensaudits unterscheidet sich von der beschriebenen Zertifizierung in mehreren Punkten. Es ist nicht auf einen Zeitpunkt beschränkt, sondern auf eine fortdauernde Prüfung des Datenverarbeiters gerichtet. Es ist nicht statisch, sondern zielt auf eine kontinuierliche Verbesserung des Datenschutzes bei diesem. Indem es nicht auf ein singuläres Objekt fokussiert, sondern den Datenverarbeiter in den Blick nimmt, trägt es zu einer umfassenden „Datenschutz-Compliance" bei. Ein solches Audit wird oftmals deutlich komplexer sein als die objektbezogene Zertifizierung.

Auditgegenstand sollte die konkrete Fähigkeit eines bestimmten Verfahrens zu dynamischen Lösungen datenschutzrechtlicher Probleme sein. Ein Verfahren i.S.d. Konzeption ist „der einer übergreifenden Zielsetzung einer oder mehrerer Stellen dienende Prozess des systematischen Zusammenwirkens technisch-organisatorischer Komponenten, in dem personenbezogene Daten erhoben, verarbeitet oder genutzt werden".[18]

Auch auf dieser im Vergleich zur Produktzertifizierung höheren Abstraktionsebene einer vollumfänglichen Datenschutzkonformität besteht die Herausforderung eines sich ändernden Prüfungsgegenstands, weil Datenverarbeiter ihre Organisationsstrukturen, Abläufe und eingesetzte Technik fortlaufend verändern. Ein Verfahrensaudit muss daher (auch) als Prüfung des Datenschutzmanagements mit dem konkreten Verfahren als Bezugspunkt verstanden werden. Bewertet wird dann die Frage, ob dieses Management so im Unternehmen verankert ist, dass zum einen konkrete betriebliche oder behördliche Verfahren einen rechtskonformen Datenumgang sicherstellen, zum anderen ein kontinuierlicher Lern- und Verbesserungsprozess angeregt wird.[19] Im Idealfall wird hierdurch die dynamische, durch Marktbedingungen induzierte Veränderung der Prozesse des Datenverarbeiters in datenschutzkonforme Bahnen gelenkt.

Ein Prüfungspunkt i.R.e. Audits kann durchaus die Verwendung zertifiziert datenschutzfreundlicher Produkte durch die auditierte Stelle sein.[20] Hierdurch wird eine sinnvolle Brücke zwischen Verfahrensaudit und Produktzertifizierung geschlagen.

2. Prüfungsmaßstab

Bei Audits und Zertifizierungen stellt sich die wichtige Frage, ob sich die Prüfung auf die Einhaltung gesetzlicher Vorgaben beschränken oder mehr umfassen soll. Aus Sicht des Datenverarbeiters kann Ersteres durchaus sinnvoll sein, wenn er unsicher ist, ob er sich rechtskonform verhält oder ein bestimmtes IT-System rechtskonform einsetzbar ist.[21] Im Bereich neuer Technolo-

11 Man kann dies im Anschluss an § 9a BDSG als „Produktaudit" bezeichnen, s. *Scholz*, in: Simitis, BDSG, 7. Aufl. 2011, § 9a Rdnr. 24.
12 S. zum Folgenden für das Datenschutzaudit *Roßnagel*, in: Hempel/Krasmann/Bröckling, Sichtbarkeitsregime, 2011, 266 f.; *Scholz* (o. Fußn. 11), § 9a Rdnr. 2 ff. m.w.Nw.; s.a. Erwägungsgrund 77 DS-GVO-E.
13 Zum Einfluss der Auditierung auf die Stellung des betrieblichen Datenschutzbeauftragten s. *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 9a Rdnr. 9 ff. m.w.Nw.
14 *Roßnagel* (o. Fußn. 12), S. 266.
15 Vgl. *Roßnagel* (o. Fußn. 12), S. 267; *Scholz* (o. Fußn. 11), § 9a Rdnr. 24.
16 S. *Roßnagel* (o. Fußn. 3), S. 58; *Meissner*, DuD 2008, 525, 526; *Schläger*, DuD 2008, 459, 460.
17 *Schläger*, DuD 2008, 459, 460.
18 *Roßnagel* (o. Fußn. 12), S. 276.
19 Vgl. *Roßnagel* (o. Fußn. 3), S. 58 f.; so i.E. auch *Hammer/Schuler*, DuD 2007, 77, 79, die allerdings auf den Verfahrensbezug verzichten wollen.
20 *Roßnagel* (o. Fußn. 3), S. 141 f.
21 Für diesen Maßstab z.B. *Weichert*, in: Däubler/Klebe/Wedde/Weichert, 3. Aufl. 2010, § 9a Rdnr. 11.

gien wird dies oftmals der Fall sein – gerade wenn ihre Rechtskonformität am Maßstab offener Generalklauseln wie dem Erforderlichkeitsprinzip zu bestimmen ist.

Sieht man allerdings das maßgebliche Ziel von Audits und Zertifizierungen in der Schaffung von Marktanreizen, so können diese sich nicht auf eine bloße Prüfung der Gesetzestreue beschränken[22] – es sei denn, es handelt sich um einen Markt, auf dem die Kunden von massenhaften Rechtsbrüchen der Anbieter ausgehen und deshalb bereits die (geprüfte) Einhaltung der gesetzlichen Vorgaben einen Marktvorteil verspricht.

Verlangt man ein „Mehr" an Datenschutzfreundlichkeit, so stellt sich die Frage, nach welchem Maßstab dies beurteilt werden soll. Hierfür kommen einerseits Kriterien in Betracht, die dem Datenverarbeiter von außen vorgegeben werden, also durch Aufsichtsbehörden, Auditoren oder Branchenverbände ausgearbeitet werden.[23] Andererseits kommen individuelle Maßstäbe in Frage, die der Datenverarbeiter für sich selbst bestimmt. Diese können als zweiter Schritt auf eine Gesetzesvollzugsprüfung aufbauen und ein Datenschutz-„Plus" sein, dessen Maß der Datenverarbeiter individuell vorgibt.[24] Die zweite Lösung vermindert die Markttransparenz, da mit einem Auditzeichen kein fester Prüfungsmaßstab verbunden wird, sondern dieser im Einzelfall mittels Datenschutzerklärungen transparent gemacht und von den Kunden wahrgenommen werden muss.[25] Allerdings sind derartige individuelle Prüfungen auch ansonsten nicht unüblich, bieten Teilnahmeanreize für noch wenig datenschutzfreundliche Unternehmen und können dem Problem entgegenwirken, dass einheitliche Prüfmaßstäbe und -verfahren zu stark unterschiedlichen Belastungen für unterschiedlich große Unternehmen führen.[26]

3. Prüfstelle

Effektive Audits und Zertifizierungen benötigen fachlich kompetente und unabhängige Gutachter.[27] Um die Prüfungen bei Bedarf zeitnah durchführen zu können, bedarf es einer hinreichenden Zahl entsprechender Stellen.[28] Diese Dienstleistung kann marktförmig erbracht werden, ist in dieser Form freilich nicht ohne Risiken: Wenn private Gutachter von der Beauftragung durch den Datenverarbeiter abhängen und von diesem ihr Honorar erhalten, kann sich ein Abhängigkeitsverhältnis und der Verdacht von Gefälligkeitsprüfungen ergeben.[29] Datenschutz als Wettbewerbsvorteil setzt aber zwingend Vertrauen in die Aussagekraft eines Audit- oder Produkt-Siegels voraus, das schon bei einem Verdacht auf Vorliegen eines bezahlten Marketingmechanismus getrübt wird.

Diesem Verdacht kann mit einer staatlichen Letztkontrolle entgegengewirkt werden.[30] Dabei wird überwiegend das Modell staatlich akkreditierter Gutachter vorgeschlagen,[31] das z.B. in § 3 DSGSVO SH umgesetzt ist. Das Akkreditierungsverfahren und die Möglichkeit des Entzugs der Akkreditierung sichern das nötige Vertrauen in die Unabhängigkeit der Gutachter. Dieses Vertrauen dürfte bei einer staatlichen Akkreditierung höher sein als bei anderen Modellen (etwa einer Beteiligung der neuen *Stiftung Datenschutz*).[32] Jedenfalls kann nur die staatliche Vergabe den Gutachtern eine direkte Legitimation verschaffen, die je nach den mit dem Audit oder der Zertifizierung verbundenen Rechtsfolgen wichtig ist.

4. Rechtsfolgen

Audits und Zertifizierungen zielen auf die Schaffung von Marktanreizen, können aber auch direkt mit Rechtsfolgen verknüpft werden. Hierfür spricht, dass Marktanreizen offenbar in der Praxis Grenzen gesetzt sind. So lässt sich oftmals beobachten, dass Nutzer ein erhebliches Datenschutzinteresse bekunden, paradoxerweise bei tatsächlichen Entscheidungen dann aber doch anderen Kriterien den Vorzug geben.[33] Zertifizierte Produkte und auditierte Anbieter können z.B. im Rahmen staatlicher Vergabeentscheidungen privilegiert werden.[34] Sollte es i.R.d. aktuellen Reform zu einer Gefährdungshaftung auch für nicht-öffentliche Stellen kommen (entsprechend § 8 BDSG),[35] so könnten auditierte Anbieter hiervon ausgenommen werden, weil sie implizit den Beweis einer fehlenden Gefahrenquelle angetreten haben.[36]

Auch eine jüngst diskutierte Rechtsfolge erscheint sinnvoll: die Privilegierung i.R.e. Auftragsdatenverarbeitung. Auftraggeber stehen – insbesondere im Cloud Computing – vor dem praktischen Problem der Einhaltung ihrer Prüfpflichten aus § 11 Abs. 2 Satz 4 BDSG. Diese sind vor allem für kleine Auftraggeber, die sich faktisch in einer unterlegenen Stellung befinden, kaum zu erfüllen.[37] Hier könnten Ausnahmen für unabhängig auditierte Cloud Provider vorgesehen werden.[38] Dazu sind entsprechende Standards auszuarbeiten.[39]

Kaum möglich ist es, Anbietern Rechtssicherheit im Hinblick auf eine spätere Kontrolle durch die Aufsichtsbehörde zu verschaffen. Hierdurch würde zwar ein starker Anreiz zur Mitwirkung gesetzt. Eine Bindung der Behörde würde aber mit ihrer „völligen" Unabhängigkeit (Art. 28 Abs. 1 DS-RL) in Konflikt kommen,[40] die inzwischen auch primärrechtlich in Art. 16 Abs. 2 AEUV abgesichert ist und vom *EuGH* sehr weit ausgelegt wird.[41] Möglich sind insoweit Audits und Zertifizierungen, die die Behörde selbst durchführt oder zumindest anerkennt. Auch diese binden aber andere Aufsichtsbehörden in Deutschland und im Ausland nicht.

---

22 *Hammer/Schuler*, DuD 2007, 77, 81, i.R.d. Novelle 2009 wurde dieser „Minimalmaßstab" als bloße bürokratische Verdoppelung der allgemeinen Pflicht abgelehnt, Gesetze einzuhalten, s. *Grentzenberg/Schreibauer/Schuppert*, K&R 2009, 535, 542 und unter II.2.

23 Denkbar sind auch Mischmodelle und die Beteiligung weiterer Institutionen wie Verbraucherschutzverbände, Stiftungen (etwa die *Stiftung Datenschutz*, jedenfalls mit beratender Funktion) etc.

24 So das Konzept von *Roßnagel* (o. Fußn. 3), S. 85 ff.; mit anderer Terminologie *Hammer/Schuler*, DuD 2007, 77, 81.

25 Zum Problem einer „Zerfaserung" des Zertifikats auch *Hammer/Schuler*, DuD 2007, 77, 78 f.

26 Auch dies war 2009 einer der Kritikpunkte, s. *Grentzenberg/Schreibauer/Schuppert*, K&R 2009, 535, 542 m.w.Nw.; zum Vorteil der Skalierbarkeit *Hammer/Schuler*, DuD 2007, 77, 78 f.

27 S. z.B. *Roßnagel*, DuD 1997, 505, 514; *Schläger*, DuD 2004, 459.

28 *AG Rechtsrahmen des Cloud Computing*, Datenschutzrechtliche Lösungen für Cloud Computing, 2012, S. 17.

29 *Scholz* (o. Fußn. 11), § 9a Rdnr. 11; allgemein für Sachverständigen-Vollzugsmodelle im Technikrecht *Windmann*, DÖV 2010, 396, 401 f.

30 Denkbar wäre auch ein Modell, das die prüfende Stelle für fehlerhafte Audits und Zertifizierungen in Haftung nimmt. Im Hinblick auf Beweisschwierigkeiten und ein wenig ausgeprägtes Haftungsrecht im Datenschutzrecht erscheint dies aber wenig praktikabel, s. *AG Rechtsrahmen des Cloud Computing*, (o. Fußn. 28), S. 17.

31 S. in Anlehnung an das Umweltschutzaudit *Roßnagel* (o. Fußn. 3), S. 112; *Schläger*, DuD 2004, 459.

32 Krit. zur direkten Wahrnehmung von Akkreditierungsaufgaben durch die Stiftung *Bräutigam/v. Sonnleithner*, AnwBl 2011, 240, 242.

33 S. *Hornung*, in: Hill/Schliesky, Die Neubestimmung der Privatheit, S. 146 ff. für das Beispiel sozialer Netzwerke.

34 So in Bremen, Mecklenburg-Vorpommern und Schleswig-Holstein, s. unter IV.3.

35 S. zu diesem Vorschlag *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, S. 181.

36 *Roßnagel* (o. Fußn. 12), S. 274.

37 *Hornung/Sädtler*, CR 2012, 638, 643; *AG Rechtsrahmen des Cloud Computing* (o. Fußn. 28), S. 12 ff.

38 Derartige Privilegierungen gibt es de lege lata nicht, sodass bestehende private Prüfsiegel zur Auftragsdatenverarbeitung mit dem Makel fehlender Rechtssicherheit behaftet sind, s. *Borges/Brennscheidt*, in: Borges/Schwenk, Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce, 2013, S. 68.

39 S. z.B. *AG Rechtsrahmen des Cloud Computing* (o. Fußn. 28); ein aktueller Standard (nebst Siegel) wurde 2013 durch *GDD* und *BvD* entwickelt (*Lepperhoff/Jaspers*, MMR 2013, 617) und mit dem *LfDI NRW*, DuD 2014, 6, abgestimmt; näher www.dsz-audit.de/.

40 S. *Wagner*, RDV 2011, 229, 232; *Scholz* (o. Fußn. 11), § 9a Rdnr. 15 ff.

41 *EuGH* MMR 2010, 352 m. Anm. *Petri/Tinnefeld*.

IV. Instrumente de lege lata

Derzeit existieren nur wenige normative Ansätze für Datenschutzaudits und -zertifizierungen.

1. Gemeinschaftsrechtliche Ebene

Auf europäischer Ebene fehlen bisher entsprechende Regelungen. Generell ist der gesamte Bereich „Datenschutz durch Technik" weder verfahrens- noch materiellrechtlich wirklich ausgestaltet.[42] Art. 27 DS-RL gibt (ohne detaillierte Regelung) die Erarbeitung bereichsbezogener Verhaltensregeln vor, die die Durchführung der Vorgaben der DS-RL erleichtern sollen. Forderungen der *Art. 29-Datenschutzgruppe* nach mehr tatsächlichen Datenschutzmaßnahmen enthalten unter dem Stichwort der „accountability"[43] das Konzept der Auditierung,[44] aber kein detailliertes Konzept, sondern nur allgemeine Programmvorschläge. Die *Kommission* hat diese Vorschläge aufgegriffen und bezeichnet sie als grundsätzliche Leitziele ihrer Reform.[45]

2. Die Diskussion und das Scheitern auf Bundesebene

Die Idee eines Audits als neues Steuerungsinstrument im Datenschutzrecht geht in die 1990er-Jahre zurück. Anknüpfend an das europarechtlich vorgegebene Umweltschutzaudit entwickelte die *Projektgruppe verfassungsverträgliche Technikgestaltung* (*provet*) ein Audit-Konzept, das 1997 in § 17 MDStV und 2001 in § 9a BDSG mündete,[46] der als Programmnorm ein Bundesauditgesetz ankündigt. § 9a Satz 1 BDSG stellt Weichen hinsichtlich der Adressaten und des Audit-Gegenstands (Zweiteilung in Produkt- und Verfahrensaudit; in hiesiger Terminologie also Zertifizierungen und Audits); jedoch ist dieses „Grobkonzept" für den Bundesgesetzgeber nicht bindend. Ein Auditgesetz würde schon nach dem lex posterior-Grundsatz, als Spezialgesetz aber auch nach § 1 Abs. 3 Satz 1 BDSG den Regelungen des BDSG vorgehen.[47]

Die mit § 9a BDSG verbundene Hoffnung zumindest einer „politischen Bindungswirkung"[48] hat sich bislang nicht bewahrheitet. Obwohl das Konzept auf breite Zustimmung der Fachwelt stieß,[49] scheiterten im Folgenden alle Umsetzungsversuche. Ein Referentenentwurf von 2007 sah die Zertifizierung durch private Gutachter bei Einhaltung der gesetzlichen Datenschutzvorschriften vor; er stieß auf weitgehende Ablehnung.[50] Eine überarbeitete Fassung sollte 2009 als Teil der Novellierung des BDSG beschlossen werden.[51] Sie sah die Befugnis zum Führen eines Audit-Siegels vor, wenn dies beim *Bundesbeauftragten für Datenschutz und Informationsfreiheit* angezeigt wurde; geregelt war lediglich eine ex post-Kontrolle durch private zertifizierte Kontrollstellen. Als Kontrollmaßstab war neben der Einhaltung der gesetzlichen Vorschriften auch die von Richtlinien eines zu bildenden Datenschutzausschusses vorgesehen. Nach Kritik aus dem *Bundesrat* (zu bürokratische, kostenträchtige und intransparente Umsetzung)[52] und der Fachwelt wurde das Datenschutzauditgesetz aus der Endfassung der Novelle gestrichen. Während teilweise Unverständnis über diesen Schritt geäußert und Lobbyismus von Wirtschaftsverbänden als Mitursache vermutet wurde,[53] verwiesen andere Autoren auf „fundamentale Kritik" seitens der Fachwelt.[54] So wurde die Möglichkeit, das Siegel bereits vorab zu führen, als vertrauensmindernd bemängelt. Die Bestätigung bloßer Gesetzestreue, ein zu hoher Aufwand für kleine und mittlere Unternehmen und die enge nationale Perspektive kamen hinzu.[55]

3. Landesrecht

In Brandenburg und Nordrhein-Westfalen ist ein Datenschutzaudit formell im Gesetz angelegt,[56] wie im Bund fehlt es aber an Ausführungsgesetzen.[57] Mecklenburg-Vorpommern regelt Prüfverfahren, die im Benehmen mit dem Landesdatenschutzbeauftragten durchzuführen sind; Kriterien werden aber nicht angegeben.[58] Bremen und Schleswig-Holstein verfügen demgegenüber neben einer Erwähnung im LDSG über Verordnungsermächtigungen,[59] von denen die Landesregierungen auch Gebrauch gemacht haben.[60]

Beide Landesgesetze enthalten – neben der Möglichkeit für öffentliche Stellen, sich einem freiwilligen Behördenaudit zu unterwerfen[61] – überdies die Vorgabe, dass Verfahren und technische Einrichtungen (Bremen) bzw. Produkte (Schleswig-Holstein), deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde, durch die Landesbehörden „vorrangig" eingesetzt werden sollen. Entscheidender Unterschied ist, dass die BremDSAuditV keine Möglichkeit für Anbieter enthält, eine derartige Prüfung durchzuführen.[62] Die Pflicht zum vorrangigen Einsatz geprüft datenschutzfreundlicher Produkte setzt damit zwar einen Marktanreiz; dieser kann aber nur wirksam werden, wenn entsprechende Prüfverfahren anderweitig verfügbar sind.[63]

Im Gegensatz dazu vergibt das *ULD Schleswig-Holstein* auf Basis der DSGSVO SH ein Gütesiegel für „IT-Produkte" auch an private Datenverarbeiter. Zusammen mit mehreren europäischen Partnern ist dieses Projekt zum *European Privacy Seal* (*EuroPriSe*) erweitert worden.[64]

V. Audits und Zertifizierungen in der DS-GVO

Wie andere kontroverse Fragen des Datenschutzrechts wird auch die von Audits und Zertifizierungen durch die europäische Reform entschieden werden. Diese ist zwar ins Stocken geraten, wird aber mutmaßlich nach der Europawahl wieder aufgenommen werden.

---

42 *Hornung*, ZD 2011, 51, 53.
43 Zu diesem noch nicht völlig klaren Konzept s. *Art. 29-Datenschutzgruppe*, WP 173, Opinion 3/2010 on the principle of accountability; s.a. *Hornung*, Innovation 2013, 181, 188 f.
44 Vgl. *Art. 29-Datenschutzgruppe* (o. Fußn. 43), S. 9 und vor allem 17 ff.
45 S. KOM(2010) 609 endg., S. 12 f.
46 S. *Roßnagel* (o. Fußn. 12), S. 275.
47 *Scholz* (o. Fußn. 11), § 9a Rdnr. 40.
48 *Roßnagel* (o. Fußn. 3), S. 140.
49 S. *Scholz* (o. Fußn. 11), § 9a Rdnr. 8 m.w.Nw.
50 S. *Roßnagel* (o. Fußn. 12), S. 276; exemplarisch die Stellungnahme des *DVD e.V.*: *Schuler*, DANA 2007, 181, 182: „Es ist daher fragwürdig, ... das freiwillige Zertifikat bereits für bloße Gesetzeseinhaltung zu erteilen. Das würde bedeuten, dass man ein Zertifikat dafür erteilt, dass jemand keinen Gesetzesverstoß begeht (!). Unabhängig von der falschen Botschaft ist ein Wert für Verbraucher so nicht zu erzielen."
51 BT-Drs. 16/12011.
52 BT-Drs. 16/12011, S. 38.
53 *Roßnagel* (o. Fußn. 12), S. 277.
54 *Grentzenberg/Schreibauer/Schuppert*, K&R 2009, 535, 542 m.w.Nw.
55 Vgl. o. Fußn. 55.
56 Vgl. die wortgleichen § 11c BbgDSG und § 10a DSG NW.
57 Krit. für NRW *Zilkens/Kohlhause*, ZD 2012, 119, 121 (dort Fußn. 40).
58 S. § 5 Abs. 2 DSG-MV.
59 § 7b Abs. 1 Satz 2 BremDSG; § 4 Abs. 2 Satz 2 LDSG SH.
60 Bremische Datenschutzauditverordnung (BremDSAuditV); Datenschutzgütesiegelverordnung (bis Ende 2013: Datenschutzauditverordnung) Schleswig Holstein (DSGSVO SH).
61 Dieses bezieht sich auf die „technischen und organisatorischen Maßnahmen bei der Verarbeitung personenbezogener Daten sowie die datenschutzrechtliche Zulässigkeit der Datenverarbeitung" (§ 43 Abs. 2 LDSG SH) der öffentlichen Stelle bzw. „ihre Verfahren sowie ihre technischen Einrichtungen" (§ 7b BremDSG).
62 § 7b Abs. 1 BremDSG, § 1 BremDSAuditV begrenzen die Antragsteller auf öffentliche Stellen.
63 Sie müssen zudem den Anforderungen der BremDSAuditV entsprechen (§ 7b Abs. 2 BremDSG).
64 www.european-privacy-seal.eu, vgl. *Bock*, DuD 2008, 712; seit dem 1.1.2014 hat die *EuroPriSe GmbH* die Audit-Administration vom *ULD* übernommen. Ein „advisory board", dem auch das *ULD* angehört, soll den Erhalt der bewährten Standards garantieren; näher *Meissner*, DuD 2014, 153.

1. Inhalt der Entwürfe

a) Der Kommissionsentwurf

Im Gegensatz zur DS-RL nimmt der Kommissionsentwurf die Idee von Audit und Zertifizierung auf.[65] Nach Art. 39 Abs. 1 DS-GVO-E „fördern" Mitgliedstaaten und Kommission „die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -zeichen". Diese dienen der Transparenz des gewährleisteten Datenschutzniveaus und der ordnungsgemäßen Anwendung der Verordnung; sie sollen den Besonderheiten einzelner Sektoren und Verarbeitungsprozesse Rechnung tragen.

Anforderungen, Kriterien und Standards für die Prüfverfahren bleiben hingegen ebenso offen wie die Fragen von Prüfstellen und Rechtsfolgen. Allerdings hätte die Norm durchaus eine rechtliche Wirkung. Anders als § 9a BDSG, aber vergleichbar mit § 7b Abs. 1 Satz 2 BremDSG und § 4 Abs. 2 Satz 2 LDSG SH, verlagert der Entwurf die weitere Ausführung. Die *Kommission* wird ermächtig, im Rahmen delegierter Rechtsakte Kriterien und Anforderungen für das Zertifizierungs- und Auditverfahren einschließlich Erteilung, Entzug und Anerkennung festzulegen (Art. 39 Abs. 2 DS-GVO-E), sowie mittels Durchführungsrechtsakten technische Standards für Zertifizierungen und Audits und Verfahren zu ihrer Förderung und Anerkennung festzulegen (Art. 39 Abs. 3 DS-GVO-E).

b) Der Entwurf des Europäischen Parlaments

Bereits der Berichtsentwurf von MdEP *Albrecht* ergänzte den Kommissionsentwurf um weitergehende Kriterien und die Mitwirkung des *Europäischen Datenschutzausschusses* (*EDA*).[66] Der *LIBE-Ausschuss des Parlaments* hat diesen Ansatz weitergeführt und eine im Vergleich zum Kommissionsentwurf weit detailreichere Neufassung des Art. 39 entworfen.[67] Der *LIBE*-Entwurf wurde im *Europäischen Parlament* (im Folgenden: *EP*-Entwurf) am 12.3.2014 mit großer Mehrheit angenommen.

Verantwortlichen Stellen und Auftragsverarbeitern soll es danach – i.R.e. freiwilligen, erschwinglichen, transparenten und nicht unangemessen aufwändigen Prozesses (Art. 39 Abs. 1b) – möglich sein, ein „European Data Protection Seal" zu erhalten (Abs. 1e). Die Regelung des Prüfungsgegenstands ist widersprüchlich: Nach Abs. 1a und Abs. 1e wird die Datenverarbeitung selbst geprüft (also wohl i.S.e. Verfahrensaudits),[68] nach Erwägungsgrund 77 dagegen Produkte und Dienstleistungen.

Prüfungsmaßstab ist die Einhaltung der Verordnung.[69] Ein „Plus" an Datenschutz wird nicht verlangt. Eine Bestätigung eines besonders datenschutzfreundlichen Standards dürfte wegen des unmittelbaren und abschließenden Charakters der Verordnung wohl noch nicht einmal möglich sein. Die Siegel gelten nur, solange die Verordnungsvorgaben erfüllt werden (Abs. 1f), maximal jedoch fünf Jahre (Abs. 1g). Sie werden in einem öffentlichen elektronischen Register geführt (Abs. 1h).

Als Prüfstelle sieht der *EP*-Entwurf grundsätzlich die Aufsichtsbehörden vor. Der Einsatz unabhängiger akkreditierter Gutachter ist möglich, aber keine Pflicht (Abs. 1d). Das Prüfsiegel wird nach Abs. 1d Satz 4 in jedem Fall durch die Behörde vergeben. Bemerkenswert erscheint, dass nach Abs. 1a jeder Datenverarbeiter bei jeder beliebigen Behörde in der Union eine Prüfung beantragen kann. Um der Gefahr eines Unterbietungswettbewerbs entgegenzuwirken, werden die Aufsichtsbehörden und der *EDA* nach Abs. 1c verpflichtet, i.R.d. Konsistenzmechanismus zusammenzuarbeiten, um eine einheitliche Prüfung einschließlich einheitlicher Gebühren in der Union zu garantieren.

Daneben stärkt der *EP*-Entwurf die Rolle des *EDA*. Dieser kann nach Abs. 2a in eigener Initiative einem „data protection-enhancing technical standard" bescheinigen, die Anforderungen der Verordnung zu erfüllen. Überdies wird die *Kommission* verpflichtet, i.R.d. delegierten Rechtsakte den *EDA* und weitere Beteiligte aus Industrie und Zivilgesellschaft anzuhören; die Befugnis zur Verabschiedung von Durchführungsrechtsakten in Abs. 3 des Kommissionsentwurfs wurde gestrichen. Die Anforderungen der delegierten Rechtsakte müssen nach Abs. 3 Satz 2 des *EP*-Entwurfs ausdrücklich von den Betroffenen durchgesetzt werden können.

Auf Rechtsfolgenseite führt die erfolgreiche Auditierung zu einer Privilegierung im Rahmen aufsichtsbehördlicher Sanktionen für Datenschutzverstöße. Während grundsätzlich ein objektiver Haftungsmaßstab gilt, soll nach Art. 79 Abs. 2b des *EP*-Entwurfs ein erfolgreich auditiertes Unternehmen nur bei Verschulden mit Bußgeldern belegt werden können.

Von potenziell enormer Bedeutung ist daneben eine weitere neue Rechtsfolge des *EP*-Entwurfs: Ein gültiges Siegel soll eine „geeignete Garantie" zum Schutz personenbezogener Daten darstellen und dementsprechend nach Art. 42 Abs. 1 und Abs. 2 eine Datenübermittlung in Drittstaaten auch dann legitimieren, wenn für diese kein Angemessenheitsbeschluss der *Kommission* nach Art. 41 vorliegt. Erforderlich ist, dass sowohl die verantwortliche Stelle innerhalb der Union als auch der Datenempfänger über ein Siegel verfügen.

2. Beurteilung der Verordnungsentwürfe

Auf der Basis des *EP*-Entwurfs ist nunmehr eine deutlich bessere Beurteilung der europäischen Reform möglich, als dies für den sehr vagen Vorschlag der *Kommission* der Fall war.

a) Detaillierungsgrad

Zunächst ist der verbesserte Detaillierungsgrad des *EP*-Entwurfs hervorzugeben.[70] Dieser schafft erheblich mehr Klarheit für Datenverarbeiter und Betroffene und beugt der Gefahr vor, dass die *Kommission* i.R.d. tertiären Rechtssetzung lediglich unverbindliche Förderungsmaßnahmen beschließt. Auch die erläuterten Rechtsfolgen einer erfolgreichen Auditierung und Zertifizierung hätte die *Kommission* nicht anordnen können.

Schließlich beugen die exakteren Normen und die Beschränkung der Kommissionsbefugnisse der Gefahr vor, dass die Regelung gegen Art. 290 Abs. 1 Unterabs. 1 AEUV verstößt, wonach sich delegierte Rechtsakte auf „nicht wesentliche Vorschriften" des Gesetzgebungsakts beschränken müssen. Hierfür gelten zwar nicht die Maßstäbe der deutschen Wesentlichkeitslehre, sondern es kommt darauf an, ob Fragen der „grundsätzlichen Ausrichtung der Gemeinschaftspolitik" betroffen sind.[71] Das mag man für den ursprünglichen Art. 39 DS-GVO-E verneinen (und die Kommissionsbefugnisse für zulässig erachten), weil Au-

65 Art. 39 DS-GVO-E verwendet den Begriff des Audits nicht, regelt diese der Sache nach aber ebenfalls.

66 A7-0402/2013.

67 S. B. v. 21.10.2013; eine deutsche Fassung besteht bislang nicht; eine inoffizielle konsolidierte Fassung ist abrufbar unter: http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf.

68 Nach Abs. 1a ist „the processing of personal data" der Prüfungsgegenstand; nach Abs. 1e wird bestätigt, dass „they [die Datenverarbeiter] process personal data in compliance...".

69 Abs. 1a und Abs. 1e beziehen sich (nur) auf die Verarbeitung „in compliance" mit der Verordnung.

70 S. schon zuvor *Roßnagel/Richter/Nebel*, ZD 2013, 103, 106; *Hornung*, Innovation 2013, 181, 186 ff.

71 *EuGH* Slg. 1992, I-5383 Rdnr. 37 – Deutschland/Kommission; es kommt also nicht auf die Grundrechtsrelevanz eines Rechtsakts, sondern auf die Bedeutung der Regelungsmaterie an, *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der EU, Art. 290 Rdnr. 37 m.w.Nw.; dies impliziert einen erheblichen Spielraum, s.a. *Gärditz*, DÖV 2010, 453, 456; *Möllers/v. Achenbach*, EuR 2011, 39, 48 f.; zum Verfahren der exekutiven Rechtssetzung nach dem Vertrag von Lissabon s. *Sydow*, JZ 2012, 157 ff.

ditierung und Zertifizierung danach ohnehin keine direkten Rechtsfolgen gehabt hätten.[72] Mangels echten Norminhalts hätte die Rechtssetzung freilich de facto vollständig bei der *Kommission* gelegen. Der *EP*-Entwurf trägt insofern dazu bei, den primärrechtlichen Maßstab einzuhalten, der durch den Kommissionsentwurf angesichts der extremen Zahl von Ermächtigungen (die langen Kataloge in Art. 86 DS-GVO-E sprechen hier Bände) jedenfalls im Gesamtbild kaum gewahrt würde.[73]

b) Prüfungsgegenstand

Der *EP*-Entwurf differenziert nicht hinreichend zwischen der Auditierung eines Verfahrens eines Datenverarbeiters und der Zertifizierung von Produkten und Dienstleistungen. Art. 39 DS-GVO-E bezieht sich nunmehr direkt auf Ersteres, während versäumt wurde, Erwägungsgrund 77 entsprechend anzupassen, sodass die beiden nunmehr nicht zusammenpassen. Der Sache nach besteht kein Grund, warum die Grundverordnung nicht auch eine Produktzertifizierung enthalten sollte. Hierfür enthält der *EP*-Entwurf keinerlei Vorgaben. Der neue Art. 39 Abs. 2a enthält zwar die Möglichkeit für den *EDA* zur Verabschiedung datenschutzfreundlicher technischer Standards, aber keine Regelung zur Zertifizierung einzelner Produkte. Die Eigenschaften derartiger IT-Produkte können somit zwar mittelbar eine Rolle für die Auditierung nach Art. 39 spielen, sind aber nicht selbst Prüfungsgegenstand.

Angesichts des Potenzials entsprechend zertifizierter IT-Produkte im europäischen Binnenmarkt sollten im Zuge des weiteren Reformprozesses entsprechende Regelungen aufgenommen werden. Ohne derartige produktbezogene Prüfsiegel ist auch eine weitere Neuerung des *EP*-Entwurfs kaum umsetzbar, nämlich, im Rahmen öffentlicher Vergabeverfahren den Grundsatz des „data protection by design" als Grundvoraussetzung vorzugeben (Art. 23 Abs. 1a). Schließlich besteht auch die Gefahr, durch eine absichtliche Nichtregelung der Materie in der Grundverordnung nationale Produktzertifizierungen unmöglich zu machen.

c) Prüfungsmaßstab

Der *EP*-Entwurf stellt allein auf die Einhaltung der Verordnung ab. Er zielt damit einseitig auf die Rechtssicherheit für die verantwortlichen Stellen und vernachlässigt die Möglichkeit von Markteffekten, die sich nicht bei der Prämierung bloßer Rechtstreue, sondern nur bei der Werbung eines geprüften „Plus" an Datenschutz einstellen können (s. unter III.2).

Ein gewisses dynamisches Element enthält die Auditierung allerdings dadurch, dass die Einhaltung von Normen des Entwurfs geprüft wird, die ihrerseits zu einer fortlaufenden Selbstüberprüfung des Datenverarbeiters anhalten. Ein Beispiel sind die Prinzipien des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen (Art. 23 DS-GVO-E), auf die in Art. 39 Abs. 1a des *EP*-Entwurfs sogar ausdrücklich verwiesen wird. Dieser Entwurf erweitert Art. 23 überdies erheblich und sieht nicht nur eine Berücksichtigung des Stands der Technik und des jeweils aktuellen technischen Wissens vor, sondern auch eine umfassende Einbeziehung des „entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data".

Art. 39 und Art. 23 könnten so einen echten Mehrwert für den Datenschutz in Unternehmen und Behörden bringen. Allerdings sollte innerhalb von Art. 39 klargestellt werden, dass sich die Auditierung tatsächlich auf derartige datenschutzfreundliche Verfahren erstreckt oder zumindest erstrecken kann. Andernfalls besteht die Gefahr, dass das ausdrückliche und ausschließliche Abstellen auf die Datenverarbeitung „in compliance" mit den Vorschriften der Grundverordnung als statisch und auf den heutigen Wissensstand bezogen aufgefasst wird.

d) Prüfstelle

Der *EP*-Entwurf fixiert die Vergabe bei den Aufsichtsbehörden, eröffnet diesen jedoch Flexibilität hinsichtlich der selbstständigen Prüfung oder Einbindung akkreditierter Auditoren. Wenn sich Audits und Zertifizierungen am Markt durchsetzen, dürfte die Zahl der Verfahren allerdings die Behörden überfordern. Auch mit Blick auf den Freiwilligkeitscharakter der Prüfung ist die Durchführung durch die Behörde selbst nicht anzuraten.[74] Audits und Zertifizierungen drohen auf diesem Weg zu einer „freiwilligen Vorabgenehmigung" zu werden.[75]

Die Einbindung akkreditierter Auditoren und Zertifizierungsstellen ist aus diesen sowie aus ordnungspolitischen Gründen vorzuziehen. Dagegen ist gegen die behördliche Akkreditierung und Siegelvergabe angesichts der positiven Erfahrungen aus Schleswig-Holstein nichts einzuwenden;[76] mit Blick auf die neu vorgesehenen Rechtsfolgen erscheint diese Letztverantwortung sogar geboten. Art. 39 Abs. 3 des *EP*-Entwurfs zeigt auf, wie die Akkreditierungskriterien erarbeitet werden sollten, nämlich unter Beteiligung des *EDA*, der datenverarbeitenden Wirtschaft und von Nichtregierungsorganisationen.[77]

e) Rechtsfolgen

Der *EP*-Entwurf „prämiert" erfolgreiche Audits in sinnvoller Weise und setzt damit auf eine Mischung aus Marktmechanismen und rechtlichen Anreizen, die auch eine mittelbare Vergabeprivilegierung einschließt: Nach Art. 39 Abs. 1a ist insbesondere die Einhaltung des Prinzips des Datenschutzes durch Technik Gegenstand der Auditierung; zugleich gibt Art. 23 Abs. 1a dieses Prinzip als Voraussetzung für öffentliche Vergabeentscheidungen vor.[78] Bei einer Erweiterung des Entwurfs um die Zertifizierung von IT-Produkten (s. unter V.2.b) wären entsprechende Rechtsfolgen vorzusehen.

Neben der Privilegierung im Rahmen aufsichtsbehördlicher Maßnahmen (Art. 79 Abs. 2b) wäre auch eine Berücksichtigung bei der Haftung gegenüber den Betroffenen (Art. 77) denkbar. Mittelbar kann ein Audit allerdings schon de lege lata wirksam werden, weil es dem Datenverarbeiter bei der ihm obliegenden Exkulpation (Art. 77 Abs. 3) helfen kann.

Die Ermöglichung von Drittstaatenübermittlungen bei Vorliegen gültiger Auditsiegel auf Seiten des Übermittels und des Empfängers (Art. 42 Abs. 2 des *EP*-Entwurfs) erscheint sinnvoll, wenn

72 Die teilweise geforderte Einschränkung der weiten Interpretation des Delegationsvorbehalts auf Fälle, in denen die relevanten Gemeinschaftsziele von Schnelllebigkeit geprägt sind, so GA *Kokott*, SchlA, Slg. 2005, I-10553 Rdnr. 55 ff. – Vereinigtes Königreich/Parlament und Rat, wäre dabei kein Hindernis, weil dieses Kriterium im Datenschutzrecht erfüllt sein dürfte.

73 S. zur Kritik schon *Hornung*, ZD 2012, 99, 104 ff.; i.E. ebenfalls krit. *Costa/Poullet*, CLSR 2012, 254, 560 f.; *Roßnagel*, DuD 2012, 553; *ders.*, MMR 2012 781, 782; *Schild/Tinnefeld*, DuD 2012, 312, 316 f.; *Traung*, CRi 2012, 33, 34 f.; *Roßnagel/Richter/Nebel*, ZD 2013, 103, 104.

74 S. *Roßnagel* (o. Fußn. 3), S. 111.

75 Insofern zutreffend *Härting*, CR 2013, 715, 720; wieso es allerdings problematisch sein soll, dass die Behörde, wenn sie i.R.e. Audits Rechtsverstöße feststellt, nicht lediglich die Auditierung verweigert, sondern auf das Abstellen der Verstöße besteht (ebd.), ist nicht ersichtlich. Dieses Abstellen ist Aufgabe der Behörde und sollte im Interesse aller Beteiligten sein.

76 A.A. *AG Rechtsrahmen des Cloud Computing* (o. Fußn. 28), S. 21: Bestimmung der Akkreditierungsstelle durch die Mitgliedstaaten. Zur staatlichen Letztkontrolle (s. unter III.3) müsste dann aber diese Stelle akkreditiert werden.

77 Ähnlich *AG Rechtsrahmen des Cloud Computing* (o. Fußn. 28), S. 19 f.

78 Damit würden auch die teilweise geäußerten europarechtlichen Bedenken ggü. einer Vergabeprivilegierung de lege lata, z.B. *Schantz*, in: BeckOK-BDSG, § 9a Rdnr. 8, obsolet.

(und weil) die mit dem Audit verbundene Prüfung nicht hinter anderen Zulässigkeitsalternativen, wie verbindliche unternehmensinterne Vorschriften, Standarddatenschutzklauseln und Vertragsklauseln, zurückbleibt. Überdies eröffnet der vorgeschlagene Mechanismus die Chance eines „Exports" europäischer Standards. Die Durchführung der Auditierung im Ausland dürfte allerdings besondere Probleme aufwerfen; diese müssten sich in entsprechenden Ausführungsbestimmungen nach Art. 39 Abs. 3 niederschlagen.

Eine grundsätzliche Frage sollte noch adressiert werden: Mit dem Instrument der Datenschutz-Folgenabschätzung (Art. 33)[79] enthält der Entwurf ein Instrument, in dem der Datenverarbeiter das gesamte „lifecycle management" (so Art. 33 Abs. 3 des *EP*-Entwurfs) seiner Datenverarbeitung erfassen und bewerten muss. Vergegenwärtigt man sich Aufbau und Ziele eines Audits, so fällt auf, dass die Idee einer Selbstreflektion über bestehende Datenverarbeitungsvorgänge und das Element einer Risikoanalyse Bestandteil beider Instrumente sind.[80] Dies spricht für eine zumindest teilweise Verzahnung der beiden Instrumente, die in den Entwürfen bislang nebeneinander stehen.

79 S. z.B. *Kaufmann*, ZD 2012, 358, 361 f.; zum Risikomanagement im Datenschutz *Thoma*, ZD 2013, 578.

80 Vgl. das Audit-Konzept mit Erwägungsgrund 70 zur Datenschutz-Folgenabschätzung, wonach diese „... sich insbesondere mit den Maßnahmen, Garantien und Verfahren befasst, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden sollen."

VI. Fazit

Mit Blick auf die vorgestellten Konzepte ist der *EP*-Entwurf ein klarer Schritt nach vorn, weil er erheblich präzisere Vorgaben zu Gegenstand, Maßstab, Zuständigkeit und Rechtsfolgen der Prüfung vorsieht. Hauptkritikpunkt ist, dass keine Regelungen zur Produktzertifizierung aufgenommen wurden und auf der Basis des Entwurfs auch nicht durch die *Kommission* verabschiedet werden könnten. Daneben sollte der Prüfungsmaßstab hinsichtlich der Möglichkeit, ein „Plus" an Datenschutz nachweisen und damit am Markt werben zu können, präzisiert werden. Diese Punkte sind im weiteren Verlauf der Beratungen behebbar. Audits und Zertifizierungen könnten so nach Inkrafttreten der Reform wichtige Bausteine eines modernen und effektiven Datenschutzrechts im Binnenmarkt werden.

Prof. Dr. Gerrit Hornung, LL.M.
ist Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau und Sprecher des dortigen Institute of IT-Security and Security Law (ISL) sowie Mitglied des Wissenschaftsbeirats der ZD.

Korbinian Hartl
ist Wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau.