WINFRIED VEIL

Accountability – Wie weit reicht die Rechenschaftspflicht der DS-GVO?

Nachweispflicht
Risikobasierter Ansatz
Dokumentation
Technische und organisatorische Maßnahmen

Praktische Relevanz und Auslegung eines unbestimmten Begriffs

■ Klar ist, dass die DS-GVO wegen Auslegungsoffenheit, Inkohärenzen, Wertungswidersprüchlichkeiten und Lückenhaftigkeit (bei gleichzeitiger Präskriptivität) die Fachwelt auf Jahre hinaus intensiv beschäftigen wird. Eine der vielen ungeklärten Fragen ist, was unter dem Grundsatz der „Accountability" zu verstehen ist. Der Begriff selbst taucht in der englischen Fassung der DS-GVO nur in Art. 5 Abs. 2 auf und wird mit „Rechenschaftspflicht" ins Deutsche übersetzt. Die Norm besagt, dass der Verantwortliche die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen können muss. Das „Nachweisen-Können-Müssen" findet sich darüber hinaus an einer weiteren zentralen Stelle der DS-GVO: in Art. 24 Abs. 1. Danach muss der Verantwortliche „den Nachweis dafür erbringen ... können, dass die Verarbeitung gemäß dieser Verordnung erfolgt". Schließlich gibt es weitere spezialgesetzlich geregelte Nachweispflichten. Der Beitrag untersucht, was diese Rechenschafts- bzw. Nachweispflichten bedeuten und wie weit sie reichen.
Lesedauer: 33 Minuten

■ The EU General Data Protection Regulation (GDPR/DS-GVO) will keep experts very busy for years to come due to its openness to interpretation, incoherencies, contradictions in evaluations, and gaps (with simultaneous prescriptiveness). One of the many unanswered questions is what is to be understood under the principle of "accountability". The term itself only appears in Art. 5 Subsec. 2 of the English version of the GDPR and is translated into German as "Rechenschaftspflicht". The rule states that the person responsible must be able to prove that the maxims for processing personal data were fulfilled. The "must-be-able-to-prove" is also found in another central place of the GDPR: in Art. 24 Subsec. 1. Pursuant thereto the person responsible must "be able to... provide evidence that processing is undertaken pursuant to this Regulation". Finally, there are further obligations to prove which are set forth in specific legislations. The article will examine what these obligations for accountability, or, as the case may be, for proving mean and how far they reach.

I. Problem

Die praktische Relevanz dieser Frage lässt sich gar nicht hoch genug einschätzen. Bei extensiver Auslegung der Rechenschafts- und Nachweispflichten muss der Verantwortliche jede zur Erfüllung jeder einzelnen Pflicht der DS-GVO[1] ergriffene technische und organisatorische Maßnahme (TOM) präventiv nachweisen können. Je nach Zählweise enthält die DS-GVO für den Verantwortlichen ca. 46 Pflichten.[2] Der Verantwortliche müsste somit nachweisen können, welche mindestens 46 Maßnahmen er zur Erfüllung dieser 46 Pflichten ergriffen hat. Da viele Pflichten an einzelne Daten oder einzelne Verarbeitungsvorgänge anknüpfen, müsste der Verantwortliche darüber hinaus jedes einzelne Datum mit mehreren Metadaten versehen, jeden Verarbeitungsschritt protokollieren und die Protokollierung ebenfalls nachweisen können. Eine solche Dokumentation wäre erforderlich, um nachweisen zu können, dass die Datenverarbeitung zu jedem Zeitpunkt gemäß der DS-GVO erfolgte, erfolgt und erfolgen wird. Dies würde insgesamt zu einem ungeheuren Dokumentationsaufwand beim Verantwortlichen führen. Hierfür zwei Beispiele:

■ **Beispiel 1:** Gem. Art. 17 Abs. 1 müssen Daten unverzüglich gelöscht werden, wenn einer von sechs Löschtatbeständen vorliegt. Diese Löschpflicht ist als Dauerpflicht ausgestaltet, die zu jedem Zeitpunkt der Datenverarbeitung vom Verantwortlichen zu beachten ist. An sich müsste der Verantwortliche daher in jeder Sekunde seiner Datenverarbeitung überprüfen, ob nicht bereits einer der Löschtatbestände eingreift. An sich müsste deshalb jedes vom Verantwortlichen erhobene Datum mit mehreren Metadaten versehen werden, mit deren Hilfe eine dauerhafte Überwachung und erforderlichenfalls unverzügliche Löschung erreicht werden kann. Mehrere Metadaten wären erforderlich, weil es unterschiedliche Gründe gibt, weswegen die Notwendigkeit der Datenverarbeitung entfallen kann (z.B. Zweckerfüllung, Zweckfortfall, Zweckvereitelung, Widerruf der Einwilligung, Widerspruch gegen die Datenverarbeitung, Unrichtigwerden des Datums), und mehrere Gründe, weswegen die Daten ausnahmsweise doch nicht gelöscht werden müssen (Art. 17 Abs. 3).

Bei extensiver Auslegung des Art. 24 Abs. 1 Satz 1 müsste der Verantwortliche an sich nachweisen können, dass er jederzeit zur sofortigen Löschung in der Lage ist. Hierfür müsste er nachweisen, dass er TOM ergriffen hat, die dies sicherstellen. Mit

1 Normen ohne nähere Bezeichnung sind Normen der DS-GVO.

2 Dies sind die folgenden Vorgaben, die vom Verantwortlichen als Pflichten zu beachten sind: (1) Verbot mit Erlaubnisvorbehalt (2) Verarbeitung auf rechtmäßige und transparente Weise sowie nach Treu und Glauben (3) Grundsatz der Zweckbindung (4) Grundsatz der Datenminimierung (5) Richtigkeitsgrundsatz (6) Grundsatz der Speicherbegrenzung (7) Grundsätze der Integrität und Vertraulichkeit (8) Rechenschaftspflicht (9) Einholung der Einwilligung und Einwilligungsvoraussetzungen (10) Schutzvorschriften zu Gunsten von Kindern (11) Regeln für sensible Daten (12) Vorgaben für die transparente Information und Kommunikation (13) Informationspflichten (14) Auskunftspflichten (15) Zurverfügungstellung einer Kopie der Daten (16) Berichtigung (17) Vervollständigung (18) Löschung und De-listing (19) Verarbeitungsbeschränkungen (20) Benachrichtigungen (21) Datenportabilität (22) Widerspruchsrecht (23) Vorgaben für automatisierte Einzelentscheidungen (24) Vornahme technischer und organisatorischer Maßnahmen (25) Nachweispflicht (26) Datenschutz durch Technik und zu datenschutzfreundlichen Voreinstellungen (27) Vorgaben für „joint controllers" (28) Benennung eines Vertreters (29) Vorgaben für die Auftragsdatenverarbeitung (30) Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten (31) Zusammenarbeit mit der Aufsichtsbehörde (32) Vorgaben für die Datensicherheit (33) Benachrichtigung der Datenschutzaufsichtsbehörden bei „data breaches" (34) Benachrichtigung des Betroffenen bei „data breaches" (35) Datenschutz-Folgenabschätzungen (36) Vorherige Konsultation der Datenschutzaufsichtsbehörden (37) Bestellung eines Datenschutzbeauftragten (38) Regeln für die Drittstaatenübermittlung (39) Interessenabwägung im Zusammenhang mit den Kommunikationsfreiheiten (40) Sonderregeln für den Zugang zu amtlichen Dokumenten (41) Sonderregeln für nationale Kennziffern (42) Sonderregeln im Beschäftigungskontext (43) Sonderregeln für Datenverarbeitung zu archivarischen Zwecken (44) Sonderregeln für Datenverarbeitung zu wissenschaftlichen und historischen Forschungszwecken (45) Sonderregeln für Datenverarbeitung zu statistischen Zwecken (46) Geheimhaltungsvorschriften.

welchen anderen Maßnahmen außer durch Metadaten gewährleistete Löschroutinen könnte dieser Nachweis geführt werden? Der Verantwortliche müsste aber nicht nur nachweisen können, dass er zur Löschung in der Lage ist. Er müsste auch nachweisen können, dass er in konkreten Fällen eine Löschung durchgeführt hat, denn nur so kann er nachweisen, dass er ein konkretes Löschbegehren erfüllt hat oder dass er die Pflicht zur dauerhaften Überprüfung und ggf. sofortigen Löschung auch vollzogen hat. Der Verantwortliche müsste also jede einzelne Löschung dokumentieren, was wiederum dem Löschzweck (die endgültige Beseitigung der personenbezogenen Daten) zuwiderliefe und auch nicht gerade dem Gebot zur Datenminimierung entspräche.

■ **Beispiel 2:** Gem. Art. 13 Abs. 1 lit. c und Abs. 3 oder Art. 14 Abs. 1 lit. c und Abs. 4 muss der Verantwortliche gegenüber dem Betroffenen zu Beginn der Datenverarbeitung für jeden Verarbeitungsvorgang die Verarbeitungszwecke und die Rechtsgrundlagen der Datenverarbeitung angeben. Ein Verantwortlicher kann für die Verarbeitung desselben Datums verschiedene Zwecke (z.B. Vertragserfüllung, Kundenmanagement, Direktmarketing) und verschiedene Rechtsgrundlagen (z.B. Einwilligung, Vertrag, berechtigtes Interesse) haben. Zu Beginn der Verarbeitung muss er für jedes einzelne verarbeitete Datum passgenau die richtigen Zwecke und Rechtsgrundlagen angeben.

Bei extensiver Auslegung des Art. 24 Abs. 1 Satz 1 müsste der Verantwortliche an sich nachweisen können, dass er jederzeit in der Lage ist, jedem Datum den richtigen Verarbeitungszweck und die richtige Rechtsgrundlage zuzuordnen, und jederzeit in der Lage ist, den Betroffenen zu Beginn der Datenverarbeitung mit diesen Informationen zu versorgen. Hierfür müsste er die erforderlichen TOM ergriffen haben und das Ergreifen dieser Maßnahmen auch nachweisen können. Und er müsste nachweisen, dass die Information auch in jedem Einzelfall korrekt erfolgt ist. Hierfür müsste er jeden Informationsvorgang dokumentieren.

Die beiden Beispiele zeigen, dass bei sehr strengem Verständnis die Nachweispflichten vielleicht ansatzweise von perfekt organisierten Konzernen mit eigenen Datenschutzabteilungen und nur mit Hilfe umfassender Privacy-Compliance-Management-Programme erfüllt werden können.[3]

Die DS-GVO gilt jedoch grundsätzlich für alle Verantwortlichen gleichermaßen. Dies ist dem „One-size-fits-all"-Ansatz[4] der DS-GVO geschuldet. Privatpersonen, die eine Webseite betreiben, Einzelkaufleute, Kleinstunternehmen, kleine und mittelständische Unternehmen und Non-Profit-Organisationen, die nicht mit komplexen und teuren Managementsystemen arbeiten, können weit verstandene Nachweispflichten faktisch kaum erfüllen. Auch im Hinblick auf Datenverarbeitungen durch natürliche Personen, die von ihrer Meinungs- oder Informationsfreiheit Gebrauch machen, ist die Verknüpfung der ohnehin zahlreichen Verarbeiterpflichten mit zusätzlichen (womöglich präventiv zu erfüllenden) Nachweispflichten problematisch. Eine stärkere Ausdifferenzierung der Nachweispflichten nach verschiedenen Normadressaten wäre wünschenswert gewesen.

II. Reichweite der Nachweispflicht

Daher ist die Reichweite der Rechenschafts- und Nachweispflichten der Art. 5 Abs. 2 und 24 Abs. 1 genauer zu analysieren, was – soweit ersichtlich – von der bislang zur DS-GVO erschienenen Literatur kaum geleistet wurde.[5] Dies soll zunächst mit Hilfe der klassischen Auslegungsmethoden geschehen.

1. Wortlautauslegung

Der Verantwortliche muss die Einhaltung der Grundsätze der Datenverarbeitung des Art. 5 Abs. 1 nachweisen können (Art. 5 Abs. 2). Und er muss nachweisen können, dass er TOM umgesetzt hat, die sicherstellen, dass die Verarbeitung gemäß der DS-GVO erfolgt (Art. 24 Abs. 1). Der Wortlaut dieser beiden Regelungen lässt eine Auslegung zu, nach der der Nachweis in der in den Beispielen beschriebenen Feingranularität zu erfolgen hat.

2. Historische Auslegung

Es stellt sich die Frage, ob eine solche Auslegung auch dem Willen des Normgebers entspricht:

In den Ratsverhandlungen zur DS-GVO hat die Nachweispflicht eine untergeordnete Rolle gespielt und wurde kaum diskutiert. Die Bedeutung, die ihr unter dem Gesichtspunkt der „Accountability" nunmehr von manchen zugeschrieben wird, wurde jedenfalls von den Mitgliedstaaten nicht erkannt.[6]

Nachweispflichten waren zwar auch bereits im ursprünglichen Entwurf der *EU-Kommission* enthalten. Doch beschränkte Art. 22 Abs. 3 KOM-E die präventive Nachweispflicht noch auf die Dokumentation (das spätere Verarbeitungsverzeichnis), die Datensicherheit, die Datenschutz-Folgenabschätzung, die Vorabkonsultation und den Datenschutzbeauftragten. Nach Art. 5 lit. f KOM-E sollten personenbezogene Daten zwar „unter der Gesamtverantwortung" des Verantwortlichen verarbeitet werden, der dafür haften sollte, „dass bei jedem Verarbeitungsvorgang die Vorschriften dieser Verordnung eingehalten werden, und der den Nachweis hierfür erbringen muss". Die Nachweispflicht sollte hier jedoch „nur" eine Beweislastregel i.R.d. Haftung sein.

Die Ausdehnung der Nachweispflichten auf alle Pflichten der DS-GVO gelangte erst mit dem EP-Entwurf und mit dem Ratsentwurf in die Verordnung. Ebenso stimmten *Europäisches Parlament (EP)* und *Rat* darin überein, die konkret zu erfüllenden Pflichten vom risikobasierten Ansatz abhängig zu machen.

Der EP-Entwurf war in verschiedener Hinsicht konkreter. So sollten die Pflichten des Art. 24 nach Vorstellungen des *EP* ausdrücklich auch vom Stand der Technik abhängig gemacht werden (Art. 22 Abs. 1 und 1a EP-E). Der Nachweis für die Wirksamkeit der Sicherstellungsmaßnahmen hätte u.a. durch regelmäßige Berichte analog den obligatorischen Berichten kapitalmarktorientierter Unternehmen geführt werden sollen (Art. 22 Abs. 3 EP-E). Auch eine Regelung zu Datenübermittlungen innerhalb einer Unternehmensgruppe in der EU fand sich in der Norm (Art. 22 Abs. 3a EP-E).

Dass die umfassenden Nachweispflichten erst durch das *EP* und den *Rat* in die DS-GVO gelangt sind, spricht zwar dafür, dass sich der Normgeber Gedanken über die Idee der Nachweispflichten gemacht haben mag. Über den konkreten Umfang der vom Verantwortlichen zu erfüllenden Nachweispflichten bestand allerdings – soweit ersichtlich – keine konkrete Vorstellung.[7]

---

3 Nach *Hamann*, BB 2017, 1090, 1092, „zwingt" das Accountability-Prinzip sogar zur Etablierung eines solchen Datenschutz-Managementsystems; ähnl. *Centre for Information Policy Leadership*, The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society, Discussion Draft v. 21.10.2015, S. 2; *Wichtermann*, ZD 2016, 422.

4 Krit. hierzu z.B. *Leucker*, PinG 2015, 195, 200.

5 Nach *Feiler/Forgó*, EU-DSGVO, 2016, Art. 24 Rdnr. 1, konkretisiert Art. 24 Abs. 1 den in Art. 5 Abs. 2 normierten Grundsatz der Rechenschaftspflicht. Nach *Hartung*, in: Kühling/Buchner, DS-GVO, 2017, Art. 24 Rdnr. 20, wiederholt Art. 24 Abs. 1 lediglich die Rechenschaftspflicht des Art. 5 Abs. 2 und weitet sie auf TOM aus. Nach *Martini*, in: Paal/Pauly, DS-GVO, 2017, Art. 24 Rdnr. 24, wird die Nachweispflicht des Art. 24 Abs. 1 durch die Pflicht zur Führung eines Verarbeitungsverzeichnisses (Art. 30) konkretisiert. Nach *Piltz*, in: Gola, DS-GVO, 2017 Art. 24 Rdnr. 12, sind viele der Art. 25 ff. konkretere Ausformungen der Rechenschaftspflicht des Art. 24 Abs. 1.

6 Der *Autor* arbeitete von 2013 bis 2015 für die Projektgruppe Datenschutz im *BMI*, die federführend für die *Bundesregierung* die Verhandlungen auf Ratsebene geführt hat.

7 Ähnl. *Buchholtz/Stentzel*, in: Gierschmann/Schlender/Stentzel/Veil, DS-GVO, 2017, Art. 5 Rdnr. 44.

3. Teleologische Auslegung

Gem. Art. 24 Abs. 1 soll durch die Regelung sichergestellt werden, dass „die Verarbeitung gemäß dieser Verordnung erfolgt". Die Regelung betrifft somit den gesamten von der DS-GVO festgelegten Pflichtenkreis des Verantwortlichen und wird dadurch zu einer „vor die Klammer" gezogenen, die gesamte DS-GVO überwölbenden Zentralnorm.[8] Sie steuert Art und Umfang jeder einzelnen Pflicht des Verantwortlichen in folgender Weise:

Der Verantwortliche muss geeignete interne Maßnahmen ergreifen, um seine aus der DS-GVO erwachsenden Verpflichtungen zu erfüllen. Mit dieser Handlungspflicht soll Datenschutzeffizienz erreicht werden, also die Wirksamkeit der Umsetzung der datenschutzrechtlichen Pflichten durch den Verantwortlichen.[9]

Der Verantwortliche muss nachweisen können, dass er solche geeigneten Maßnahmen ergriffen hat. Diese Rechenschaftspflicht wird als Triebfeder für die effektive Umsetzung der Grundsätze des Datenschutzes bezeichnet.[10] Sie wird von vielen dem Konzept der Accountability zugerechnet. Sie soll die Grundsätze des Datenschutzes weder ändern noch beeinträchtigen, sondern vielmehr bewirken, dass sie besser funktionieren.[11] Sie soll die Beweislage für die Aufsichtsbehörden verbessern, da eine Prüfung bislang oft daran scheitere, dass der Verantwortliche keine ausreichenden Dokumentationen und Protokolle seiner Abläufe vorhalte.[12]

4. Systematische Auslegung

In systematischer Hinsicht erweist es sich als sehr problematisch, dass die DS-GVO neben den allgemeinen Nachweispflichten der Art. 5 Abs. 2 und 24 Abs. 1 bei den folgenden Tatbeständen weitere spezielle Nachweispflichten enthält:

- Einwilligung (Art. 7 Abs. 1; Erwägungsgrund 42 Satz 1)
- Identitätsfeststellung (Art. 11 Abs. 2)
- Identitätsfeststellung (Art. 12 Abs. 2)
- Widerspruch (Art. 21 Abs. 1 Satz 2; Erwägungsgrund 69 Satz 2)
- Datenschutz „by design" und „by default" (Art. 25 Abs. 1; Erwägungsgrund 78 Satz 2)
- Verzeichnis aller Verarbeitungstätigkeiten (Art. 30; Erwägungsgrund 82 Satz 1)
- Datensicherheit (Art. 32 Abs. 3)
- Datenschutzverletzung (Art. 33 Abs. 5; Erwägungsgrund 85 Satz 2)
- Datenschutz-Folgenabschätzung (Art. 35 Abs. 7 lit. d; Erwägungsgrund 84 Satz 2)
- Drittstaatentransfer (Art. 49 Abs. 1 Unterabs. 2 i.V.m. Abs. 6)
- Haftung (Art. 82 Abs. 3)

Fraglich ist, ob die Tatsache der gesonderten Erwähnung einzelner Nachweispflichten in verschiedenen Tatbeständen der DS-GVO bedeutet, dass es doch keine aus Art. 5 Abs. 2 und 24 Abs. 1 folgende umfassende Nachweispflicht gibt, oder ob die spezialgesetzlich geregelten Nachweispflichten lediglich strenger als die allgemeine Nachweispflicht sind.

Es spricht einiges dafür, dass die gesonderte Erwähnung einer Nachweispflicht in einer Einzelnorm i.R.d. Risikoanalyse zu berücksichtigen ist. Ergibt die Risikoanalyse, dass ein Nachweis unter Risikogesichtspunkten gem. Art. 24 nicht unbedingt erforderlich oder verhältnismäßig ist, kann sich aus der Einzelnorm u.U. doch eine Nachweispflicht ergeben, es sei denn, auch in der Einzelnorm steht die Nachweispflicht unter dem Vorbehalt der Risikoadäquanz.

Enthält die Einzelnorm hingegen eine ausdrückliche Ausnahme von der Nachweispflicht, kann diese nicht über den Umweg von Art. 24 wieder aufleben. Der Ausschluss der Nachweispflicht ist dann als lex specialis zur Regelung der allgemeinen Nachweispflicht der Art. 5 Abs. 2 und 24 Abs. 1 anzusehen. Ist z.B. ein Verzeichnis von Verarbeitungstätigkeiten grundsätzlich nicht erforderlich, weil der Verantwortliche weniger als 250 Mitarbeiter beschäftigt und seine Verarbeitung kein Risiko für den Betroffenen birgt (Art. 30 Abs. 5), entfällt die Verpflichtung zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten. Das bedeutet aber nicht nur, dass kein Verzeichnis geführt werden muss. Der Nachweis über die in Art. 30 Abs. 1 und 2 genannten Gesichtspunkte (u.a. Verarbeitungszwecke, Drittstaatenübermittlungen, Löschfristen, Maßnahmen zur Datensicherheit) muss dann auch nicht mehr auf Grund anderer Normen der DS-GVO geführt werden. Anderenfalls würde der Ausschluss von der Pflicht zur Führung eines Verfahrensverzeichnisses durch die allgemeine Nachweispflicht der Art. 5 Abs. 2 und 24 Abs. 1 umgangen.[13]

Ob eine solche Auslegung von allen Datenschutzaufsichtsbehörden geteilt wird, ist fraglich. Die *Datenschutzkonferenz des Bundes und der Länder* schreibt, das Verzeichnis von Verarbeitungstätigkeiten sei nur ein Baustein, um der in Art. 5 Abs. 2 normierten Rechenschaftspflicht zu genügen. Die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1) müsse durch entsprechende Dokumentationen nachgewiesen werden.[14] Wenn mit der Dokumentation der „Ordnungsmäßigkeit der gesamten Verarbeitung" auch die Dokumentation der Gesichtspunkte gemeint sein sollte, über die gem. Art. 30 Abs. 5 kein Verzeichnis von Verarbeitungstätigkeiten angelegt werden muss, dann wäre die Ausnahme des Art. 30 Abs. 5 ohne Anwendungsbereich.

5. Zwischenergebnis

Der Wortlaut der Art. 5 Abs. 2 und 24 Abs. 1, die historische Auslegung und die teleologische Auslegung lassen es zumindest möglich erscheinen, dass die DS-GVO jedem Verantwortlichen exorbitante Rechenschafts- und Nachweispflichten auferlegt. Daher stellt sich die Frage, welche Gesichtspunkte gegen eine solche Auslegung sprechen und ob die Nachweispflichten auf ein vernünftiges Maß beschränkt werden können.

III. Einschränkung weit verstandener Nachweispflichten

1. Darlegungs- und Beweislast

Fraglich ist, ob der Verantwortliche auf Grund der Rechenschaftspflicht des Art. 5 Abs. 2 und der Nachweispflicht des 24 Abs. 1 Satz 1 gegenüber der Datenschutzaufsichtsbehörde tatsächlich die Darlegungs- und Beweislast für die Rechtmäßigkeit des eigenen Handelns trägt, sodass bereits die fehlerhafte Dokumentation als Verletzung datenschutzrechtlicher Pflichten anzusehen wäre.[15]

Eine solche Interpretation wäre jedenfalls in einem Ordnungswidrigkeiten- oder Strafverfahren mit der Unschuldsvermutung

8 *Veil*, in: Gierschmann/Schlender/Stentzel/Veil (o. Fußn. 7), Art. 24 Rdnr. 1. Nach *Martini* (o. Fußn. 5), Rdnr. 1, ist Art. 24 die „Generalnorm der Verantwortungszuweisung".
9 *Hladjk/Kramer*, DSB 9/2011, 8.
10 *Art. 29 Data Protection Working Party*, WP 173 (2010), Opinion 3/2010 on the principle of accountability (adopted on 13 July 2010), S. 4.
11 *Art. 29 Data Protection Working Party* (o. Fußn. 10), S. 5.
12 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2016, S. 56, Rdnr. 19.
13 In diesem Sinne für alle spezialgesetzlich geregelten Nachweispflichten *Buchholtz/Stentzel* (o. Fußn. 7), Rdnr. 45.
14 *Datenschutzkonferenz*, Kurzpapier Nr. 1 – Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO (Stand: 29. Juni 2017), S. 2.
15 Bejahend z.B. *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, S. 55 f.; *Hamann*, BB 2017, 1090, 1091; *Schneider,* in: Schneider, Hdb. EDV-Recht, 5. Aufl. 2017, A. Datenschutz und IT-Management Rdnr. 538.

nach Art. 48 Abs. 1 GRCh unvereinbar. Daher ist die Nachweispflicht auch keine Beweislastregel, sondern eine materielle Nachweispflicht.[16]

Im Verwaltungsverfahrensrecht gilt grundsätzlich der Untersuchungsgrundsatz (§ 24 Abs. 1 und 2 VwVfG). Das bedeutet, dass die Behörde den für die Entscheidung erheblichen Sachverhalt von Amts wegen selbst zu ermitteln hat. Hierfür kann sie jedes für die Sachverhaltsermittlung im konkreten Fall geeignete und rechtlich zulässige Erkenntnismittel nutzen. Sie hat die Befugnis, sich bestimmter Beweismittel (wie Einholung von Auskünften, Anhörung von Beteiligten, Beiziehung von Urkunden und Akten, Inaugenscheinnahme) zu bedienen (§ 26 Abs. 1 VwVfG).

Die Beteiligten sollen bei der Sachverhaltsermittlung lediglich mitwirken (§ 26 Abs. 2 Satz 1 VwVfG). Für die Mitwirkungslast der Beteiligten gilt somit nur eine Sollvorschrift. Der Gesetzgeber will den Beteiligten nicht zumuten, auch zur Aufklärung solcher Umstände beizutragen, die ihre Stellung im Verwaltungsverfahren verschlechtern oder sie in sonstiger Weise belasten würden. Eine weitergehende Pflicht, bei der Sachverhaltsermittlung mitzuwirken, besteht nur, soweit dies durch Rechtsvorschrift besonders vorgesehen ist (§ 26 Abs. 2 Satz 3 VwVfG). Die Mitwirkungspflicht ist somit die Ausnahme.

Im aktuell noch geltenden Datenschutzrecht hat der Verantwortliche auf Verlangen der Aufsichtsbehörde die für die Erfüllung der Aufgaben der Aufsichtsbehörde erforderlichen Auskünfte unverzüglich zu erteilen (Art. 38 Abs. 3 Satz 1 BDSG). Auch darin kann keine allgemeine Mitwirkungspflicht des Verantwortlichen gesehen werden. Die Behörde muss die gewünschten Informationen „verlangen" und möglichst präzise beschreiben.[17] Das Auskunftsverlangen hat Verwaltungsaktsqualität und kann mit Verwaltungszwang durchgesetzt werden.[18] Das bedeutet gleichzeitig, dass sich der Verantwortliche mit Widerspruch und Anfechtungsklage dagegen zur Wehr setzen kann. Die Mitwirkungspflicht ist somit auch gem. § 38 Abs. 3 Satz 1 BDSG die Ausnahme und rechtlicher Einhegung unterworfen.

Dieses Regel-Ausnahme-Verhältnis würde zu Lasten des Verantwortlichen vollständig aus den Angeln gehoben, wenn der Verantwortliche von sich aus die Erfüllung jeder einzelnen datenschutzrechtlichen Pflicht nachweisen müsste. Einer solchen Pflicht vergleichbar wäre, wenn Autofahrer die Einhaltung sämtlicher Verkehrsvorschriften (inklusive der Geschwindigkeitsbegrenzung) jederzeit für jeden Zeitpunkt ihrer Fahrt gegenüber Polizei und Verkehrsbehörden nachweisen können müssten.[19]

Zwar ist eine Mitwirkungspflicht eines Beteiligten auch im Verwaltungsverfahrensrecht zulässig, wenn sie durch Rechtsvorschrift besonders vorgesehen ist. Dieser Gesetzesvorbehalt unterliegt aber dem Bestimmtheitsgebot. Eine generelle Nachweispflicht für die Einhaltung jeder einzelnen Verpflichtung der DS-GVO würde nicht dem Erfordernis gerecht, dass „dies durch Rechtsvorschrift besonders vorgesehen" sein muss.

Das bedeutet, dass auch i.R.d. DS-GVO und trotz der darin enthaltenen Nachweispflichten die Aufsichtsbehörden von den Verantwortlichen nicht ohne weiteres den vollständigen Nachweis der Einhaltung der DS-GVO verlangen können. Sie müssen vielmehr die ihnen nach Art. 58 Abs. 1 zustehenden Untersuchungsbefugnisse zwangsweise durchsetzen.

2. Verbot der Selbstbezichtigung

Das allgemeine rechtsstaatliche Prinzip, dass der Staat keinen Zwang zur Selbstbezichtigung ausüben darf, gilt auch für die Datenschutzkontrolle.[20] Nach § 38 Abs. 3 Satz 1 BDSG haben Verantwortliche zwar auf Verlangen der Aufsichtsbehörde die für die Erfüllung der Aufgaben der Aufsichtsbehörde erforderlichen Auskünfte unverzüglich zu erteilen. Der Verantwortliche kann die Auskunft auf solche Fragen, deren Beantwortung ihn der Gefahr strafgerichtlicher Verfolgung oder eines Ordnungswidrigkeitenverfahrens aussetzen würde, aber verweigern (§ 38 Abs. 3 Satz 2 BDSG).

Fraglich ist, wie sich dieses rechtsstaatliche Prinzip zu einer weit verstandenen Nachweispflicht des Verantwortlichen verhält. Verfahrensrechtlich ist die Aufsichtsbehörde gem. Art. 58 Abs. 1 lit. a zwar befugt, den Verantwortlichen anzuweisen, „alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind". Materiell-rechtlich treten jedoch die Rechenschaftspflicht des Art. 5 Abs. 2, die Nachweispflicht des Art. 24 Abs. 1 Satz 1 und die besonderen Nachweispflichten weiterer Tatbestände hinzu.

Der deutsche Gesetzgeber hat immerhin in den §§ 42 Abs. 4 und 43 Abs. 4 BDSG 2018 festgelegt, dass Meldungen über Datenschutzverletzungen nach Art. 33 und 34 in einem Ordnungswidrigkeiten- oder Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden nicht ohne weiteres verwendet werden dürfen.

Dieselbe Problemlage ergibt sich jedoch bei allen anderen Nachweispflichten. Eine umfassende Nachweispraxis kann für den Verantwortlichen diverse Vorteile haben, wenn er seine Compliance gegenüber den Datenschutzaufsichtsbehörden nachweisen will (neben dem tatsächlichen Nachweis der Compliance stellt sie nicht zuletzt eine vertrauensbildende Maßnahme dar). Andererseits erhöht der Versuch lückenloser Nachweise die Wahrscheinlichkeit, dass Lücken gefunden werden. Dann hätte sich der Verantwortliche gegenüber der Datenschutzaufsichtsbehörde selbst „ans Messer geliefert". Dies soll im Rechtsstaat durch das Verbot der Selbstbezichtigung gerade verhindert werden.

Man wird daher eine umfassend zu verstehende, präventiv zu erfüllende Nachweispflicht des Verantwortlichen auch aus diesem Grunde ablehnen müssen.

3. Erteilung von Geldbußen

Die Rechenschaftspflicht des Art. 24 gehört zu den wenigen Vorschriften der DS-GVO, die nicht bußgeldbewehrt sind. Verstößt ein Verantwortlicher gegen die Pflicht zum Nachweis der Einhaltung einer datenschutzrechtlichen Pflicht, können die Aufsichtsbehörden ihm deswegen kein Bußgeld auferlegen. Diese Aussage gilt aber nur mit zwei wesentlichen Einschränkungen:

Zum einen stellen Verstöße gegen die Rechenschaftspflicht des Art. 5 Abs. 2, die sich auf die Einhaltung der Grundsätze des Art. 5 Abs 1 bezieht, Ordnungswidrigkeiten dar. Die Datenschutzaufsichtsbehörden können hierfür Geldbußen von bis zu € 20 Mio. oder im Falle eines Unternehmens bis zu 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängen (Art. 83 Abs. 5 lit. a). Sofern eine Pflicht der DS-GVO ein solches Gewicht hat, dass ihre Verletzung auch eine Verletzung der Datenschutzgrundsätze darstellen würde, ist somit auch eine Verletzung der Rechenschaftspflicht bußgeldbewehrt. Während die Verletzung von Form- und Verfahrensvorschriften nicht in jedem Fall eine Verletzung

16 *Feiler/Forgó* (o. Fußn. 5), Rdnr. 5.
17 *Petri*, in: Simitis, BDSG, 8. Aufl. 2014, § 38 Rdnr. 54.
18 *Petri* (o. Fußn. 17).
19 *Buchholtz/Stentzel* (o. Fußn. 7), Rdnr. 46, sprechen in diesem Zusammenhang von „Gesinnungsnachweis" bzw. „Gesinnungskontrolle".
20 *Petri* (o. Fußn. 17), Rdnr. 57.

von Datenschutzgrundsätzen darstellen wird, ist z.B. die Vornahme einer Datenverarbeitung ohne Rechtsgrundlage auch ein Verstoß gegen Datenschutzgrundsätze. Würde von einem Verantwortlichen nicht nachgewiesen, dass und wie er die Voraussetzungen des Art. 6 Abs. 1 einhält, könnten die Aufsichtsbehörden schon hierfür Bußgelder erlassen. (Nicht weiter vertieft werden kann an dieser Stelle die Frage, ob der auf einen Verstoß gegen „Grundsätze der Datenverarbeitung" gerichtete Bußgeldtatbestand nicht den Bestimmtheitsgrundsatz verletzt.)

Zum anderen enthalten zahlreiche Normen der DS-GVO eigenständige Nachweispflichten (s.u. II.4). Verstößt der Verantwortliche gegen eine dieser Normen, können die Aufsichtsbehörden ebenfalls Bußgelder erlassen, wenn die jeweilige Norm in Art. 83 Abs. 4 oder 5 genannt ist.

Des Weiteren kann die Einhaltung der Nachweispflichten durch den Verantwortlichen Einfluss darauf haben, in welcher Höhe eine Geldbuße verhängt wird. Die Datenschutzaufsichtsbehörden können nämlich bei der Festlegung von Geldbußen „gebührend berücksichtigen":

- Jegliche vom Verantwortlichen getroffenen Maßnahmen zur Minderung des dem Betroffenen entstandenen Schadens (Art. 83 Abs. 2 lit. c; die Erbringung von Nachweisen kann eine schadensmindernde Maßnahme sein).
- Den Grad der Verantwortung des Verantwortlichen unter Berücksichtigung der von ihm gem. Art. 25 und 32 getroffenen technischen und organisatorischen Maßnahmen (Art. 83 Abs. 2 lit. d; die Erbringung von Nachweisen kann den Grad der Verantwortung schmälern).
- Jegliche anderen erschwerenden oder mildernden Umstände (Art. 83 Abs. 2 lit. k; die Erbringung von Nachweisen kann ein mildernder Umstand sein).

Bei der Erteilung von Geldbußen durch die Datenschutzaufsichtsbehörden führt die Einhaltung der Nachweispflichten jedoch nicht zu einer Rechtsvermutung dafür, dass auch die entsprechende Pflicht eingehalten worden wäre. Ein Verantwortlicher kann die erforderlichen Sicherstellungsmaßnahmen durchgeführt, überprüft und nachgewiesen haben und dennoch gegen die Datenschutzvorschriften verstoßen.[21]

4. Haftung auf Schadensersatz

Auf die Einhaltung der Nachweispflicht des Art. 24 Abs. 1 hat der Betroffene keinen Anspruch. Eine private Durchsetzung der Nachweispflicht scheidet daher aus.[22] Allerdings kann die Nachweispflicht i.R.v. Schadensersatzprozessen eine Rolle spielen. Bei der Haftung auf Schadensersatz gegenüber Personen, denen wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, führt die Einhaltung der Rechenschafts- und Nachweispflichten nicht zu einer Exkulpationsmöglichkeit. Vielmehr kann sich der Verantwortliche von der Haftung nur befreien, wenn er „nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist" (Art. 82 Abs. 3).

Das Verschulden des Verantwortlichen wird somit vermutet. Auch mit guter Betriebsorganisation (wie etwa bei § 831 Abs. 1 Satz 2 BGB) kann sich der Verantwortliche nicht durch Entlastungsbeweis exkulpieren. Gegenüber der aktuellen Rechtslage werden die Anforderungen an die Exkulpation deutlich angehoben. Gem. § 7 Satz 2 BDSG entfällt die Ersatzpflicht, soweit der Verantwortliche die nach den Umständen des Falls gebotene Sorgfalt beachtet hat. Hätte man sich bei der DS-GVO für eine solche Regelung entschieden, wäre ein Anreiz für die Einhaltung der Sicherstellungs- und Rechenschaftspflicht des Art. 24 Abs. 1 Satz 1 geschaffen worden. Dann hätte der Verantwortliche mit der Implementation eines entsprechenden Managementprogramms die Gefahr, für die Entstehung eines Schadens des Betroffenen haften zu müssen, reduzieren können.

Unter Umständen trägt der Verantwortliche wegen seiner Rechenschaftspflicht in Umkehrung der üblichen Beweislastregeln, wonach jeder Anspruchsteller die ihm günstigen Tatbestandsvoraussetzungen beweisen muss, sogar die Darlegungs- und Beweislast dafür, dass er den haftungsauslösenden Verstoß gegen die DS-GVO nicht begangen hat.[23] So trägt der Verantwortliche bei einer einwilligungsbasierten Datenverarbeitung wohl die Darlegungs- und Beweislast dafür, dass der Betroffene eingewilligt hat, und für das fehlende Verschulden, um Schadensersatzansprüche abzuwehren.[24]

5. Risikobasierter Ansatz

De lege lata wird man insbesondere auf den risikobasierten Ansatz zurückgreifen können und müssen, um eine übermäßige Belastung von Verantwortlichen, die risikoarme Datenverarbeitungen vornehmen, zu vermeiden.

Der „risikobasierte Ansatz"[25] skaliert die Handlungspflichten des Verantwortlichen – und zwar nach oben und nach unten. Besonders risikoreiche Datenverarbeitungen erfordern schärfere Maßnahmen. Weniger riskante Datenverarbeitungen lassen weniger strenge Maßnahmen zu. Unter Umständen entfallen einzelne Handlungspflichten ganz, wenn kein großes Risiko zu beobachten ist.

a) Nachweispflichten als risikoferner Vor-Vorfeldschutz

Der zuletzt genannte Gesichtspunkt spielt für die Nachweispflichten der DS-GVO eine besondere Rolle. Schon weite Teile des Datenschutzrechts sind lediglich präventive Vorfeldregelungen. Diese knüpfen an Datenverarbeitungen an, die zum maßgeblichen Zeitpunkt noch gar nicht zu einer konkreten Gefährdung eines Rechtsguts (z.B. des Rechts auf Privatleben gem. Art. 7 GRCh) geführt haben. Eine weite Auslegung der Nachweispflichten setzte gefahrenabwehrrechtlich noch weiter im Vorfeld der Gefahr an. Nicht genug, dass eine für die Rechte des Betroffenen womöglich völlig ungefährliche Datenverarbeitung bereits die Ergreifung einer Vielzahl von Schutzmaßnahmen erfordert (Vorfeldschutz); bei weiter Auslegung der Nachweispflichten müssen auch jeder Verarbeitungsschritt protokolliert werden und alle Schutzmaßnahmen jederzeit nachgewiesen werden können. Dies wäre ein Vor-Vorfeldschutz, der noch weiter vom konkreten Risiko der Datenverarbeitung entfernt wäre als die eigentlichen Schutzmaßnahmen.[26]

Der in Art. 24 Abs. 1 formulierte risikobasierte Ansatz gilt deswegen nicht nur für die Sicherstellungspflicht, sondern auch für die Nachweispflicht. Das bedeutet: Nicht nur die Frage, welche TOM zur Sicherstellung der Einhaltung der DS-GVO zu ergreifen sind, ist risikoabhängig zu beantworten. Auch der Umfang der Nachweispflichten ist abhängig vom Risiko. Es sind nur solche Nachweise zu erbringen, die unter Risikogesichtspunkten erforderlich und angemessen sind. Bei geringem Risiko reduzieren sich die Nachweispflichten oder sie fallen gänzlich weg. Damit wird der risikobasierte Ansatz für die Nachweispflicht zum beschränkenden Element.

---

21 *Art. 29 Data Protection Working Party* (o. Fußn. 10), S. 11 f.
22 *Feiler/Forgó* (o. Fußn. 5), Rdnr. 5.
23 Bejahend *Hamann*, BB 2017, 1090, 1092.
24 *Albrecht/Jotzo* (o. Fußn. 12).
25 Eingehend *Veil*, ZD 2015, 347; *Quelle*, The 'risk revolution' in EU data protection law: We can't have our cake and eat it, too', in: Leenes/van Brakel/Gutwirth/De Hert, Data Protection and Privacy: The Age of Intelligent Machines (i.E.).
26 Vgl. *Buchholtz/Stentzel* (o. Fußn. 7), Rdnr. 49 f.

b) Gewichtungsparameter des risikobasierten Ansatzes
Art. 24 Abs. 1 enthält verschiedene Tatbestandsmerkmale, die für eine pflichtenreduzierende Auslegung in Anspruch genommen werden können.

■ **Art der Verarbeitung**
Spricht die Art der Verarbeitung dafür, dass das Risiko für den Betroffenen geringer ist, können auch die Nachweispflichten geringer ausfallen. „Profiling" und „monitoring" sind nach der DS-GVO z.B. Arten der Datenverarbeitung, die tendenziell als risikoerhöhend anzusehen sind.[27] Der Betrieb einer Kundendatei durch einen Bäcker, der auch einen Brötchenlieferservice anbietet, dürfte hingegen als eine Art der Datenverarbeitung angesehen werden können, für die die Nachweispflicht nur sehr eingeschränkt gilt.

■ **Umfang der Verarbeitung**
Der Umfang der Verarbeitung kann allenfalls ein Indiz für eine potenziell riskante Datenverarbeitung sein. Die Schwere eines potenziellen Eingriffs in Persönlichkeitsrechte kann sich nicht allein an der Zahl der Daten oder der Zahl der Betroffenen bemessen. Auch die Verarbeitung eines einzigen hochsensiblen Datums kann zu einem hohen Risiko führen.[28] Ist die Verarbeitung nicht besonders umfangreich, kann dies jedoch tendenziell als Indiz für eine weniger umfangreiche Nachweispflicht gewertet werden.

■ **Umstände der Verarbeitung**
Mit den Umständen der Verarbeitung, die bei der Risikoprüfung zu berücksichtigen sind, ist vor allem ihre Kontextabhängigkeit gemeint. So kann z.B. eine geringere Vertraulichkeitserwartung des Betroffenen, die von der DS-GVO in Erwägungsgrund 47 Satz 1 und Erwägungsgrund 50 Satz 6 Erwähnung findet, das in der Abwägung zu berücksichtigende Risiko (und damit auch die Nachweispflichten) mindern. Eine geringere Vertraulichkeitserwartung besteht z.B. bei vom Betroffenen offensichtlich öffentlich gemachten Daten (vgl. Art. 9 Abs. 2 lit. e), aber auch i.Ü. bei allgemein zugänglichen Daten. Für den Kontext der Verarbeitung kann es auch eine Rolle spielen, ob die Daten durch öffentliche Register, durch öffentliche oder nicht-öffentliche Stellen oder im Beschäftigungskontext verarbeitet werden.[29]

■ **Zwecke der Verarbeitung**
Dass die Zwecke der Verarbeitung in die Risikoabwägung einzubeziehen sind, bedeutet, dass nicht nur – zu Gunsten des Betroffenen – eine besondere Gefährlichkeit der Verarbeitungszwecke zu berücksichtigen ist, sondern auch – zu Gunsten des Verantwortlichen – ein dem Verarbeitungszweck innewohnender besonderer Nutzen (für die Allgemeinheit, für den Datenverarbeiter oder für Dritte).[30] So kann es einen Unterschied machen, ob Daten für kommerzielle oder für nicht-kommerzielle Zwecke verarbeitet werden. Für private, insbesondere kommunikative Aktivitäten im Internet dürfte ein weniger strenger Maßstab gelten, weil die Kommunikationsfreiheiten (Meinungs-, Presse- und Informationsfreiheit) für den Verantwortlichen streiten.

Grundsätzlich muss der Einzelne nach der Rechtsprechung des *BVerfG* Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen.[31] Auch die DS-GVO anerkennt dies, wenn sie in Erwägungsgrund 4 Satz 1 feststellt, dass die Verarbeitung personenbezogener Daten im Dienste der Menschheit stehen soll, und in Erwägungsgrund 4 Satz 2 erklärt, dass das Recht auf Schutz der personenbezogenen Daten kein uneingeschränktes Recht ist, sondern im Hinblick auf seine gesellschaftliche Funktion gesehen werden muss. Beispiele für Gemeinwohlnutzen sind die Verbesserung der Gesundheitsversorgung, die Terror- oder Verbrechensbekämpfung, die Unterstützung des Umweltschutzes oder der Daseinsvorsorge.[32]

Aber nicht nur der Nutzen der Datenverarbeitung für die Allgemeinheit, sondern auch der Nutzen für den Datenverarbeiter und der Nutzen für Dritte sind zu berücksichtigen. Dies anerkennt die DS-GVO in Art. 1 Abs. 2, wenn sie feststellt, dass die Verordnung die Grundrechte und Grundfreiheiten natürlicher Personen schützt, und in Erwägungsgrund 4 Satz 2, wenn sie erklärt, dass das Recht auf Schutz der personenbezogenen Daten gegen andere Grundrechte abgewogen werden muss. Der Nutzen für den Einzelnen kann z.B. in größerer Bequemlichkeit oder Effizienz, dem Zugang zu bestimmten Gütern oder Dienstleistungen, der Möglichkeit, eine Transaktion durchzuführen, einer besseren medizinischen Versorgung, dem Schutz vor Betrug oder anderen Straftaten bestehen.[33]

An vielen Stellen wird in der DS-GVO gesondert zur Beurteilung der Gefährlichkeit einer Datenverarbeitung auf den Zweck der Datenverarbeitung abgestellt. Zahlreiche Zwecke werden jedoch von der DS-GVO auch privilegiert:

- Die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke und für statistische Zwecke wird generell durch die DS-GVO privilegiert (Art. 5 Abs. 1 lit. b und e, 9 Abs. 2 lit. j, 14 Abs. 5 lit. b, 17 Abs. 3 lit. d, 21 Abs. 6 und 89).
- Art. 9 Abs. 2 nennt zahlreiche Zwecke, die die Verarbeitung sensibler Daten (u.U. nur i.V.m. mitgliedstaatlichen Gesetzen) erlauben: u.a. Arbeitsrecht, soziale Sicherheit, Sozialschutz (Art. 9 Abs. 2 lit. b), Schutz lebenswichtiger Interessen (Art. 9 Abs. 2 lit. c), politische, weltanschauliche, religiöse oder gewerkschaftliche Tätigkeit einer Organisation (Art. 9 Abs. 2 lit. d), Gesundheitsvorsorge, Arbeitsmedizin, medizinische Diagnostik, Gesundheits- oder Sozialbereich (Art. 9 Abs. 2 lit. h).
- Sonderregelungen für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen sehen die Art. 9 Abs. 2 lit. f (Verarbeitung sensibler Daten), 17 Abs. 3 lit. e (Ausnahme vom Recht auf Löschung), 18 Abs. 2 (Ausnahme vom Recht auf Einschränkung der Verarbeitung), 21 Abs. 1 (Ausnahme beim Widerspruchsrecht), 23 Abs. 1 lit. j (Befugnis der Union und der Mitgliedstaaten zur Festlegung von Ausnahmen von den Betroffenenrechten) und 49 Abs. 1 lit. e (Rechtsgrundlage für Drittstaatentransfers) vor.
- Für Datenverarbeitungen zum Zwecke der Direktwerbung sieht Art. 21 Abs. 2 und 3 ein strengeres Widerspruchsrecht vor. Erwägungsgrund 47 Satz 7 erkennt an, dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden kann.
- Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ein berechtigtes Interesse des jeweiligen Verantwortlichen dar (Erwägungsgrund 47 Satz 6).
- Die Verarbeitung für Zwecke der Netz- und Informationssicherheit kann ein berechtigtes Interesse des Verantwortlichen darstellen (Erwägungsgrund 49).
- Für die Fälle der Datenverarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken sind die Mitgliedstaaten verpflichtet Ausnahmen und Abwägungsregeln im nationalen Recht vorzusehen, sofern die Datenverarbei-

27 Eingehend *Veil* (o. Fußn. 8), Rdnr. 81 ff.
28 Eingehend *Veil* (o. Fußn. 8), Rdnr. 87 ff.
29 Eingehend *Veil* (o. Fußn. 8), Rdnr. 93 ff.
30 Eingehend *Veil* (o. Fußn. 8), Rdnr. 103 ff.
31 BVerfGE 63, 43, Rdnr. 174.
32 Vgl. auch *Centre for Information Policy Leadership,* Protecting Privacy in a World of Big Data – Paper 2: The Role of Risk Management, Discussion Draft (16 February 2016), S. 9.
33 Vgl. auch *Centre for Information Policy Leadership* (o. Fußn. 32).

tung unter Inanspruchnahme der Meinungs- und Informationsfreiheit erfolgt (Art. 85 Abs. 1 und 2).

- Die Verarbeitung von personenbezogenen Daten innerhalb einer Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, kann ein berechtigtes Interesse darstellen (Erwägungsgrund 48 Satz 1).
- Darüber hinaus ist die Verarbeitung von Daten im öffentlichen Interesse an vielen Stellen der DS-GVO gesondert geregelt.

Der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b) beherrscht das gesamte Datenschutzrecht. Andere Grundsätze sind von der Zweckbindung abhängig, wie z.B. der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c), der Grundsatz der Richtigkeit (Art. 5 Abs. 1 lit. d) und der Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e). Verantwortlicher ist, wer über die Zwecke und Mittel der Datenverarbeitung entscheidet (Art. 4 Nr. 7). Die Zwecke der Datenverarbeitung haben maßgeblichen Einfluss auf den Umfang der Zulässigkeit der Erst- und Weiterverarbeitung der Daten und auf die Reichweite der Betroffenenrechte (vgl. insbesondere Art. 6 Abs. 1 lit. a i.V.m. 7, 6 Abs. 4, 9 Abs. 2 lit. a, 11 Abs. 1, 13 Abs. 3, 14 Abs. 4, 16 Satz 2, 17 Abs. 1 lit. a, 18 Abs. 1 lit. c).

Es ist daher sehr gut vertretbar, auch den Umfang der Rechenschaftspflicht davon abhängig zu machen, inwieweit die Zwecke der Datenverarbeitung als besonders schutzwürdig anzusehen sind. Besonders schutzwürdig sind Zwecke, die in der DS-GVO ausdrücklich privilegiert werden, die einen besonderen Nutzen für die Allgemeinheit versprechen oder deren Verfolgung zum Wesensgehalt der Grundrechte des Verantwortlichen zählt (wenn dieser z.B. von den Kommunikationsfreiheiten Gebrauch macht). In diesen Fällen kann sich auch die Rechenschaftspflicht der DS-GVO reduzieren.

c) Risiko für den Betroffenen

Da das Nachweiserfordernis des Art. 24 Abs. 1 Satz 1 risikoabhängig ist, ist das Risiko für die Rechte und Freiheiten natürlicher Personen zu ermitteln. Dafür muss eine objektive Bewertung vorgenommen werden (Erwägungsgrund 76 Satz 2). Art. 24 jedoch konkretisiert nicht, welche Rechte und Freiheiten natürlicher Personen durch die Norm geschützt sein sollen. Dies ist höchst bemerkenswert, da damit auch nicht klar wird, für welche Rechte und Freiheiten das Risiko ermittelt werden soll. Der Maßstab aller Risikoüberlegungen bleibt somit offen.[34]

Das Problem reicht über Art. 24 hinaus und betrifft die gesamte DS-GVO. Das Schutzgut oder die Schutzgüter der DS-GVO werden an keiner Stelle definiert. Während § 1 Abs. 1 BDSG den Zweck des Datenschutzrechts noch ausdrücklich darin sieht, den Einzelnen davor zu schützen, dass er in seinem Persönlichkeitsrecht beeinträchtigt wird, erwähnt die DS-GVO den Persönlichkeitsrechtsschutz nicht einmal mehr als Schutzzweck. Lediglich Erwägungsgrund 4 Satz 3 benennt das Recht auf Achtung des Privat- und Familienlebens noch als eines von mehreren Grundrechten – allerdings nur in dem Sinne, dass die DS-GVO mit diesem und anderen Grundrechten in Einklang stehe.

Statt ein konkretes Schutzgut zu benennen, schützt die DS-GVO gem. Art. 1 Abs. 2 „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten". Es stellt sich die Frage, was „die Grundrechte und Grundfreiheiten", die geschützt werden sollen, eigentlich sind. Etwa alle existenten Grundrechte und Grundfreiheiten oder doch nur das Recht auf Privatleben (Art. 7 GRCh) und das Recht auf Datenschutz (Art. 8 GRCh)? Oder wie werden die Menschenwürde, das Recht auf informationelle Selbstbestimmung, die allgemeinen Persönlichkeitsrechte, die Privatsphäre, die Verhaltensfreiheit, das Recht auf Selbstdarstellung und alle sonstigen Grundrechte im Verhältnis zu diesen beiden Grundrechten geschützt?

Auch die Erwägungsgründe geben keinen weiteren Aufschluss. Erwägungsgrund 2 Satz 1 bestätigt, dass die DS-GVO gewährleisten soll, dass die Grundrechte und Grundfreiheiten natürlicher Personen gewahrt bleiben. Des Weiteren werden nur politische Ziele, aber keine individuellen Schutzgüter genannt. Nach Erwägungsgrund 4 Satz 1 sollte die Verarbeitung personenbezogener Daten im Dienste der Menschheit (!) stehen.

Die Tatsache, dass in der gesamten DS-GVO nicht entschieden wird, welches Schutzgut zu Grunde liegt, ist Sinnbild für die Unfähigkeit oder den Unwillen des Normgebers, sich auf Schutzziele für den Datenschutz zu verständigen.[35] In den Rats- und den Trilogverhandlungen zur DS-GVO wurde eine Diskussion über das Schutzgut oder die Schutzgüter der DS-GVO, soweit ersichtlich, nicht geführt. Die Folge ist eine Konturlosigkeit des Datenschutzrechts, das für alle Gefahren der Datenverarbeitung zuständig wird. Dies kann nur zu einer Überforderung bei den Verantwortlichen führen, die alle nur denkbaren Rechte und Freiheiten natürlicher Personen zu schützen haben, und zu Enttäuschungen bei den Betroffenen, deren Erwartung genährt wird, das Datenschutzrecht allein könne sie vor den Gefahren insbesondere der digitalen Datenverarbeitung schützen.[36]

Das Rechtsproblem kann an dieser Stelle nicht weiter vertieft werden. Klar ist jedenfalls, dass bei Datenverarbeitungen, die in geringerem Maße Risiken für die Rechte und Freiheiten des Betroffenen beinhalten, auch die Nachweispflichten geringer ausfallen können.

d) Eintrittswahrscheinlichkeit und Schwere der Risiken

Schließlich hängt der Umfang der Rechenschaftspflicht von der Eintrittswahrscheinlichkeit und der Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen ab. Bei geringer Eintrittswahrscheinlichkeit und/oder geringen Risiken für den Betroffenen können sich die Nachweispflichten entsprechend reduzieren oder sie können ganz entfallen.

6. Verhältnismäßigkeitsgrundsatz

Auch der Verhältnismäßigkeitsgrundsatz (Art. 51 Abs. 1 Satz 2 GRCh) gilt für das Spannungsverhältnis zwischen dem Kontrollbedürfnis der Datenschutzaufsichtsbehörden und dem Interesse des Verantwortlichen an einer Begrenzung des Anforderungsniveaus auf das ihm Zumutbare.[37] Der Verantwortliche muss daher keine Nachweispflichten erfüllen, die für ihn unverhältnismäßig sind. Der risikobasierte Ansatz reduziert im Zusammenspiel mit dem Verhältnismäßigkeitsprinzip den Pflichtenumfang des Verantwortlichen.

7. Bestimmtheitsgrundsatz

Schließlich leiden Rechenschafts- und Nachweispflichten an ihrer Unbestimmtheit. Schon die gem. Art. 5 Abs. 1 einzuhaltenden Grundsätze und die gem. Art. 24 Abs. 1 zu ergreifenden TOM sind reichlich unbestimmt. Mit der Rechenschafts- bzw.

34 Zum fehlenden Konsens über die Frage, vor welchen Schäden das Datenschutzrecht eigentlich schützen soll, auch *Centre for Information Policy Leadership*, A Risk-based Approach to Privacy: Improving Effectiveness in Practice (19 June 2014).
35 In diese Richtung auch *Stentzel*, PinG 2015, 185.
36 Eingehend zur Ableitung der Schutzgüter aus den in der DS-GVO genannten Risikokategorien und zu einer darüber hinausgehenden Schutzgutskonzeption *Veil* (o. Fußn. 8), Rdnr. 120 ff.
37 *Martini* (o. Fußn. 5), Rdnr. 11.

Nachweispflicht potenziert sich die Unbestimmtheit.[38] Auch unter diesem Gesichtspunkt ist eine Minimierung der Nachweispflichten geboten.

IV. Fazit

Die datenschutzrechtliche Grundkonzeption der DS-GVO beruht auf Misstrauen gegenüber jedem Datenverarbeiter. Daher setzt sie auf die Prinzipien von Verbot und Vorsorge. Diese werden in ein System der verpflichtenden präventiven Selbstkontrolle eingebettet, das seinerseits einer ständigen und (theoretisch) lückenlosen repressiven Überwachung durch staatliche Aufsichtsbehörden unterliegt. Dabei müssen dem Wortlaut der DS-GVO nach jeder Verarbeitungsschritt und jede TOM dokumentiert und nachgewiesen werden:

- **Verbotsprinzip:** Jedes personenbezogene Datum wird als potenziell gefährlich angesehen, weswegen die Verarbeitung personenbezogener Daten erst einmal grundsätzlich verboten ist.
- **Vorsorgeprinzip:** Weil die Verarbeitung personenbezogener Daten als so gefährlich angesehen wird, muss der Verantwortliche präventiv eine Vielzahl von Vorsorge-, Schutz- und Begleitpflichten erfüllen.
- **Selbstkontrolle:** Um sicherzugehen, dass der Verantwortliche auch alle ihm von der DS-GVO auferlegten Pflichten erfüllt, muss er präventiv Vorkehrungen treffen, Garantien gewährleisten, Maßnahmen ergreifen, Überprüfungen und Aktualisierungen vornehmen, u.v.m.
- **Überwachung:** All dies wird durch staatliche Aufsichtsbehörden mit extensiven Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen überwacht.
- **Rechenschafts- und Nachweispflichten:** Zwei allgemein formulierte Nachweispflichten und zahlreiche spezifische Nachweispflichten legen nahe, dass im Grunde jeder Verarbeitungsschritt protokolliert, die Ergreifung sämtlicher Maßnahmen zur Erfüllung der Pflichten dokumentiert und der Nachweis hierüber geführt werden können muss.

Letzteres wird gerne mit dem Begriff der Accountability in Verbindung gebracht. Unklar ist jedoch, wie weit das Konzept der Accountability reicht. Selbst im angloamerikanischen Rechtskreis, wird es als „eher konturlos"[39] angesehen und „seine exakte Bedeutung in der Praxis [sei] schwierig zu definieren"[40]. Auf Grund der Nähe zu den Begriffen „social corporate accountability" und „political accountability" wird darunter in den USA wohl das Bekenntnis bzw. die Bereitschaft („commitment") des Verantwortlichen zum Datenschutz verstanden – also eine freiwillig übernommene Verantwortung.[41] Mit rechtlicher Haftung („legal responsibility"/„liability"/„compliance") oder präventiv zu erfüllenden Nachweispflichten hat dies nichts zu tun.[42]

Mit Übernahme des Begriffs in den europäischen Rechtskreis und Einfügung in das präskriptive System der DS-GVO könnte jedoch ein Bedeutungswandel einhergehen. Die *Art. 29-Datenschutzgruppe* gibt zwar zu, dass sich der Begriff Accountability nur schwer in die meisten anderen europäischen Sprachen übersetzen lässt.[43] Und auch im Zusammenhang mit der DS-GVO wird das Konzept der „accountability" als „elusive" und „chameleon-like" bezeichnet.[44] Die Advokaten des Konzepts leiten gleichwohl konkrete Maßnahme- und Nachweispflichten daraus ab. Der Wortlaut des Art. 24 scheint diesem Verständnis auf den ersten Blick Recht zu geben. Bemerkenswert ist allerdings, dass Art. 24 nicht sanktionsbewehrt ist. Der Annahme präventiv zu erfüllender Sicherstellungspflichten, haftungsrechtlicher Konsequenzen einer Verletzung von Accountability-Pflichten und einer echten Beweislastumkehr zu Lasten des Verantwortlichen stehen zahlreiche systematische und rechtsstaatliche Gesichtspunkte entgegen.

Daher müssen die Nachweispflichten restriktiv interpretiert werden. Anderenfalls käme es zu einer rechtsstaatlich nicht zu begründenden Beweislastumkehr. Angesichts der Unschuldsvermutung darf es nicht sein, dass der Verantwortliche grundsätzlich die Rechtmäßigkeit seines Verhaltens gegenüber staatlichen Behörden nachweisen muss. Das gilt für Verwaltungs-, Ordnungswidrigkeiten- und Strafverfahren gleichermaßen. Eine umfassend und präventiv zu verstehende Nachweispflicht verstieße auch gegen das Verbot der Selbstbezichtigung.

Der risikobasierte Ansatz und das Verhältnismäßigkeitsprinzip bieten genug Anhaltspunkte, um die Rechenschaftspflichten des Art. 5 Abs. 2 und die Nachweispflichten des Art. 24 Abs. 1 in rechtsstaatlich verträglicher Weise zu reduzieren. Demnach muss ein Nachweis überhaupt nur geführt werden, wenn die nachzuweisende Maßnahme unter Berücksichtigung des Risikos der Datenverarbeitung für den Betroffenen erforderlich ist, um die Rechtmäßigkeit der Verarbeitung sicherzustellen. Eventuell kann selbst bei Erforderlichkeit einer Maßnahme unter Risikogesichtspunkten auf den Nachweis verzichtet werden.

Einfaches Beispiel: Der „Bäcker um die Ecke", der lediglich eine kleine Kundendatei für Brötchenlieferungen in die Nachbarschaft führt, benötigt kein ausgeklügeltes „Privacy-Compliance-Management"-System, um ein etwaiges Auskunftsbegehren eines Kunden nach Art. 15 zu erfüllen. Angesichts des geringen Risikos und der geringen Komplexität seiner Datenverarbeitung wird der Bäcker gar keine technischen und organisatorischen Maßnahmen treffen müssen, um sicherzustellen, dass er einen etwaigen Auskunftsanspruch erfüllen kann. Und auch eine Nachweispflicht wird er insofern nicht zu erfüllen haben.

Es ist noch unklar, welche Anforderungen die Datenschutzaufsichtsbehörden an Quantität und Qualität der Nachweispflichten stellen werden. Vollkommen unklar ist, welches Gewicht die Gerichte und insbesondere der *EuGH* den rechtsstaatlichen Bedenken gegenüber umfassend und präventiv verstandenen Nachweispflichten beimessen werden. Verantwortlichen, die „auf Nummer sicher gehen" wollen, ist selbstverständlich zur Implementation von Privacy-Compliance-Management-Systemen zu raten. Verantwortliche, die mit guten Gründen behaupten können, ihre Datenverarbeitung berge auf Grund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke mit großer Wahrscheinlichkeit keine hohen Risiken für den Betroffenen, können auf die rechtsstaatlich gebotene Reduzierung der Nachweispflichten verweisen. Interpretierte man die Rechenschafts- und Nachweispflichten der DS-GVO nicht restriktiv, verstießen sie mit einiger Wahrscheinlichkeit gegen die Unschuldsvermutung, gegen das Verbot der Selbstbezichtigung, gegen das Verhältnismäßigkeitsprinzip und gegen den Bestimmtheitsgrundsatz und wären demnach primärrechtswidrig.

Dr. Winfried Veil
ist Referent im Referat IT I 1 (Digitale Agenda; Grundsatz- und Rechtsangelegenheiten der IT und Digitalisierung) im Bundesministerium des Innern.

Der Beitrag gibt ausschließlich die persönliche Meinung des Autors wieder.

38 *Buchholtz/Stentzel* (o. Fußn. 7), Rdnr. 51.
39 *Haug*, JurPC Web-Dok. 160/2011, Abs. 4.
40 *Art. 29 Data Protection Working Party* (o. Fußn. 10), S. 8, Ziff. 21.
41 *Haug*, JurPC Web-Dok. 160/2011, Abs. 10 f.
42 *Haug*, JurPC Web-Dok. 160/2011, Abs. 7.
43 Vorgeschlagen werden „reinforced responsibility" (verstärkte Verantwortung), „assurance" (Zusicherung, Garantie), „reliability" (Zuverlässigkeit), „trustworthiness" (Vertrauenswürdigkeit) und die französische Wendung „obligation de rendre des comptes" (Rechenschaftspflicht), vgl. *Art. 29 Data Protection Working Party* (o. Fußn. 10), S. 8, Ziff. 22.
44 *van Alsenoy*, Regulating Data Protection – The Allocation of Responsibility and Risk among Actors involved in Personal Data Processing, 2016, S. 267.