Kapitel D: Speicherung und Überwachung von Finanzdaten

Die bislang dargestellte Rechtsprechung hat sich noch nicht tiefergehend mit der Rolle von Finanzdaten im Sicherheitsverfassungsrecht auseinandergesetzt. Dabei besteht eine ganze Reihe von Vorschriften, die auch bzgl. der Finanzdaten bestimmte Speicher- und Analysekonzepte etabliert haben, insbesondere § 8 Abs. 1 GwG. Anders als im Rahmen der Telekommunikations- und PNR-Daten handelt es sich aber nicht nur um Normen aus dem Sicherheitsrecht.

Diese Vorschriften sollen im Folgenden beschrieben werden, bevor untersucht werden soll, wie sich die Rechtsprechung zu staatlichen Überwachungsmaßnahmen auf ihre Bewertung auswirkt.

I. Bestandsdatenspeicherung nach § 24c KWG

Eine Anordnung zur Vorhaltung bestimmter Informationen findet sich zunächst in § 24c KWG[642] hinsichtlich der Bestandsdaten von Kontoinhabern bei Kreditinstituten. Auf § 24c KWG verweisen die §§ 93 b, § 93 Abs. 7, 8 AO und § 27 Abs. 2 ZAG, § 28 Abs. 2 KAGB, die den Umfang der Speicherpflicht erweitern und den Anwendungsbereich auf Zahlungsinstitute und Kapitalanlagegesellschaften ausdehnen. Die angeführten Normen können als gemeinschaftliches Speicherregime verstanden werden.

Nach § 24c Abs. 1 KWG haben Kreditinstitute ein Dateisystem zu führen, in dem für jedes Konto, Depot oder Schließfach die Kontonummern, Namen der Inhaber, Verfügungsberechtigten und, soweit vorhanden, wirtschaftlich Berechtigten i. S. d. § 3 GwG[643], außerdem das Geburtsdatum der Inhaber sowie Eröffnungs- und Schließungsdatum gespeichert werden. Es handelt sich somit um eine Speicherpflicht für Bestandsdaten. Allerdings werden die Daten in diesem Kontext oft nicht so bezeichnet, sondern als

642 Kreditwesengesetz (KWG) in der Fassung der Bekanntmachung vom 09.09.1998 (BGBl. I S. 2776), zuletzt geändert durch Gesetz vom 22.02.2023 (BGBl. I S. 51).

643 Geldwäschegesetz (GwG) vom 23. Juni 2017 (BGBl. I S. 1822), zuletzt geändert durch durch Artikel 8 des Gesetzes vom 31. Mai 2023 (BGBl. 2023 I Nr. 140).

„Kontostammdaten".[644] Da dieser Arbeit aber u. a. ein Vergleich mit den TK-Vorschriften zugrunde liegt, soll hier die aus § 3 Nr. 6 TKG bekannte Bezeichnung „Bestandsdaten" verwendet werden. [645]

I. Historische Entwicklung

§ 24c KWG wurde durch das Vierte Finanzmarktförderungsgesetz vom 21. Juni 2002[646] mit Wirkung zum 1. April 2003 als Teil der gesetzgeberischen Reaktion auf die Terroranschläge vom 11. September 2011[647] eingeführt[648].

Die Bankenaufsicht sollte in die Lage versetzt werden, auf einen Schlag herauszufinden, bei welchen Instituten eine oder mehrere bestimmte Personen ein Konto unterhält bzw. unterhalten, um somit die Recherche von Finanzströmen durch die Strafverfolgungsbehörden erheblich zu erleichtern.[649] Insbesondere, wenn lediglich die Namen von verdächtigen Personen bekannt wurden, ging der Gesetzgeber von der Notwendigkeit aus, herauszufinden, wo die Verdächtigen über Konten verfügten, um sodann darüber hinausgehende Ermittlungen bei den entsprechenden Instituten einleiten zu können.[650] Vor der Einführung des § 24c KWG war dies nur durch massenhafte Einzelanfragen, gestützt auf § 44 KWG , bei den (im Jahr 2002 etwa 2900) in der Bundesrepublik lizensierten Instituten möglich.[651] Dieses Verfahren hielt der Gesetzgeber für zu zeitaufwendig.[652]

644 Vgl. BVerfGE 118, 168 – Kontostammdaten; *Achtelik* in Herzog GwG, KWG § 24c Rn. 2; *Tolani*, BKR 2007, 275 (276 ff.).

645 So auch *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 38; *Gnüchtel*, NVwZ 2016, 13 (16); zum Inhalt des § 3 TKG siehe nur *Ricke* in Spindler/Schuster/Anton (Hrsg.), Elektronische Medien, 4. Auflage 2019, TKG § 3 Rn. 6.

646 Gesetz zur weiteren Fortentwicklung des Finanzplatzes Deutschland (Viertes Finanzmarktförderungsgesetz) vom 21 Juni 2002 (BGBl. I, S. 2010).

647 BT-Drs. 14/8017, S. 122 f.; *Deutsche Bundesbank*, (Deutsche Bundesbank), Monatsbericht, Oktober 2002, S. 28; *Schily*, WM 2003, 1249 (1252); *Kokemoor*, BKR 2004, 135 (136); *Jahn*, ZRP 2002, 109 (110); *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95 (118 ff.).

648 Zum Gesetzgebungsprozess ausf. *Zubrod*, WM 2003, 1210 (1210 f.).

649 *Schily*, WM 2003, 1249 (1252).

650 BT-Drs. 14/8017, S. 122 f.

651 Idem, S. 123; *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95 (120); *Schily*, WM 2003, 1249 (1252).

652 BT-Drs. 14/8017, S. 123.

Die Norm ging nicht auf eine europarechtliche Verpflichtung zurück, sondern wurde vom deutschen Gesetzgeber eigenständig initiiert. Im Gegensatz dazu orientierte sich die europäische Union bei den künftigen Änderungen des Anti-Geldwäscherechts an der deutschen Vorlage. So wurde zunächst durch Art. 32 der 3. EU-Geldwäscherichtlinie (GWRL)[653], begleitet von dem Verbot anonymer Konten nach Art. 6, eine Auskunftsverpflichtung der Banken und anderer Verpflichteter entsprechend § 44 KWG eingeführt. Eine europarechtliche Pflicht zur automatisierten Bestandsdatenabfrage, die sich an § 24c KWG orientierte[654], wurde erst mit Art. 32a der 5. GWRL[655] im Jahr 2018 obligatorisch.

Ursprünglich war nicht nur die automatisierte Abfrage bei speziellen Dateien der einzelnen Institute, sondern eine Kontenevidenzzentrale beim Bundesaufsichtsamt für das Kreditwesen (heute BaFin) angedacht, wo sämtliche Kontobestandsdaten zentral geführt werden sollten.[656] Eine solche zentrale Datei hätte aber einen deutlich höheren Arbeitsaufwand sowohl der Kreditwirtschaft als auch der führenden staatlichen Stelle bedeutet, weshalb man sich dafür entschied, dezentrale, von den Banken selbst geführte Dateien einzuführen.[657] Eine ähnliche Regelung, die insofern für § 24c KWG als Vorbild diente[658], fand sich in § 90 TKG aF,[659] der die Anbieter von Telekommunikationsdiensten zur Vorhaltung von Bestandsdaten für Sicherheitsbehörden im Rahmen eines automatisierten Verfahrens verpflichtete (heute §§ 172 ff. TKG).

---

653 Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, ABl. 2005, L 309/15.

654 *BaFin,* Journal, Mai 2018, S. 23; *Engels*, WM 2018, 2071 (2077 f.).

655 Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU, ABl. 2018, L 156/43.

656 *Deutsche Bundesbank*, (Deutsche Bundesbank), Monatsbericht, Oktober 2002, S. 28; *Escher*, BKR 2002, 652 (658); *Teichmann/Achsnich* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 33 Rn. 8; *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95 (120); *Jahn*, ZRP 2002, 109 (110); *Internetredaktion beck-aktuell*, (Beck Online, Verlag C.H. Beck), Bundesfinanzministerium Maßnahmenpaket, becklink 34689, 08.10.2001.

657 *Teichmann/Achsnich* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 33 Rn. 8; *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95 (120).

658 BT-Drs. 14/8017, S. 123.

659 Telekommunikationsgesetz (TKG) vom 25. Juli 1996, BGBl. I, S. 1120.

Im Übrigen hat die Bestandsdatenauskunft nach § 24c KWG, § 93b, § 93 Abs. 7, 8 AO seit ihrer Einführung nur eine überschaubare Anzahl an Änderungen erfahren.[660] Erwähnenswert sind etwa die Erweiterung der Vorhaltefrist nach Ende der jeweiligen Geschäfts- bzw. Kontobeziehung von ursprünglich drei auf zehn Jahre[661] im Jahr und die Erweiterung des Anwendungsbereichs auf Schließfächer durch das Gesetz zur Umsetzung der 4. GWRL.

2. Übersicht

Unmittelbar nach § 24c Abs. 1 Nr. 2 KWG sind als persönliche Daten eigentlich nur Name und Geburtsdatum des Kontoinhabers im Dateisystem aufzuführen. Die Angabe der Anschrift ist nur für die vom Inhaber abweichenden wirtschaftlich Berechtigten vorgesehen, § 24c Abs. 1 Nr. 2 GWG.

Eine Erweiterung der notwendigen Daten des Inhabers finden sich aber im Steuerrecht. Nach § 93 b Abs. 1a AO müssen zusätzlich zu den nach § 24c Abs. 1 KWG zu erhebenden Daten auch die Adressen und die in § 154 Abs. 2a AO genannten steuerrechtlichen Ordnungsmerkmale[662] aller Verfügungsberechtigten in das Dateisystem übernommen werden. Bei Letzteren handelt es sich um die Steuer-Identifikationsnummer i. S. d. § 139b AO und die Wirtschafts-Identifikationsnummer nach § 139c AO sowie bei natürlichen Personen um die Steuernummer.

Diese steuerrechtlichen Erweiterungen gelten jedoch nur für die Abfrage nach § 93b Abs. 1, 93 Abs. 7, 8 AO, also für die Abfrage durch das BZSt. Die BaFin darf nur die in § 24c KWG aufgeführten Daten abfragen.[663] Dies stellt die Rechenzentren vor ein Problem, da sie abhängig vom Anfrageersuchen unterschiedliche Daten bereitstellen müssen, gleichzeitig aber nicht erkennen dürfen, zu welchem Zweck die Abfrage stattfindet.[664] Ab dem 01. Januar 2020 sollen nach Art. 97 § 26 Abs. 3 EGAO deshalb alle nach den steuerrechtlichen Vorschriften und § 24c Abs. 1 KWG zu erhebenden

660 *Achtelik* in Herzog GwG, § 24c KWG Rn. 1.
661 Gesetz zur Bekämpfung der Steuerumgehung und zur Änderung weiterer steuerlicher Vorschriften (StUmgBG) vom 23. Juni 2017, BGBl. I S. 1682.
662 *C. Pohle* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap 11 Rn. 77 ff; 204.
663 BT-Drs. 18/12127, S. 51; *Achtelik* in Herzog GwG, § 24c KWG Rn. 5.
664 BT-Drs. 18/12127, S. 51.

Daten einheitlich im selben Datensatz gespeichert werden.[665] Da § 24c Abs. 1 KWG noch nicht an § 93b Abs. 1a AO angepasst wurde, muss die Differenzierung durch das Informationstechnikzentrum Bund (ITZBund) als gemeinsames Rechenzentrum des BZSt und der BaFin im Rahmen der Zuordnung der Ausgabe-Datensätze erfolgen.[666]

§ 24c KWG ist begrenzt auf Konten, die der Legitimationsprüfung des § 152 Abs. 2 AO unterfallen. Unter den Begriff fallen nach der noch heute gültigen[667] Definition des Reichsfinanzhofes alle *„im Rahmen einer laufenden Geschäftsbeziehung für Kunden geführte Rechnung, in der Zu- und Abgänge von Vermögensgegenständen erfasst werden/buch- und rechnungsgemäße Darstellung einer Geschäftsbeziehung zwischen Kontoinhaber und kontoführendem Institut"*.[668] Hierzu zählen nur externe, keine internen Verrechnungskonten.[669] Außerdem gilt § 24c KWG nicht für klassische Kreditkartenkonten, bei denen keine Einlagen eingezahlt werden, sondern eine turnusmäßige Umsatzabrechnung im Wege des Lastschrifteinzugs erfolgt.[670] Noch recht neu ist die Einbeziehung virtueller IBAN von Zahlungsdienstleistern, die mit einem Konto bei einem Kreditinstitut verknüpft sind,[671] aufgrund Allgemeinverfügung[672] der BaFin. Diese virtuellen IBAN werden von Kreditinstituten an Zahlungsdienstleister, z. B. Prepaid-Kreditkarten, ausgegeben und fungieren als Konto des Endkunden.[673] Zwar gelangen Zahlungen zunächst auf das Konto des Zahlungsdienstleisters, diese werden aber umgehend dem Zahlungskonto des Endkunden zugeschrieben. Insofern ist dieser wirtschaftlich Berechtigter.[674]

Die Dateien müssen bei den Verpflichteten gesondert geführt und technisch so eingerichtet werden, dass die befugten Behörden unmittelbar und ohne, dass dies zur Kenntnis des dateiführenden Instituts gelangt, darauf

665 Ibid.
666 Vgl. Ibid.
667 Vgl. *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 24c KWG Rn. 4.
668 RFHE 24, 203 (205).
669 *Achtelik* in Herzog GwG, § 24c KWG Rn. 6; *Kokemoor*, BKR 2004, 135 (138).
670 *Bundesministerium der Finanzen*, (Bundesministerium der Finanzen), Schreiben KWG 11.80c (VII B 7 – WK 5023 – 26/03), 15. Januar 2003; *Escher*, BKR 2002, 652 (659).
671 *BaFin,* Allgemeinverfügung zu § 24c KWG, 08.12.2020.
672 Gestützt auf § 6 Abs. 3 i. V. m. § 24c Abs. 1 KWG.
673 Ibid.
674 Ibid.

zugreifen können. Die technischen Einzelheiten dieser Schnittstelle werden von der BaFin vorgeschrieben.[675]

Die Schnittstelle muss jederzeit erreichbar sein, unabhängig von den Geschäftszeiten.[676] Die Dateien müssen allerdings nicht zwingend von den Kreditinstituten selbst vorgehalten werden. Nach § 25b KWG dürfen Kreditinstitute bestimmte Aktivitäten und Prozesse unter gewissen Umständen an andere Unternehmen auslagern. Von dieser Möglichkeit haben die Institute im Rahmen des § 24c KWG mehrheitlich Gebrauch gemacht.[677] Abhängig ist dies stets von der Art, Umfang, Komplexität und dem Risikogehalt des jeweiligen Prozesses. Die Verantwortung für die Durchführung des Auskunftsverfahren bleibt aber stets bei den jeweiligen Kreditinstituten.[678]

Nach § 24c Abs. 1 KWG sind die Daten *unverzüglich* zu speichern, wobei der Begriff der Unverzüglichkeit dem BGB entnommen ist, also *ohne schuldhaftes Zögern* bedeutet.[679] Dasselbe gilt nach § 24 Abs. 1 S. 2 KWG, wenn sich an bestehenden Daten Änderungen ergeben. In diesem Fall werden die Daten auch nicht überschrieben, etwa bei einer Namensänderung, sondern ein neuer Datensatz angelegt. Der alte Datensatz muss nach Ablauf von drei Jahren nach Anlage des neuen gelöscht werden, § 24 Abs. 1 S. 3 Alt. 2 KWG. In der Praxis wird dem Unverzüglichkeitserfordernis durch eine tägliche Aktualisierung des Datenbestandes nachgekommen.[680] Zehn Jahre nach Auflösung eines Kontos sind die Daten nach § 24c Abs. 1 S. 3 KWG endgültig zu löschen.

Auf die nach § 24c KWG zu führenden Dateien der Kreditinstitute und anderen Verpflichteten hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) nach § 24c Abs. 2, 5, 6 KWG automatisierten Zugriff. Diesen darf sie nicht nur zur Erfüllung ihrer bankenaufsichtsrechtlichen Pflichten nach dem KWG nutzen, sondern nach § 24c Abs. 2, 3 KWG auch für

675 Vgl. *Achtelik* in Herzog GwG, KWG § 24c Rn. 17; danach zuletzt wohl *BaFin*, Rundschreiben 01/2018 (GW), das aber nicht öffentlich zugänglich ist.

676 *C. Pohle* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 11 Rn. 21; *Kokemoor*, BKR 2004, 135 (140).

677 *Zubrod*, WM 2003, 1210 (1212) verweist etwa auf die FIDUCIA AG (seit 01.09.2021: Atruvia AG), welche als Zentralstelle für die Mitglieder der Genossenschaftlichen FinanzGruppe VolkbankenRaiffeisenbanken tätig wird; *Achtelik* in Herzog GwG, § 24c KWG Rn. 4; *ders.* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 24c KWG Rn. 3.

678 *Schatz* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 549 (566).

679 *Kokemoor*, BKR 2004, 135 (139).

680 *Zubrod*, WM 2003, 1210 (1212); *Kokemoor*, BKR 2004, 135 (139).

dezidiert sicherheitsrechtliche Pflichten.[681] So kann sie einmal eigenständig Daten abrufen, um ihre Pflichten aus dem GWG zu erfüllen oder sonstige strafbare Handlungen zuungunsten der Institute zu verhindern, und andererseits auf Anfragen der Strafverfolgungsbehörden reagieren, soweit dies zur Erfüllung derer Pflichten notwendig ist. Ob diese Auskunftsersuchen legitim sind, hat die BaFin gem. § 24c Abs 3 S. 3 KWG nur zu prüfen, wenn ein *besonderer Anlass* dazu besteht.

Neben der BaFin haben auch das Bundeszentralamt für Steuern (BZSt) nach § 93, Abs. 7, 8, § 93b AO und die Zentralstelle für Finanztransaktionsuntersuchungen (Financial Intelligence Unit – FIU) nach § 31 Abs. 6 GWG automatisierten Zugriff auf das Dateisystem. Sie sind ebenfalls berechtigt, diese Daten auf deren Ersuchen an bestimmte Sicherheitsbehörden, insbesondere die Gefahrenabwehrbehörden, weiterzuleiten.

Die Umstände des Zugriffs staatlicher Stellen auf das Dateisystem sollen im Einzelnen an späterer Stelle noch detailliert erörtert werden (Kap. E. II. 1.). Außerdem soll die Diskussion rund um die Kontobestandsdatenauskunft samt dem hierzu ergangenen Urteil des Bundesverfassungsgerichts umfänglich beschrieben und kommentiert werden (Kap. F. I.).

II. Speicherpflichten für Inhaltsdaten außerhalb des Sicherheitsrechts

Neben den viel besprochenen Kontobestandsdaten[682] fristen diese Kontoinhaltsdaten überraschenderweise noch ein Schattendasein, was sich vielleicht mit der deutlich komplexeren Gesetzeslage erklären lässt. Anders als bei den Bestandsdaten fehlt es hier an einem einheitlichen Dateisystem bzw. einer konkreten Norm, die sowohl Speicherpflicht als auch Zugriffsrechte einheitlich normiert und somit dem § 24c KWG oder §§ 173, 174 TKG entsprechen würde. Die Speicherung von Kontoinhaltsdaten, also die Details von Kontoständen, Transaktionen und anderen Kontobewegungen, wird jedoch ebenso im Rahmen einer ganzen Reihe von Vorschriften vorgeschrieben.

In den bisherigen Untersuchungen der sicherheitsrechtlichen Zugriffe auf Kontoinhaltsdaten wurde bislang zumeist nur unzureichend dargestellt, welche Kontoinhaltsdaten von den Finanzinstituten über ihre Privatkunden

681 Vgl. *Kokemoor*, BKR 2004, 135 (136).
682 Übersicht bei *Pfisterer*, JöR 2017, 393.

gespeichert werden und auf welcher Grundlage dies geschieht.[683] Zwar finden sich in der Literatur zum GwG durchaus entsprechende Ansätze, eine umfassende Betrachtung auch der Normen außerhalb des Sicherheitsrecht wird aber nicht vorgenommen.[684]

Für die sicherheitsrechtliche Debatte lässt sich dieser Umstand damit erklären, dass die allermeisten Speicherpflichten für Kontodaten nicht mit entsprechenden (sicherheitsrechtlichen) Zugriffsnormen verknüpft sind. Im Rahmen einer sicherheitsrechtlichen Betrachtung können nur solche Datenpools als unmittelbar grundrechtsrelevante Vorratsdatenspeicherung angesehen werden, die es gerade bezwecken, dass der Staat im Rahmen der Sicherheitsgewährleistung (zum Begriff des Sicherheitsrechts, oben Kap. B. I. 2. c.) unmittelbar und verdeckt auf sie zugreifen kann. Die schiere Tatsache, dass Daten gesammelt werden, auf die sich Sicherheitsbehörden nach ihren allgemeinen Ermittlungsbefugnissen Zugriff verschaffen können, ist ein gewöhnlicher Umstand der Kommunikationsgesellschaft (s. o. Kap B. III. 2. b. aa.).

Dokumentations- und Aufbewahrungspflichten der kontoführenden Institutionen finden sich im Privat- und Steuerrecht und zielen – soweit man diesen Bereich der Finanzverwaltung insbesondere das Steuerstrafrecht einmal außen vorlässt – nicht unmittelbar darauf ab, den Staat zur Aufklärung und Abwehr von Gefahren bzw. zur Sanktionierung von Kriminalität mit Daten zu versorgen. Sie dienen vielmehr dem Rechtsverkehr und der ordnungsmäßigen Abwicklung der Finanzverwaltung.

683 Von „vast/large amount of stored data" in Bezug auf die Geldwäscherechtlichen Speicherpflichten sprechen etwa *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (243) und *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 103. Bei *Kahler,* Kundendaten, 2017, S. 16 Ist von „riesigen Kundendaten" die Rede. Auf die zivil- und steuerrechtlichen Vorschriften wird jeweils nicht eingegangen.

684 *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 438 stellt immerhin fest, dass die Geldwäscherechtlichen Fristen neben § 257 Abs. 1 HGB und § 147 Abs. 1 Nr. 4, Abs. 3 AO leerlaufen

1. Allgemeine Rechnungslegungspflicht nach §§ 666, 675 BGB, 355 HGB – Kontoauszüge

Bei den Kontokorrentverträgen i. S. d. § 355 HGB – zu diesen gehört insbesondere auch das Girokonto eines Bankkunden[685] – handelt es sich um Geschäftsversorgungsverträge i. S. d. § 675 BGB. Im Rahmen dieser hat der Kunde einen Anspruch gegenüber dem Geschäftsbesorger auf Auskunft und Rechnungslegung gem. §§ 675, 666 BGB.[686]

Sowohl im Rahmen von Giro- als auch Kreditkartenverträgen schulden die jeweiligen Institute danach die fortlaufende Dokumentation von Kontobewegungen in Form von Kontoauszügen.[687] Diese können auch digital ausgestellt werden, wovon die Kunden heutzutage in großem Umfang Gebrauch machen.[688]

Dabei dienen die Auszüge nicht als Rechnungsabschluss i. S. d. § 355 Abs. 1 HGB, sondern lediglich der Information des Kunden über den Stand und Verlauf seines Kontos.[689] Damit der Kunde diesen Verlauf nachvollziehen kann, sind die Kreditinstitute im Rahmen von Treu und Glauben zu einer umfassenden Darstellung aller Änderungen[690], also sämtlicher Einzahlungen, Auszahlungen und anderer Buchungen verpflichtet.

Die Kontoauszüge beinhalten regelmäßig die Höhe der Buchung, den Namen des Empfängers sowie einen Verwendungszweck.[691] Schon die Verpflichtung zur Ausstellung von „klassischen Kontoauszügen" verpflichtet die Kreditinstitute also dazu, die Kontobewegungen ihrer Kunden in vollem Umfang aufzuzeichnen.

Der Informationsanspruch des Kunden wird durch die einmalige Aushändigung der Kontoauszüge grundsätzlich erfüllt, eine erneute Auskunft kann nur ausnahmsweise auf §§ 666, 675 BGB gestützt werden. [692]

685 *Fest* in MüKo HGB Bd. VI BankvertragsR, Teil 2 N Rn. 263.
686 *Bitter* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 33 Rn. 56; BGH, NJW-RR 2003, 1555 (1556).
687 *Löhnig*, JR 2007, 73 (75); BGHZ 165, 53; BGH, NJW 1985, 2699.
688 siehe etwa *Deutsche Bundesbank,* Zahlungsverhalten in Deutschland, 2017, S. 21; *BayLfSt* DB 2017, 280.
689 *Canaris,* Handelsrecht, 24. Aufl. 2020, § 25 Rn. 19.
690 BGH, NJW 1985, 2699 (2699).
691 Vgl. *Bankenverband,* Elektronische Kontoauszüge, 2009, https://bankenverband.de/media/publikationen/elektronische-k.pdf.
692 BGH, NJW 2001, 1486 (1486); OLG Schleswig, NJW-RR 2000, 780 (781).

Bankgeschäfte fallen als „Standardgeschäfte" grundsätzlich auch in den Anwendungsbereich des § 675a BGB, der eine Pflicht zur Information über Entgelte und Auslagen der Geschäftsbesorgung (etwa einer Überweisung) vorsieht. Durch die Einführung der §§ 675c ff. BGB (s. u.) wurden jedoch die Informationspflichten hinsichtlich sämtlicher Zahlungen abschließend geregelt. Für Informationen über Kontobewegungen spielt der § 675a BGB daher keine Rolle mehr.[693]

2. Unterrichtungspflicht für Zahlungen nach § 675d BGB, Art. 248 EGBGB, Art. 5 SEPA-VO

Aufgrund der 1. EU-Zahlungsdiensterichtlinie (PSD 1)[694] wurde das bargeldlose Zahlungsrecht im deutschen Privatrecht mit Einführung der §§ 675c ff. BGB modifiziert.[695] Die zahlungsrechtlichen Vorschriften betreffen gem. § 675c Abs. 3 BGB nicht nur Banken bzw. Kreditinstitute, sondern den umfangreichen Katalog an verpflichteten Dienstleistern aus § 1 ZAG. Aus sicherheitsrechtlicher Perspektive sind vor allem die Zahlungsdienstleister relevant, die von Privatpersonen regelmäßig in Anspruch genommen werden, also Banken, Sparkassen, Kreditkartenunternehmen und Online-Zahlungsdienste wie PayPal.[696]

Soweit Kreditinstitute als Zahlungsdienstleister i. S. d. § 675 f. BGB in Erscheinung treten, etwa Banken und Sparkassen im Rahmen der gängigen Giro-Konten,[697] ergeben sich hieraus spezielle Informations- bzw. Un-

693 BT-Drs. 16/11643, S. 98; *Heermann* in MüKo BGB, § 675a Rn. 15.

694 Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG, ABl. 2007 L 319/1; neu gefasst durch Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/E, ABl. 2015, L337/35.

695 Gesetz zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht vom 28. Juli 2009, BGBl. I S. 2355.

696 PayPal (Europe) S.à r.l. et Cie, S.C.A. ist allerdings als Kreditinstitut geführt und wird in Luxemburg gelistet, vgl. https://www.paypal.com/de/webapps/mpp/impr int, zuletzt aufgerufen am 12.01.2025.

697 Vgl. *Herresthal* in MüKo HGB Bd. VI BankvertragsR, Teil 1 A Rn. 38, 169; *Wahlers,* Zahlungssysteme, 2013, S. 30 ff.

terrichtungspflichten gegenüber den Kunden nach § 675d Abs. 1, 3 BGB i. V. m. Art. 248 §§ 7,8, 14, 15 EGBGB.[698] Danach müssen die jeweiligen Zahlungsdienstleister sowohl des Zahlenden als auch des Empfängers der Zahlung ihre Kunden über die Umstände der Zahlung unterrichten. Dazu gehören eine Kennung der Zahlung, der Zahlungsbetrag, die Höhe der Entgelte, das Wertstellungsdatum und Angaben zum Zahlungsempfänger, § 248 §§ 7, 8, 14, 15 EGBGB. Soweit Kontobewegungen bargeldlos abgewickelt werden, tritt diese Unterrichtungspflicht neben die allgemeine vertragliche Informationspflicht aus §§ 666, 675 BGB.[699]

Die Unterrichtung hat grundsätzlich durch „Mitteilung" in der besonderen Form des Art. 248 § 3 EGBGB zu erfolgen, was grundsätzlich die Übergabe der gespeicherten Informationen auf einem dauerhaften Datenträger i. S. d. § 126b BGB voraussetzt.[700] Allerdings erlaubt Art. 248 § 10 EGBGB abweichende Vereinbarungen. Von diesen haben die meisten Banken Gebrauch gemacht und teilen die Informationen als Online-Kontoauszüge mit.[701] Durch die Kontoauszüge werden die zahlungsdienstrechtlichen Informationspflichten also abgedeckt.[702]

Bei Überweisungen und Buchungen im Wege des SEPA-Lastschriftverfahrens gilt im Ergebnis dasselbe. Die Zahlstelle, also die Bank des zahlenden Giro-Kunden, muss die Daten aus dem Lastschriftdatensatz auf dem Kontoauszug mitteilen, Art. 5 Abs. 1, 3 SEPA-VO[703] i. V. m. Nr. 1, 2 Anhang SEPA-VO. Hierzu gehören u. a. der Betrag, das Fälligkeitsdatum, die IBAN der einzahlenden Stelle, der Verwendungszweck und eine Angabe, ob die Zahlung wiederkehrend oder einmalig ist, Nr. 1,2 Anhang SEPA-VO. [704]

698 Umsetzung von Art. 30 ff. der ZahlungsdiensteRL 2007/64/EG (a.F.); dazu BT-Drs. 16/11643, S. 100; nunmehr geregelt in Art. 43 ff. (Einzelzahlungen) und Art. 50 ff. (Zahlungen innerhalb von Rahmenverträgen) EU-ZahlungsdiensteRL (EU) 2015/2366.

699 vgl. *Schmieder* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 47 Rn. 24c f.

700 BT-Drs. 16/11643, S. 98; *Casper* in MüKo BGB, Art 248 § 3 EGBGB Rn. 2.

701 *Casper* in MüKo BGB, Art 248 § 10 EGBGB Rn. 1; *Henn/Kuballa*, DB 2016, 1900.

702 BT-Drs. 16/11643, S. 136; BGH, NJW 2014, 922 (922); *Casper* in MüKo BGB, Art. 248 § 7 EGBGB Rn. 4.

703 Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009, ABl. 2012 L 94/22.

704 Siehe auch *Zahrte* in Bunte/Zahrte Banken/Sparkassen-AGB, Teil 4, VII Rn. 31.

Aus den zahlungsrechtlichen Vorschriften § 675d BGB, Art. 248 EGBGB und Art. 5 SEPA-VO folgen also spezifische Dokumentationspflichten für Zahlungen und Lastschriften, die einen Großteil der Kontobewegungen im alltäglichen Geschäftsverkehr ausmachen dürften. In der Praxis werden diese Dokumentationspflichten zumindest im Rahmen der Giro-Konten über die Ausstellung von Kontoauszügen abgedeckt.[705]

3. Aufbewahrungspflicht nach §§ 25a KWG, 257 HGB, 22 UStG, 147 AO

Die umfangreiche Dokumentation der Transaktionen geht Hand in Hand mit der bankenaufsichts-, steuer- und handelsrechtlichen Aufbewahrungspflicht. Diese ist in den insoweit aufeinander abgestimmten[706] §§ 25a KWG, 257 HGB und 147 AO normiert.

Nach § 257 HGB ist jeder Kaufmann i. S. d. § 1 HGB – das werden aufgrund der Eigenart des Gewerbes alle aus sicherheitsrechtlicher Perspektive interessanten Institute sein – verpflichtet, die im Katalog des § 257 HGB aufgeführten Unterlagen für teilweise sechs, teils für zehn Jahre aufzubewahren. Eine fast identische Regelung findet sich im Steuerecht in den §§ 22 UstG und § 145 ff. AO, wonach zur Erhebung der Steuer Aufzeichnungen zu machen, §§ 22 UstG, 146 AO, und aufzubewahren sind, § 147 AO. Die hier geregelte Pflicht dient freilich der Steuerhebung, also nicht dem (Privat-) Rechtsverkehr, sondern der Finanzverwaltung. Die Aufzeichnungspflicht des §§ 22 UstG regelt den materiellen Inhalt, der sich aus den Aufzeichnungen für die Steuerbehörden erschließen lassen muss.[707] Die §§ 146, 147 AO hingegen stellen auf die Form der aufzuzeichnenden Dokumente ab. Eine Pflicht zur Aufbewahrung der Aufzeichnungen folgt aber nur aus § 147 AO[708]. Das UStG enthält diesbezüglich keine eigene Regelung.

Die steuerrechtliche Aufbewahrungspflicht bestimmter Dokumente aus § 147 AO unterscheidet sich von § 257 HGB wiederum nur darin, dass sie in Nr. 5 mit den „sonstigen Unterlagen von steuerlicher Bedeutung" einen Auffangtatbestand enthält und die Aufbewahrungsfrist in Einzelfällen auch

705 *Schmieder* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 47 Rn. 24b, § 49 Rn. 112.
706 *Shin,* Organisationspflichten, 2013, S. 169; *Rätke* in Klein AO, § 147 Rn. 147.
707 Siehe § 63 Abs.1 UStDV; *Heidner* in Bunjes UStG, § 22 Rn. 5.
708 Vgl. *Heuermann* in Sölch/Ringleb UStG, § 22 Rn. 68.

über zehn Jahre anordnet, wenn die Unterlagen für laufende Steuerverfahren von Bedeutung sind.[709]

Die Aufbewahrungspflicht aus § 147 AO betrifft sämtliche buchführenden Steuerpflichtigen, wozu nach § 238 Abs. 1 HGB wiederum alle Kaufleute gehören. Für Banken und Zahlungsdienstleister wird schon deshalb in allen relevanten Fällen eine Aufzeichnungs- und Aufbewahrungspflicht bestehen.

Zu den Buchungsbelegen i. S. d.. § 237 Abs.1 Nr. 4 HGB, § 147 Nr. 4 AO gehören alle Unterlagen, die sich auf die in den Büchern und Aufzeichnungen enthaltenen Geschäftsvorfälle beziehen[710], also auch Kontoauszüge.[711] Dabei ist zu berücksichtigen, dass die Kontoauszüge aus Sicht der Bank immer einen Geschäftsvorfall betreffen. Rein privat geführte Kontoauszüge müssen deshalb zwar nicht von den Kunden[712], wohl aber stets von den Banken bzw. Kredit- und Zahlungsinstituten aufbewahrt werden[713]. Davon gehen auch die Banken selbst aus.[714] Aufgrund der Fülle an Dokumenten ist die Aufbewahrung heute nur noch digital möglich.[715] Die §§ 257 Abs. 3 HGB, 147 Abs. 2 AO und 25a Abs. 1 S. 6 Nr. 2 KWG erlauben dies ausdrücklich, soweit die *Grundsätze ordnungsmäßiger Buchführung* beachtet werden. Hierzu hat das Bundesfinanzministerium ein interpretierendes Schreiben herausgebracht (GoBD),[716] das den aktuellen Stand der rechtlichen Anforderungen an die digitale Aufbewahrung aus Sicht der Steuerverwaltung zusammenfasst.[717]

---

709 Zum Verhältnis der Normen *Schober*, BC 2013, 528; *Treppmann* DB 1989, 1482 (1483).

710 *Cöster* in Koenig AO, § 147 Rn. 12.

711 *Ders.* in Koenig AO, § 147 Rn. 12; *Rätke* in Klein AO, § 147 Rn. 35.

712 *BayLfSt* DB 2017, 280, 50; FG Rheinland-Pfalz, Urteil vom 25.04.1988 – 5 K 351/87; *Cöster* in Koenig AO, § 157 Rn. 12.

713 *T. Knierim* in Bannenberg/Wabnitz/Janovsky ua. (Hrsg.), Hdb. Wirtschafts- & Steuerstrafrecht, 5. Aufl. 2020, Kap. 10 Rn. 25.

714 *Comdirect,* Aufbewahrung Kontoauszüge, https://magazin.comdirect.de/finanzwissen/wie-lange-kontoauszug-aufbewahren#muss-ich-kontoauszuege-aufbewahren, zuletzt aufgerufen am 12.01.2025.

715 *T. Knierim* in Bannenberg/Wabnitz/Janovsky ua. (Hrsg.), Hdb. Wirtschafts- & Steuerstrafrecht, 5. Aufl. 2020, Kap 10 Rn. 25; *Commerzbank,* Kontoauszüge, https://www.commerzbank.de/portal/de/ratgeber/finanzen/aufbewahrungsfrist-Ihrer-kontoauszuege-das-muessen-sie-wissen.html, zuletzt aufgerufen am 12.01.2025.

716 *Bundesministerium der Finanzen,* GoBD, 2019, BMF-Schreiben vom 28.11.2019 - IV A 4 - 0316/19/10003:001 -, BStBl I S.1269, Anhang 64).

717 *U. Braun* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25a KWG Rn. 679.

Die aufsichtsrechtlichen Aufbewahrungspflichten gem. § 25a S. 6 Nr. 2 KWG verlangen von den in §§ 1, 53, 53b KWG genannten Instituten, dazu gehören insbesondere sämtliche im deutschen Inland tätigen Banken, eine „vollständige Dokumentation der Geschäftstätigkeit, die eine lückenlose Überwachung durch die Bundesanstalt für ihren Zuständigkeitsbereich gewährleistet." Die aufsichtsrechtliche Aufbewahrungspflicht ist folglich offen formuliert und nur auf den Aufsichtsbereich der BaFin beschränkt.[718] Nach der einschlägigen Literatur geht sie dem Umfang nach über die steuer- und handelsrechtlichen Pflichten hinaus.[719]

Für die im Bereich dieser Arbeit interessanten Kontodaten der Privatkunden dürfte dieser erweiterte Umfang aber keine besondere Rolle spielen, da durch die Aufzeichnung der Einlagen, Auszahlungen und Transaktionen auf den Kontoauszügen bereits das Gros der sensiblen Privatdaten abgedeckt wird.

Festzuhalten ist damit zunächst, dass zumindest für einen Zeitraum von zehn Jahren[720] aufgrund verschiedener Regelungen außerhalb des Sicherheitsrechts eine Pflicht zur Aufzeichnung und Aufbewahrung von sämtlichen Geschäftsvorfällen im Rahmen von Giro- und anderen Zahlungskonten besteht, die von den Finanzdienstleistern durch die (digitale) Speicherung der Kontoauszüge erfüllt wird.

III. Sicherheitsrechtliche Speicherpflicht und Überwachung von Kontoinhaltsdaten

Die dargestellten Speicherpflichten verfolgen, abgesehen von der Ahnung von Steuerdelikten, keine unmittelbaren sicherheitsrechtlichen Zwecke. Sie unterscheiden sich damit grundlegend von Normen wie §§ 112b, c TKG, § 2 FlugDaG oder § 24c KWG. Diese zielen darauf ab, private Akteure als Gehilfen der Sicherheitsbehörden einzubinden, indem sie zur Einrichtung und anlasslosen Speisung gesonderter Datenpools verpflichtet werden, die wiederum primär von den Sicherheitsbehörden zur Erfüllung derer Zwecke genutzt werden.

Eine diesem System vergleichbare Speicherung findet sich bei genauerem Hinsehen aber auch im Geldwäschegesetz (GwG) und der Geldtransfer-

718 Idem, Rn. 658

719 *Shin,* Organisationspflichten, 2013, S. 169; *U. Braun* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25a KWG Rn. 668.

720 Vgl. auch die Tabelle bei *Schober*, BC 2013, 528 (532).

verordnung. Dieses Anti-Geldwäscherecht soll im Folgenden beschrieben werden, wobei der Fokus auf den Überwachungsaspekten dieses Systems liegen soll.

1. Geldtransferverordnung

Zunächst ist dabei die GeldtransferVO[721] zu untersuchen. Diese wurde ursprünglich im Jahr 2006[722] erlassen und neun Jahre später, im Zuge der Überarbeitung der GWRL (dazu unten II. 2. a. gg.), überarbeitet.

Die GeldtransferVO und die GWRL stehen in einem engen inhaltlichen Zusammenhang und dienen der Verhinderung von Geldwäsche und Terrorismusfinanzierung.[723] Dabei kommt der GeldtransferVO die Aufgabe zu, die „Papierspur" bzw. den elektronischen Geldverkehr lückenlos rückverfolgbar zu machen.[724] Sie setzt damit Punkt VII der *Special Recommendations* der Financial Action Task Force (FATF) aus dem Jahr 2001[725] um, die heute in Nr. 16 der FATF-Empfehlungen enthalten sind.[726] Anders als etwa die PSD[727] verfolgt sie also primär einen sicherheitsrechtlichen, keinen wirtschaftsrechtlichen Zweck.

Zur Auslegung und Anwendung der Verordnung werden von den Europäischen Aufsichtsbehörden gem. Art. 25 GeldtransferVO Leitlinien verfasst[728], die von der BaFin grundsätzlich übernommen werden.[729]

721 Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006, Abl. 2015, L 141/1.

722 Verordnung (EG) Nr. 1781/2006 des Europäischen Parlaments und des Rates vom 15. November 2006 über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers, Abl. 2006, L 345/1.

723 Erwägungsgründe 8,9 , EU-GeldtransferVO, (EU) 2015/847.

724 Ibid.

725 *FATF,* IX Special Recommendations, 2001, konsolidierte Fassung Feb. 2008.

726 *Dies.,* IX Special Recommendations, 2001, konsolidierte Fassung Feb. 2008, VII; *dies.,* Recommendations 2012, konsolidierte Fassung März 2022, Nr. 16; zur Historie der FATF unten; s.a. *B. Michael Lindner/Lienke/Aydur*, CCZ 2016, 90; *Kunz* CB 2016, 54.

727 Vgl. Erwägungsgründe 4, 5, 7, PSD2, (EU) 2015/2366.

728 Zuletzt *ESA,* Leitlinien Geldtransfer, JC/GL/2017/16, 16.01.2018, dt. Fassung.

729 Vgl. *BaFin,* Leitlinien und Q&As der ESA, https://www.bafin.de/DE/RechtRegelungen/Leitlinien_und_Q_and_A_der_ESAs/Leitlinien_und_Q_and_A_der_ESAs_node.html, zuletzt aufgerufen am 12.01.2025.

a. Geltungsbereich

Die Verordnung enthält Vorschriften über Angaben, die von Zahlungsdienstleistern i. S. d. Art. 1 PSD2[730] bzw. § 1 ZAG bei der Ausführung von Geldtransfers übermittelt werden müssen. Der Begriff des Geldtransfers aus Art. 3 Nr. 9 EU-Geldtransferverordnung ist denkbar weit. Er umfasst sämtliche, zumindest teilweise elektronisch ausgeführten Transaktionen von Geld durch einen Zahlungsdienstleister, insbesondere Überweisungen und Lastschriftzahlungen – nach der BaFin aber auch Bareinzahlungen auf ein Fremdkonto.[731]

Allerdings wird eine ganze Reihe an Geldtransfers von der Verordnung ausgenommen, etwa nach Art. 2 Abs. 2 GeldtransferVO alle in Artikel 3 lit. a) – m) und o) PSD2 aufgeführten Zahlungen.[732]

Hierzu gehören insbesondere Bargeldeinzahlungen von Bankkunden auf deren Konto. Außerdem, nach Art. 2 Abs. 4 UAbs. 2 lit. a) – d) GeldtransferVO, Bargeldabbuchungen des Kontoinhabers, Zahlungen an Verwaltungsbehörden, Überweisungen von Zahlungsdienstleistern untereinander in eigenem Namen und Transfers mittels des Austausches von eingelesenen Schecks, einschließlich beleglosem Scheckeinzug

Ebenfalls ausgenommen sind nach Art. 2 Abs. 3 „Geldtransfers, die mit einer Zahlungskarte, einem E-Geld-Instrument oder einem Mobiltelefon oder anderen im Voraus oder im Nachhinein bezahlten digitalen oder IT-Geräten mit ähnlichen Merkmalen durchgeführt werden", wenn die Zahlung ausschließlich für Waren oder Dienstleistungen ergeht und die Nummer des Zahlinstruments übermittelt wird. Dies aber nur, wenn der Geldtransfer an einen Unternehmer geleistet wird, Art. 2 Abs. 3 S. 2, Art. 3 Nr. 12 GeldtransferVO.

Art. 2 Abs. 5 GeldtransferVO erlaubt den Mitgliedstaaten eine weitere Ausnahme einzuführen. Danach können Inlandtransfers bis zu einem Wert von 1.000,00 € auf ein Konto ausgenommen werden. Voraussetzung ist, dass auf das Konto ausschließlich Zahlungen für die Lieferung von Gütern

730 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (Text von Bedeutung für den EWR), ABl. 2015, L 337/35.

731 *BaFin.,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 28.

732 Art. 2 Abs. 2 EU-GeldtransferVO verweist (auch in der konsolidierten Fassung, Document 02015R0847-20200101) auf die PSD1., 2007/64/EG.

oder Dienstleistungen vorgenommen werden können. Außerdem muss der Zahlungsdienstleister des Begünstigten den Verpflichtungen der GeldtransferVO unterliegen und in der Lage sein, anhand einer individuellen Transaktionskennziffer über den Begünstigten den Geldtransfer bis zu der Person zurückzuverfolgen, die mit dem Begünstigten eine Vereinbarung über die Lieferung von Gütern und Dienstleistungen getroffen hat. Die Bundesrepublik Deutschland hat von dieser Möglichkeit in § 14 Abs. 5 GwG Gebrauch gemacht.

b. Übermittlung von Angaben

Kernvorschriften der Verordnung sind deren Art. 4 – 6. Diese enthalten Pflichten der Zahlungsdienstleister bei Ausführung von Geldtransfers. Art. 4 nimmt dabei den Zahlungsdienstleister des Auftraggebers in den Blick, also etwa eine Bank, die im Rahmen eines Girovertrags eine Überweisung im Online-Banking durchführt.[733]

Der Zahlungsdienstleister des Auftraggebers muss nach Art. 4 Abs. 1 lit. a) – c) GeldtransferVO sicherstellen, dass Name (lit. a)) und Kontonummer (lit. b)) sowie Kundennummer, Anschrift, Geburtsort- und Datum oder die Nummer eines amtlichen persönlichen Dokuments (lit. c)) des Auftraggebers übermittelt werden.

Auch bzgl. des vom Transfer Begünstigten muss der Zahlungsdienstleister Angaben übermitteln: nach Art. 4 Abs. 2 lit. a) und b) GeldtransferVO Name und Kontonummer des Begünstigten. Erfolgt der Transfer nicht von oder auf ein Konto, muss nach Art. 4 Abs. 3 anstelle der Nummer(n) des Zahlungskontos bzw. der Zahlungskonten eine individuelle Transaktionskennziffer übermittelt werden.

Die Richtigkeit aller Angaben sind von dem Zahlungsdienstleister zu überprüfen, Art. 4 Abs. 4 GeldtransferVO. Diese Überprüfung gilt aber in den Fällen des Art. 4 Abs. 5 GeldtransferVO als automatisch ausgeführt, insbesondere wenn die geldwäscherechtliche Identifikation i. S. d. § 10 Abs. 1 Nr. 1 GwG i. V. m. §§ 11 ff. GwG stattgefunden hat.

Von diesen Übermittlungserfordernissen bestehen bedeutende Ausnahmen nach Art. 5, 6 GeldtransferVO. So reicht nach Art. 5 Abs. 1 GeldtransferVO bei Transfers innerhalb der Union die Übermittlung der Kontonum-

733 *Lienke/Gittfried* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 10 Rn. 20.

mern oder der individuellen Transaktionsnummern aus. Die Regelungen der SEPA-VO bleiben hiervon gem. Art. 5 Abs. 1 S. 2 GeldtransferVO unberührt.

Der Zahlungsdienstleister der Begünstigten darf allerdings innerhalb von drei Tagen die Übermittlung der Informationen verlangen, Art. 5 Abs. 2 GeldtransferVO – bei Transfers unterhalb von 1.000,00 € jedoch nur die Namen von Begünstigtem und Auftraggeber sowie die Kontonummern bzw. Transaktionsnummern. Bei den Transfers unterhalb dieser Schwelle entfällt gem. § 5 Abs. 3 lit. a) und b) GeldtransferVO auch generell die Überprüfungspflicht nach Art. 4 Abs. 4 – es sei denn, es besteht der Verdacht auf Geldwäsche oder Terrorismusfinanzierung oder die zu transferierenden Gelder wurden in Form von Bargeld oder anonymem E-Geld entgegengenommen. Für Geschäfte und Überweisungen des alltäglichen Lebens, die zumeist unter 1.000,00 € liegen und sich innerhalb der EU abspielen, hat die Verordnung somit nur eine untergeordnete Bedeutung.

Die Zahlungsdienstleister müssen stets über Systeme verfügen, mit denen sie jeweils feststellen können, ob und welche Voraussetzungen der Ausnahmetatbestände erfüllt sind.[734]

c. Überprüfungspflichten beim Zahlungsdienstleister des Begünstigten

Die Pflichten des Zahlungsdienstleisters des Begünstigten enthalten die Art. 7 GeldtransferVO. Nach Art. 7 Abs. 1 hat der Zahlungsdienstleister des Begünstigten wirksame Verfahren einzurichten, mit denen er zunächst prüfen kann, ob die Felder für alle notwendig zu übermittelnden Daten eines Transfers in dem verwendeten System überhaupt ausgefüllt wurden.

Mit den eingerichteten Systemen muss er nach Art. 7 Abs. 2, 4 – 6 GeldtransferVO aber auch erkennen können, ob die jeweils notwendigen Angaben nach Art. 4, 5 vorhanden sind. Diese Überprüfungen sollen jedenfalls beim Zahlungsdienstleister des Begünstigten in Echtzeit erfolgen.[735] Ob dies auch für den Zahlungsdienstleister des Auftraggebers gilt, lässt sich den Leitlinien, geschweige denn der Verordnung, nicht entnehmen.

Bei Transfers über 1.000,00 € müssen die Angaben nach Art. 7 Abs. 3 darüber hinaus auf ihre Richtigkeit überprüft werden. Unter diesem Betrag ist keine Prüfung notwendig – es sei denn die Auszahlung erfolgt bar oder

734 *ESA,* Leitlinien Geldtransfer, JC/GL/2017/16, 16.01.2018, dt. Fassung, lfd. Nr. 11.
735 Dazu Ibid. lfd. Nr. 22.

in anonymen E-Geld oder es besteht ein hinreichender Verdacht auf Geldwäsche oder Terrorismusfinanzierung. Die Überprüfung gilt aber auch hier als ausgeführt, wenn die geldwäscherechtliche Identifikation stattgefunden hat und die entsprechenden Daten gespeichert wurden, Art. 7 Abs. 5 GeldtransferVO. Außerdem dürfen die Zahlungsdienstleister der Begünstigten nach den ESA-Leitlinien davon ausgehen, dass sie die Vorschriften nach Artikel 7 Absatz 1 und Artikel 11 der Verordnung (EU) 2015/847 einhalten, *wenn sie sich davon überzeugt haben und gegenüber ihrer zuständigen Behörde nachweisen können, dass sie mit den Validierungsregeln des Nachrichten- oder Zahlungs- und Abwicklungssystems vertraut sind und dieses System die Voraussetzungen der Verordnung erfüllt.*[736] Das ist etwa bei der SEPA-Überweisung der Fall.[737]

Nach Art. 8 Abs. 1 GeldtransferVO sind überdies Verfahren einzurichten, „mit deren Hilfe festgestellt werden kann, ob ein Geldtransfer, bei dem die vorgeschriebenen vollständigen Angaben zum Auftraggeber und zum Begünstigten fehlen, auszuführen, zurückzuweisen oder auszusetzen ist, und welche angemessenen Folgemaßnahmen zu treffen sind."

Wird festgestellt, dass Angaben fehlen oder unvollständig sind, so muss der Zahlungsdienstleister des Begünstigten den Transfer zurückweisen oder die Angaben anfordern, bevor er den transferierten Betrag gutschreibt oder sonst zur Verfügung stellt, Art. 8 Abs. 2 GeldtransferVO.

d. Informationserteilung und Speicherung von Daten

Die Art. 14 ff. GeldtransferVO regeln den Umgang der Zahlungsdienstleister mit den aufgrund der Verordnung entstandenen Informationen. Art. 14 bestimmt, dass die Zahlungsdienstleister den für die Terrorismusfinanzierung und Geldwäschebekämpfung zuständigen Behörden unter Einhaltung der Verfahrensvorschriften des Rechts ihrer Sitzmitgliedstaaten auf deren Anfragen hin die nach der Verordnung erhobenen Daten übermitteln müssen.

Die nach Art. 4–7 genannten Angaben sind von den Zahlungsdienstleistern nach Art. 16 Abs. 1 S. 2 GeldtransferVO fünf Jahre lang aufzubewahren. Art. 16 der GeldtransferVO legt allerdings nicht fest, wann die Frist beginnt. Art. 40 Abs. 1 lit. b) der GWRL stellt für den Fristbeginn bzgl. Transaktions-

736 *ESA,* Leitlinien Geldtransfer, JC/GL/2017/16, 16.01.2018, dt. Fassung, lfd. Nr. 22.

737 *Lienke/Gittfried* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap 10 Rn. 57.

belegen aus Geschäftsbeziehungen nicht auf das Entstehen des Beleges ab, sondern auf das Ende des Kalenderjahres, in dem der Beleg entstand (siehe unten III. 2. d. bb. (3)). Eine analoge Anwendung drängt sich auf, damit ein Gleichlaufen der Fristen erzielt werden kann.

Es ist somit festzustellen, dass auch nach der GeldtransferVO eine Speicherpflicht für Kontotransaktionsdaten besteht. Aufgrund der umfassenden Ausnahmen, insbesondere Art. 5 Abs. 1 GeldtransferVO und § 14 Abs. 5 GwG, umfasst die Pflicht aber etliche persönlichkeitsrelevante Alltagsgeschäfte nicht. Sie bleibt insofern hinter umfangreicheren Aufbewahrungspflichten zurück und soll daher nicht im Fokus dieser Abhandlung stehen.

2. Geldwäschegesetz – GwG

Eine weitergehende Pflicht zur Speicherung von Kontoinhaltsdaten findet sich auch im Geldwäschegesetz - GwG,[738] das im Zentrum des deutschen Geldwäscherechts steht.

a. Historische Entwicklung des GwG

Das System des GwG kann auf eine recht stringente, nunmehr schon dreißig Jahre dauernde Entwicklung zurückgeführt werden. Da das Untersuchungsobjekt dieser Arbeit das GwG in seiner aktuellen Fassung darstellt, soll die Entwicklung der Gesetzesnormen in angemessener Kürze geschildert werden. Auf eine umfassende Schilderung der einzelnen Regeln und deren Zusammenhänge in den jeweils geltenden Fassungen kann daher verzichtet werden. Stattdessen sollen nur die bedeutsamen Neuerungen der jeweiligen Gesetzesnovellen vorgestellt werden. Um die Systematik des aktuellen Normenkomplex des GwG und der verbundenen Gesetze zu verstehen, ist solch eine überschaubare Übersicht der historischen Fassungen ausreichend.[739]

738 Dass die Aufbewahrungspflichten weitergehend sind, deutet schon *ESA,* Leitlinien Geldtransfer, JC/GL/2017/16, 16.01.2018, dt. Fassung, lfd. Nr. 64 an.

739 Umfassend mit der Entwicklung des GwG beschäftigen sich *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010; *Gürkan,* Geldwäscheprävention, 2019; Übersicht zur europäischen Entwicklung bei *Herzog/Achtelik* in Herzog GwG, Einl. Rn. 80 ff.

aa. FATF-Empfehlungen, erste Geldwäscherichtlinie und GwG

Das GwG wurde ursprünglich mit Gesetz vom 25.10.1993 eingeführt[740] und setzte die 1991 erlassene Richtlinie der EG zur Bekämpfung der Geldwäsche um (1. EG-GeldwäscheRL – GWRL)[741] auf deren Grundlage ein Jahr zuvor schon der Tatbestand der Geldwäsche nach § 261 StGB neu eingeführt wurde.[742]

Die Richtlinie ging inhaltlich auf den ersten Bericht[743] und die „40 Empfehlungen"[744] der von den G-7 Staaten zwei Jahre zuvor geschaffenen „Financial Action Task Force on Money Laundering" (FATF) zurück.[745] In der Erkenntnis, dass es sich bei der Geldwäsche um ein originär internationales Problem handelt[746], war die FATF als Arbeitsgruppe mit dem Ziel gegründet worden, die Ausnutzung der weltweit vernetzten Finanzsysteme zur Verschleierung illegal erwirtschafteter Gelder (und später insbesondere die Terrorismusfinanzierung) zu bekämpfen.[747] Hierzu bedurfte es nach Auffassung der FATF-Staaten eines länderübergreifenden Systems zur Erkennung und Verhinderung illegaler Geldströme.[748]

In seiner Ursprungsform aus dem Jahr 1993 wirkte das GwG aF im Vergleich zum heute gültigen Pflichtenkatalog der §§ 10 ff. GwG noch vergleichsweise überschaubar. Es beschränkte sich zunächst auf eine Identifizierungspflicht bei bestimmten Einzahlungsgeschäften, § 2 GwG aF 1993 und bei „verdächtigen" Transaktionen gem. § 6 GwG aF 1993. Auch der

740 Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) vom 25.Oktober 1993 (BGBl. I S. 1770).

741 Richtlinie 91/308/EWG des Rates der Europäischen Gemeinschaften vom 10. Juni 1991 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche (ABl. 1991, L 166/77)

742 Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität" (OrgKG) vom 15. Juli 1992 (BGBl. I S. 1302).

743 *FATF,* Report 1990-1991, 1991.

744 *Dies.,* 40 Recommendations, 1990.

745 *Schnabl* in Bannenberg/Wabnitz/Janovsky ua. (Hrsg.), Hdb. Wirtschafts- & Steuerstrafrecht, 5. Aufl. 2020, Kap. 6 Rn. 1; zur Entstehung der FATF *Pieth* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 4 Rn. 8 f.; *Jekewitz* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 9 Rn. 27; *Krämer,* Geldwäsche und Terrorismusbekämpfung, 2008, S. 46 ff.

746 *Jekewitz* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 9 Rn. 27.

747 *Maillart* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 11 (11 f.).

748 *FATF,* 40 Recommendations, 1990, S. 4 f.; hierzu *Krämer,* Geldwäsche und Terrorismusbekämpfung, 2008, S. 81 ff.

Kreis der allgemein Verpflichteten gem. § 1 GwG aF 1993 war deutlich eingeschränkter als jener des aktuellen § 2 GwG.

Neben der Identifizierungspflicht sah das Ursprungs-GwG bereits eine Meldepflicht der Verpflichteten vor – und zwar dann, wenn eine Transaktion in dem Verdacht stand, den Tatbestand der Geldwäsche i. S. d. § 261 StGB aF 1992 zu erfüllen, § 11 GwG aF 1993. Die Meldung musste sich direkt an die zuständige Strafverfolgungsbehörde richten. Eine zwischengeschaltete Behörde, wie heute die FIU, gab es 1993 noch nicht.

Vor allem beinhaltete das GwG in seiner ersten Fassung schon die für diese Untersuchung bedeutsame Aufzeichnungs- und Aufbewahrungspflicht für alle im Rahmen der Identifizierungspflichten getroffenen Feststellungen, § 9 GwG aF 1993. Anders als Art. 4 der 1. GWRL wurde die Pflicht aber ausdrücklich auf solche Informationen beschränkt, die den Verpflichteten im Rahmen ihrer geldwäscherechtlichen Pflichten entstanden waren. Die Bundesregierung machte sich über die oben angesprochene Frage, ob die 1. GWRL eine Pflicht zur Aufbewahrung sämtlicher Transaktionsdokumente vorsieht, bei der Umsetzung der Richtlinie offenbar ebenfalls Gedanken. In der Gesetzesbegründung führte sie aus, dass sich eine gesondert geregelte Pflicht zur Aufbewahrung der einschlägigen Geschäftsunterlagen im GwG erübrigt, da sich eine solche ohnehin aus § 257 HGB ergäbe.[749]

Dass durch die Aufbewahrungspflicht eine Information „auf Vorrat" für die Ermittlungsbehörden bereitgestellt wird, wurde selbst vom zuständigen Referenten des Bundesaufsichtsamt für das Kreditwesen (BAKred) festgestellt.[750] Dementsprechend wurden die Aufzeichnungspflichten und § 10 GwG aF 1993 auch aus der Perspektive des Rechts auf informationelle Selbstbestimmung diskutiert.[751]

Da nach der GWRL nur die Informationsweitergabe zur Verfolgung der Geldwäsche vorgesehen war, musste sich jedenfalls eine Verwendung der Aufzeichnungen zu anderen Strafverfolgungszwecken oder aus steuerlichen Zwecken an den Grundrechten des Grundgesetzes messen lassen, da insofern keine europarechtlich Überlagerung vorlag.[752] Die überwiegende

749 BT-Drs. 12/2704, S. 16.
750 *Findeisen*, wistra 1997, 121 (123).
751 *Fülbier* in Fülbier/Aepfelbach GWG, 2. Aufl. 1994, § 10 S. 127; ausführlich *Werner,* Geldwäsche, 1996, S. 91 ff; 102 f.
752 *Fülbier* in Fülbier/Aepfelbach GWG, 2. Aufl. 1994, § 10 S. 129; grundlegend BVerfGE 73, 339 [1986] – Solange II;, NJW 1990, 974 – Tabaketikettierungsrichtlinie.

Ansicht kam hier zu dem Ergebnis, dass aufgrund der engen Einschränkung der Weitergabe im Bereich der Geldwäsche und dem geringen legitimen Interesse der Bankkunden an Anonymität im Bereich der betroffenen Transaktionen kein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung gegeben war.[753] Auch in der späteren Betrachtung wurde § 10 GwG aF 1993 als Ergebnis einer (gelungenen) Abwägung der durch die Aufzeichnungspflichten betroffenen informationellen Selbstbestimmung und dem Strafverfolgungsinteresse gedeutet[754] (zur Diskussion s. Kap F. II. 1.).

Eine konkrete Pflicht im Vorfeld der geldwäscherechtlichen Aufgaben, nach Auffälligkeiten in den Kontodaten ihrer Kunden zu suchen, enthielt das ursprüngliche GwG nicht. Nach § 14 Abs. 2 Nr. 2 GwG 1993 waren aber die in § 14 Abs. 1 GwG 1993 bezeichneten Verpflichteten, insbesondere Kreditinstitute und Versicherungsunternehmen gehalten, *„interne Grundsätze, Verfahren und Kontrollen zur Verhinderung der Geldwäsche*" einzuführen. Diese Norm wurde vom BAKred als geldwäscherechtliche Generalklausel[755] verstanden. Ausgehend von dieser Vorschrift wollte das BAKred ab der zweiten Hälfte der 1990er Jahre eine Verpflichtung zur Etablierung von EDV-Systemen ableiten, mit denen sich im Wege aktiver Nachforschung Auffälligkeiten, die auf einen Geldwäscheverdacht hindeuten konnten, finden ließen.[756] Dieser Prozess[757] wurde als „Research" oder „Monitoring" bezeichnet, wobei die genauen Definitionen dieser Begriffe zu Beginn noch schwammig waren.[758] Auch die Einführung dieser EDV-Prozesse wurde heftig diskutiert (zur Diskussion s. Kap. F. II. 3.).

753 *Werner,* Geldwäsche, 1996, S. 91 ff., 102 f.; *Fülbier* in Fülbier/Aepfelbach GWG, 2. Aufl. 1994, § 10 S. 127, 131.

754 *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 285.

755 *Findeisen*, wistra 1997, 121 (127).

756 *Artopeus/Findeisen*, (BAKred), Entwurfspapier Anhörung CDU/CSU im Bundestag, 21.08.1995; *BAKred,* Verlautbarung Geldwäsche, 30.03.1998, Ziff. 30, 34d; *BAKred*, Rundschreiben 5/1998, 24.04.1998; *BAKred.,* Jahresbericht, 1998, S. 92.

757 Ein erster Vorschlag zur Funktionsweise solcher Systeme bei *Bergles/Schirnding*, ZBB 1999, 58.

758 Klarheit brachten *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 642 ff., Rn. 8.77.

cc. Die zweite Geldwäscherichtlinie

Zu einer ersten Änderung der geldwäscherechtlichen Vorschriften im europäischen Raum kam es im November 2001 durch den Erlass der zweiten EG-Geldwäscherichtlinie.[759] Die 2. GWRL sah nur Änderungen am bestehenden Text vor, keine völlige Neuformulierung. Die Grundstruktur der Richtlinie wurde nicht wesentlich modifiziert. Intensiviert wurde in dieser Hinsicht allenfalls das Kooperationsverhältnis der privaten und staatlichen Akteure.[760]

Die zweite Geldwäscherichtlinie erweiterte vor allem den Anwendungsbereich und den Kreis der Verpflichteten erheblich. Ausgangspunkt dieser Entwicklung war der 1997 durch den Europäischen Rat adoptierte „Aktionsplan zur Bekämpfung der organisierten Kriminalität“[761], den eine von der EG ein Jahr zuvor eingesetzte hochrangige Gruppe ausgearbeitet hatte.[762] Die EG ging davon aus, dass die verschärften Kontrollen der Kreditinstitute dazu geführt hätten, dass sich Geldwäscher andere Wege gesucht hätten.[763] Schon im Aktionsplan war – wohl deshalb – vorgeschlagen worden, die geldwäscherechtlichen Verpflichtungen auf Berufsträger zu erweitern, die ihrer Natur nach gewöhnlich mit Geldwäschern in Berührung kommen.[764] Das sei insbesondere bei Notaren und manchen Angehörigen der Rechtsberufe der Fall.[765]

Insbesondere die Einbeziehung von Anwälten wurde dabei heftig kritisiert, vorwiegend aus den Reihen der Anwaltschaft selbst, die die Vertrau-

759 Richtlinie 2001/97/EG des Europäischen Parlaments und des Rates vom 4. Dezember 2001 zur Änderung der Richtlinie 91/308/EWG des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche - Erklärung der Kommission (ABl. 2001, L 344/76).

760 Darauf weißen auch *Herzog/Achtelik* in Herzog GwG, Einl. Rn. 82 hin.

761 ABl. 1997 C 251/01.

762 Zur Entwicklung *Stefanou/Xanthaki*, J. of Money Laundering Control 3 (2000), 325.

763 Richtlinie 2001/97/EG, Erwägungsgrund 13, ABl. 2001 L 344/76 (77).

764 Aktionsplan zur Bekämpfung der organisierten Kriminalität, Teil III Nr. 10, ABl. 1997 C 251/1 (9).

765 Richtlinie 2001/97/EG, Erwägungsgrund 16, ABl. 2001 L 344/76 (77); empirisch konnte eine solches Gefährdungspotential von Rechtsanwälten, Steuerberatern, Notaren und Wirtschaftsprüfern nicht nachgewiesen werden, *Kilchling/Lukas*, (Max-Planck-Institut für Ausländisches und Internationales Strafrecht), Endbericht Gefährdung, 2004, S. 91 ff.

lichkeit ihrer Mandantenverhältnisse angegriffen sah.[766] Zum Schutz dieser Vertrauensverhältnisse waren in der Richtlinie allerdings Schutzmechanismen implementiert worden.

Neben der Erweiterung des betroffenen Personenkreises war insbesondere die Neukonzeption des Begriffs der „kriminellen Tätigkeit" von Bedeutung, die unter dem Eindruck des Terrorismus als neuer Hauptgefahr entstand.[767] Der Begriff war zuvor auf den Rauschgifthandel gemünzt. Die Richtlinie ließ den Mitgliedstaaten aber die Möglichkeit, weitergehende Definitionen zu implementieren. Neben Deutschland hatten davon auch Frankreich und Griechenland Gebrauch gemacht.[768] Die neue Definition des Art. 1 lit. e) der 2. GWRL folgte diesem Trend und sah nun jede Form der kriminellen Beteiligung an der Begehung einer schweren Straftat als kriminelle Aktivität an. Er enthielt außerdem einen Katalog an Straftatbeständen, die *mindestens* als schwere Straftat in diesem Sinne gelten müssten.

dd. Die Umsetzung der 2. EG-Geldwäscherichtlinie vor dem Hintergrund des 11. Septembers 2001

Die Umsetzung der 2. GWRL in Deutschland wurde flankiert von acht Sonderempfehlungen der FATF, die in einer Sondersitzung zu den Ereignissen des 11. Septembers beschlossen wurden.[769] Für die Einarbeitung in den Text der EU-Richtlinie kamen die Empfehlungen noch zu spät.[770] Es wurde jedoch eine gemeinsame Erklärung des EU-Rats und des EU-Parlaments abgegeben,[771] in der die Wichtigkeit der 2. GWRL zur Bekämpfung der Terrorismusfinanzierung betont wurde.

Der deutsche Gesetzgeber konnte die FATF-Sonderempfehlungen hingegen in der Umsetzungszeit berücksichtigen. Die Implementierung der

766 *Wägenbaur*, EuZW 2002, 293 (296); *Hellwig* AnwBl 2002, 144 (146); *Wegner*, NJW 2002, 794 (795 f.); *Zuck*, NJW 2002, 1397; *Shaugnessy*, Law & Policy in Int. Business 34 (2002), 25 (29, 36 f.) mwN.

767 *Shaugnessy*, Law & Policy in Int. Business 34 (2002), 25 (30 f.); *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 404.

768 *Stefanou/Xanthaki*, J. of Money Laundering Control 3 (2000), 325 (329).

769 Abgedruckt als Annex A in *FATF,* Annual Report 2001-2002.

770 *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 404.

771 *Europäische Kommission,* Erklärung vom 19. November 2001, EU-Doc 14237/01, ADD 1, PV/CONS 69; dt. Übersetzung bei *Busch/Teichmann,* Geldwäscherecht, 2003, S. 124.

Richtlinie war dann auch geprägt von den Anschlägen des 11. Septembers 2001 und erfolgte in engem zeitlichem und inhaltlichem Zusammenhang mit dem Erlass weiterer Novellen im Sicherheitsrecht.[772] So wurden im Jahr 2002 nicht nur das die Richtlinie umsetzende Geldwäschebekämpfungsgesetz[773] erlassen, sondern zuvor auch schon das Terrorismusbekämpfungsgesetz[774] und das Vierte Finanzmarktförderungsgesetz,[775] das besonders aufgrund der Einführung des automatischen Abrufsystems von Kontostammdaten (s. o. I. 1.) für Aufsehen sorgte.[776]

Aufgrund der FATF-Sonderempfehlungen wurden als pflichtenaktivierende Verdachtsfälle neben geldwäscheverdächtigen Handlungen i. S. d. § 261 StGB auch solche Transaktionen miteinbezogen, die im Verdacht standen, der Terrorismusfinanzierung i. S. d. § § 129a, 129b StGB[777] zu dienen, § 6 GwG aF 2003.[778] Entsprechend wurde die Anzeigepflicht von Verdachtsfällen angepasst und nun ebenfalls auf die Fälle der Terrorismusfinanzierung erweitert, § 11 GwG aF 2003. Weitere Änderungen betrafen die Identifizierungspflicht, die nunmehr, ganz dem „Know-Your-Customer"[779]-Prinzip folgend[780], nicht erst bei bestimmten Einzahlungen entstand, sondern bei jeder Eröffnung einer Geschäftsbeziehung, § 2 GwG aF 2003.

Von ganz besonderer Bedeutung war weiter die Einführung einer zentralen Stelle für die Sammlung der Verdachtsanzeigen in § 5 GwG aF 2003. Hiermit wurde Empfehlung Nr. 23 der 40 FATF-Empfehlungen aus dem Jahr 1989 umgesetzt, die zwar nicht unmittelbar Einzug in die Geldwäsche-

772 hierzu *Schily*, WM 2003, 1249 (1250 f.); *Jahn*, ZRP 2002, 109 (109 f.); *Herzog/Christmann*, WM 2003, 6; *Hetzer*, ZRP 2002, 407 (408).

773 Gesetz zur Verbesserung der Bekämpfung der Geldwäsche und der Bekämpfung der Finanzierung des Terrorismus (Geldwäschebekämpfungsgesetz) vom 08. August 2002 (BGBl. I S. 3105).

774 Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 9. Januar 2002 (BGBl. I, S. 361).

775 Gesetz zur weiteren Fortentwicklung des Finanzplatzes Deutschland (Viertes Finanzmarktförderungsgesetz) vom 21 Juni 2002 (BGBl. I, S. 2010).

776 Nachweise bei *Kokemoor*, BKR 2004, 135.

777 §129b StGB wurde neu eingeführt durch das 34. Strafrechtsänderungsgesetzes vom 22. August 2002 (BGBl. I 3390); zum Zusammenhang mit den übrigen Sicherheitsgesetzen aus dem Jahr 2002: *Schily*, WM 2003, 1249 (1250 f.).

778 *Busch/Teichmann,* Geldwäscherecht, 2003, S. 43 Rn. 87.

779 Siehe *Spoerr* in BeckOK Datenschutzrecht, Grundlagen Syst. J Rn. 150; *Ruce*, Banking Law Journal 128 (2011), 548 (554); *Nave* CB 2018, 166 (167); *Kerber/Quintus* in Hauschka/Moosmayer/Lösler (Hrsg.), Hdb. Haftungsvermeidung, 3. Aufl. 2016, § 55 Rn. 19.

780 *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 408.

richtlinie der EG/EU gefunden hatte, aber nach Ansicht der Bunderegierung auch auf europäischer Ebene „konsentiert" war.[781] Die zentrale Meldestelle, schon damals Financial Intelligence Unit (FIU) genannt[782], wurde beim BKA eingerichtet. Hier wurde schon seit dem September 2000 eine Verbunddatei von GwG-Verdachtsmeldungen geführt, die bis dahin von den Landeskriminalämtern übermittelt wurden.[783]

Aus grundrechtlicher Perspektive zentral war die Änderung des § 14 Abs. 2 Nr. 2 GwG aF 2003, die Hand in Hand ging[784] mit dem zuvor durch das vierte Finanzmarktförderungsgesetz eingeführten § 25a Abs. 1 Nr. 4 KWG 2002. Die Normen sahen jeweils fast gleichlautend vor, dass die Verpflichteten „interne Grundsätze, angemessene und geschäfts- wie kundenbezogene Sicherungssysteme sowie Kontrollen zur Verhinderung von Geldwäsche und Terrorismusfinanzierung" entwickeln. Die Bundesregierung beschrieb die Änderung des § 14 Abs. 2 GwG in der Begründung zum Entwurf als bloße Konkretisierung der Norm in ihrer ursprünglichen Fassung.[785] In der Begründung zu § 25a KWG hatte sie jedoch schon selbst festgestellt, dass zu den internen Sicherungsmaßnahmen auch EDV-gestützte Systeme gehören, die eine umfassende Risikoanalyse der Kundenumsätze vornahmen.[786]

Die Begriffe *Monitoring* und *Screening* wurden zunächst weiterhin noch undifferenziert verwendet[787] und bezogen sich zumeist einheitlich und allgemein auf die Überwachung von Transaktionen mittels EDV-Systemen und manueller Prüfungen. Heutzutage definiert die BaFin das Screening als die Echtzeitkontrolle von Überweisungen, die meist dem automatischen Verweigern von verbotenen Transaktionen, etwa aufgrund eines Embargos, dient.[788] Unter Monitoring hingegen fasst sie den Vorgang der nachträglichen Kontrolle getätigter Zahlungen zusammen, unabhängig davon, ob dies automatisch bzw. digital oder manuell geschieht.[789]

781 BT-Drs. 14/8739, S. 13.
782 Idem, S. 2, 10, 13.
783 Idem, S. 13.
784 *Degen,* Geldwäsche, 2009, S. 190 ff.; *Herzog/Christmann*, WM 2003, 6 (11).
785 BT-Drs. 14/8739, S. 17; BT-Drs. 14/9043, S. 11.
786 BT-Drs. 14/8017, S. 125.
787 Hierzu schon *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 642 ff. Rn. 8.77.
788 *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14.
789 Ibid.

Die Auswirkungen der Monitoringpflicht wurden kontrovers diskutiert. Die Kritiker – etwa der Bundesrat[790] – befürchteten in den neuen Gesetzen eine Verpflichtung zur Rasterfahndung privater Bankkonten durch die Verpflichteten.[791] In der Literatur war gar von einer „Entfesselung des Rechtsstaats" die Rede.[792] (Ausführlich zur Entwicklung der Diskussion siehe Kap. F. II. 4).

ee. Die dritte Geldwäscherichtlinie

Im Jahr 2005 wurde dann die Harmonisierung der Bekämpfung von Geldwäsche und Terrorismusfinanzierung auf europäischer Ebene durch die Einführung der dritten[793], nunmehr, *EU*-Geldwäscherichtlinie weiterentwickelt. Da die 2. GWRL vor dem 11. September 2001 formuliert wurde, kam es erst mit der 3. GWRL zu einer Priorisierung der Terrorismusbekämpfung.[794] Mit der neuen Richtlinie sollten tiefgreifende Änderungen der Geldwäschebekämpfung eingeführt werden, weshalb die ersten beiden Richtlinien aufgehoben und durch einen ganz neuen Text ersetzt wurden.[795]

Die bedeutsamsten Änderungen brachte die Richtlinie für die Sorgfaltspflichten, deren Struktur grundlegend erneuert wurde. Die starren Pflichtenregelungen der ersten beiden Richtlinien wurden durch einen neuen, an verschiedenen Risiken orientierten, Ansatz ersetzt, der für verschiedenen Arten von Transaktionen und in Abhängigkeit von den jeweiligen Kunden differenzierte Pflichten vorsah. Der „Rule-Based-Approach" wurde durch den „Risk-Based-Approach" ergänzt bzw. ersetzt.[796]

790 BT-Drs. 14/9043; S. 5 f. zu §14 Abs. 2 Nr. 2 GwG 2002; BT-Drs. 14/8958, S. 2 zu § 25a KWG 2002;

791 *Bergles/Eul*, BKR 2002, 556; *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (72, 77).

792 *Herzog/Christmann*, WM 2003, 6 (6).

793 Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung (ABl. 2005, L 309/15).

794 *Culley*, Irish J. of EU Law 13 (2006), 161 (162); *Mitsilegas/Gilmore*, Int. & Comp. Law Quarterly 56 (2007), 119 (125 ff.).

795 *Herzog/Achtelik* in Herzog GwG, Einl. Rn. 85.

796 *Sotiriadis/Heimerdinger*, BKR 2009, 234 (234); *Costanzo* in Unger (Hrsg.), HdB Money Laundering, 2013, S. 349; *Gürkan,* Geldwäscheprävention, 2019, 95 ff.; Her-

Diesem Prinzip lag nunmehr die Annahme zugrunde, dass nicht alle Kunden und nicht jede Transaktion ab einem bestimmten Wert dasselbe Risiko einer Geldwäsche tragen.[797] Anstatt einheitlicher Regeln sah die Richtlinie deshalb allgemeine (Art. 6-10), vereinfachte (Art. 11-12) und verstärkte Sorgfaltspflichten (Art. 13) vor. Diese verschiedenen Pflichten wiederum waren nicht ausschließlich an starre Kundenkataloge oder Situationen geknüpft, sondern auch an offene Tatbestände.

Eine weitere heikle Neuerung lag in der Einführung einer neuen Kategorie für die Anwendung der Sorgfaltspflichten, nämlich der Geschäftsbeziehungen zu „politisch exponierten Personen."[798] Diese „PEP" wurden durch Art. 3 Nr. 8 der 3. GWRL als *„diejenigen natürlichen Personen, die wichtige öffentliche Ämter ausüben oder ausgeübt haben, und deren unmittelbare Familienmitglieder oder ihnen bekanntermaßen nahestehende Personen"* definiert.

In Anlehnung an die revidierten FATF-Empfehlungen sah die Richtlinie nunmehr auch die Aufstellung von FIUs für die Mitgliedstaaten verbindlich vor, Art. 21 der 3. GWRL. Deren Stellung im System der Geldwäschebekämpfung wurde im Vergleich zum damals geltenden GwG deutlich herausgehoben. Dass diese erheblichen Berechtigungen der FIU nicht von entsprechenden Datenschutzklauseln tangiert wurden, erregte dabei schon früh entsprechende Kritik.[799]

ff. Das Geldwäschegesetz 2008

Die 3. GWRL wurde durch das Geldwäschebekämpfungsergänzungsgesetz (GwBekErgG) vom 13. August 2008[800] in deutsches Recht implementiert. Der Gesetzgeber beabsichtigte dabei eine „Eins-zu-Eins-Umsetzung" der Richtlinie.[801]

---

zog/*Achtelik* in Herzog GwG, Einl. Rn. 86, 157 zu den Begriffen *Ross/Hannan*, J. of Money Laundering Control 10 (2007), 106 (107 ff.).

797 *Herzog/Achtelik* in Herzog GwG, Einl. Rn. 86.

798 Hierzu kritisch *Herzog/Hoch*, WM 2007, 1997 (1999); *Höche*, WM 2005, 8 (12).

799 *Mitsilegas/Gilmore*, Int. & Comp. Law Quarterly 56 (2007), 119 (127).

800 Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Geldwäschebekämpfungsergänzungsgesetz - GwBekErgG) vom 13. August 2008 (BGBl. I S. 1690).

801 Krit. BT-Drs. 16/9631, S. 6; dazu im Einzelnen *Hetzer*, EuZW 2008, 560 (561).

(1) Umsetzung des risikoorientierten Ansatzes

Die Umsetzung sollte demgemäß vor allem dem risikoorientierten Ansatz Rechnung tragen. Zunächst werden die Sorgfaltspflichten untergliedert in allgemeine Sorgfaltspflichten (§ 3 GwG 2008), vereinfachte Sorgfaltspflichten (§ 5 GwG 2008) und verstärkte Sorgfaltspflichten (§ 6 GwG 2008). Die allgemeinen Sorgfaltspflichten treffen grundsätzlich alle Verpflichteten, aber nur in einer begrenzten Anzahl an Situationen, die in § 3 Abs. 2 GwG 2008 aufgezählt wurden.

Diese Eins-zu-Eins aus der 3. GWRL (dort Art. 7) übernommenen Situationen wiederum lassen sowohl einen regel- als auch risikobasierten Ansatz erkennen.[802] So waren die Sorgfaltspflichten regelmäßig bei allen Transaktionen über 15.000 € und bei jeder Begründung einer Geschäftsbeziehung zu erfüllen. Im Übrigen müssen sie erfüllt werden, wenn der Verdacht von Geldwäsche oder Terrorismusfinanzierung aufgrund (sonstiger) Tatsachen besteht, oder wenn Zweifel an der Identität des Vertragspartners bzw. des wirtschaftlich Berechtigten bestehen. Darüber hinaus sah § 3 Abs. 4 GwG 2008 vor, dass die konkrete Anwendung der Sorgfaltspflichten an dem jeweils entsprechenden Risiko des Einzelfalls auszulegen hat.

(2) Die allgemeinen Sorgfaltspflichten: *Kontinuierliche Überwachung*

Die allgemeinen Sorgfaltspflichten wurden in § 3 i. V. m. § 4 GwG 2008 festgelegt und setzten Art. 8 der 3. EU-Geldwäscherichtlinie mit nahezu identischem Wortlaut um. Die allgemeinen Sorgfaltspflichten umfassten danach *die Identifizierung des Vertragspartners* bzw. des wirtschaftlich Berechtigten (nach Maßgabe des § 4 GwG 2008), die *Einholung von Informationen über den Zweck und die angestrebte Art der Geschäftsbeziehung*, die *Abklärung, ob der Vertragspartner für einen wirtschaftlich Berechtigten* handelt, sowie die *kontinuierliche Überwachung der Geschäftsbeziehung, einschließlich der in ihrem Verlauf durchgeführten Transaktionen*.

Die Identifizierungspflicht lag trotz einer Erweiterung bei der Betrachtung des wirtschaftlich Berechtigten. Es wurde nunmehr nicht nur noch

802 *Gürkan,* Geldwäscheprävention, 2019, S. 228; *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 461; *Ackermann/Reder*, WM 2009, 158 (166 f.).

zwischen der auftretenden Person und dem eigentlichen Vertragspartner unterschieden[803] – nichts grundsätzlich Neues.[804]

Dasselbe lässt sich über die, kontinuierliche Überwachungspflicht nach 3 Abs. 1 Nr. 4 GwG 2008 sagen,[805] die im Fokus dieser Arbeit steht. Schließlich war das sogenannte *Kontenscreening* und -*Monitoring*[806] ja zuvor schon in § 14 Abs. 2 Nr. 2 GwG 2002, § 25a Abs. 1 S. 1Nr. 4 KWG 2002[807] vorgesehen[808], und bereits seit Ende der 1990er Jahre vom BAKred etabliert.[809] Die Überwachungspflicht wurde aber durch die Einführung gleich mehrerer neuer Vorschriften deutlich ausdifferenzierter.[810]

Hierbei wurde abermals versäumt, das Verhältnis des Monitorings als interne Sicherungsmaßnahme zu der neu eingeführten Überwachungspflicht (als allgemeine Sorgfaltspflicht) verständlich im Gesetz zu regeln. Über die Definitionen dieser Begrifflichkeiten herrschte daher noch immer keine Klarheit.[811]

(3) Aufzeichnungs- und Aufbewahrungspflicht

In § 8 Abs. 3 GwG 2008 wurde weiter eine umfangreiche fünfjährige Aufzeichnungs- und Aufbewahrungspflicht bezüglich aller „sonstigen" im Rahmen der Sorgfaltspflichten erhobenen Angaben und eingeholten Informationen über Vertragspartner, wirtschaftlich Berechtigte, Geschäftsbeziehungen und Transaktionen eingeführt. Durch die Einbeziehung von sonstigen Belegen und Aufzeichnungen über Geschäftsbeziehungen und Transaktio-

803 BT-Drs. 16/9038, S. 38.
804 *Sotiriadis/Heimerdinger*, BKR 2009, 234 (236).
805 *Ackermann/Reder*, WM 2009, 158 (164); *Achtelik* in Herzog GWG, 1. Aufl. 2010, § 25c KWG Rn. 2.
806 nach *Achtelik* in Herzog GWG, 1. Aufl. 2010, § 25c KWG Rn. 2 werden diese Begriffe undifferenziert konvergent verwendet; heutige Definition bei *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14.
807 Später § 25a Abs. 1 Satz 3 Nr. 6 KWG (2005) bzw. § 25a Abs. 1 Satz 6 Nr. 3 KWG (2007). Zur Änderungsgeschichte *Achtelik* in Herzog GWG, 1. Aufl. 2010, § 25c KWG Rn. 15; *ders.* in Herzog GwG, 3. Aufl. 2018, KWG § 25h Rn. 1 f.
808 Hierzu *Jahn*, ZRP 2002, 109 (110); *Herzog/Christmann*, WM 2003, 6 (11).
809 Dazu nur *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 611 ff.; *Herzog*, WM 1996, 1753; *ders.*, WM 1999, 1905.
810 *Achtelik* in Herzog GWG, 1. Aufl. 2010, § 25c KWG Rn. 14.
811 Schon *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 642 ff. Rn. 8.77.

nen wurde die bisher in § 9 GwG 2002 geregelte Aufzeichnungs- und Aufbewahrungspflicht erweitert.[812]

Der Wortlaut wurde somit in Bezug auf Transaktionsbelege der Richtlinie angepasst. Die Aufzeichnung und Aufbewahrung waren aber – anders als bei Art. 30 lit. b) der 3. EU-Geldwäscherichtlinie – weiterhin an die Ausführung einer Sorgfaltspflicht geknüpft. Dennoch wollte die Bundesregierung mit der Neuschaffung des § 8 Abs. 3 GwG 2008 auf Art. 30 lit. b) der 3. EU-Geldwäscherichtlinie reagiert haben.[813]

Offenbar hatte die Bundesregierung die zuvor vertretene Auffassung aufgegeben, dass eine umfassende Speicherpflicht im GwG neben § 257 HGB gänzlich entbehrlich wäre.[814] Die Einführung einer eingeschränkten Speicherpflicht in Abhängigkeit von den Sorgfaltspflichten erscheint vor diesem Hintergrund als Kompromiss.

Der genaue Umfang der geldwäscherechtlichen Aufzeichnungs- und Aufbewahrungspflicht, insbesondere die inhaltliche Abgrenzung zu den umfassenden Aufbewahrungspflichten, etwa aus § 257 HGB, blieb damit weiterhin schwammig. Weder aus den Gesetzesmaterialien noch aus der zeitgenössischen Literatur lässt sich einheitlich erkennen, ob sich eine Auszeichnungspflicht für sämtliche Transaktionen aus dem GwG ergab, oder diese (wie bislang) nur auf solche Informationen beschränkt war, die im Rahmen der Erfüllung von Sorgfaltspflichten anfielen.

Die Opposition in Gestalt der FDP-Fraktion äußerte sich zu der Erweiterung des § 8 GwG entsprechend kritisch und befürchtete, dass die neue Regelung als „unbegrenzte Verpflichtung zur Datensammlung und -aufbewahrung" verstanden werden könnte.[815] Sie beantragte deshalb eine Änderung des Entwurfs zu § 8 GwG 2008 dahingehend, dass die Aufzeichnungspflicht nicht für die Überwachungspflicht nach § 3 Abs. 1 Nr. 4 GwG 2008 gelten sollte, sondern nur für die übrigen Sorgfaltspflichten.[816]

812 *Warius* in Herzog GWG, 1. Aufl. 2010, § 8 GWG Rn. 1.
813 BT-Drs. 16/9038, S. 42.; *Ackermann/Reder*, WM 2009, 200 (208) *Warius* in Herzog GWG, 1. Aufl. 2010, § 8 GWG Rn. 19.
814 So noch BT-Drs. 12/2704, S. 16.
815 BT-Drs. 16/9647, S. 3.
816 Idem, S. 4.

gg. Die vierte EU-Geldwäscherichtlinie

Als Reaktion auf die „FATF-Empfehlungen 2012“[817] beschloss die EU-Kommission, das europäische Regelwerk zur Geldwäschebekämpfung zu evaluieren und beauftragte eine große Beratungsfirma mit der Erstellung eines entsprechenden Gutachtens[818]. Obwohl dieses feststellte, dass die 3. GWRL eine effektive Geldwäschebekämpfung gewährleistete, war man sich bei der Kommission sicher, dass die Effektivität und Einheitlichkeit innerhalb der Union noch gesteigert werden müssten, um dem neuen internationalen Standard zu entsprechen.[819] Die EU-Kommission beschloss daher eine Neuauflage der Geldwäscherichtlinie.[820] In der Folge wurde die 3. GWRL im Mai 2015 aufgehoben und wiederum durch einen gänzlich neuen Gesetzestext in der 4. EU-Geldwäscherichtlinie[821] ersetzt.

Diese (in großen Teilen noch heute aktuelle) 4. GWRL basiert weiterhin auf dem risikoorientierten Ansatz bzw. versucht, diesen gegenüber ihrer Vorgängerrichtlinie sogar noch verstärkt zum Ausdruck kommen zu lassen.[822] Die Unterscheidung zwischen allgemeinen, vereinfachten und verstärkten Sorgfaltspflichten, abhängig vom jeweiligen Risiko der Geschäftsbeziehung bzw. Transaktion wird entsprechend beibehalten. Erstmals aber enthielt die Richtlinie im Anhang Faktoren bzw. Variablen, mit denen sich die Risiken von Geldwäsche und Terrorismusfinanzierung bewerten lassen. Anstatt einer weithin regelbasierten Einteilung in die einzelnen Risikogrup-

817 *FATF,* Recommendations 2012, orig. Fassung Feb. 2012; überarbeitet *dies.,* Recommendations 2012, konsolidierte Fassung März 2022.

818 *Deloitte*, AML Study, 2011.

819 *Steenwijk* in Zwaan/Lak/Makinwa ua. (Hrsg.), Governance and Security, 2016, S. 209 (219); *Europäische Kommisison*, COM(2013) 45 final, 2013/0025 (COD), S. 2.

820 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, COM(2013) 45 final, 2013/0025 (COD).

821 Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, ABl. 2015, L 141/73

822 *Ruppert*, DStR 2015, 1708 (1709); *Frantangelo* in Siclari (Hrsg.), Anti-Money-Laundering, 2016, S. 11 (11 f.); *Rößler*, WM 2015, 1405 (1407); kritisch ob dies gelingt: *Steenwijk* in Zwaan/Lak/Makinwa ua. (Hrsg.), Governance and Security, 2016, S. 209 (222).

pen sollte die Bewertung künftig noch dichter am Einzelfall ausgerichtet sein.

Die Stellung der zentralen Meldestellen wurde weiter gestärkt. Diese waren nunmehr als unabhängige, eigenständig arbeitende Behörden zu organisieren, Art. 32 Abs. 3 der 4. GWRL. Ihnen wurde nach Art. 32 Abs. 3 a. E. der 4. GWRL das Recht eingeräumt, von den Verpflichteten zusätzliche Informationen einzuholen und im *„Falle des Verdachts, dass eine Transaktion mit Geldwäsche oder Terrorismusfinanzierung zusammenhängt, unmittelbar oder mittelbar Sofortmaßnahmen zu ergreifen, um die Zustimmung zu einer laufenden Transaktion zu versagen oder auszusetzen, damit sie die Transaktion analysieren, dem Verdacht nachgehen und die Ergebnisse der Analyse an die zuständigen Behörden weitergeben kann"*, Art. 32 Abs. 7 der 4. GWRL.

Relevante Änderungen gab es weiter hinsichtlich der organisatorischen Pflichten im Vorfeld und im Nachhinein der Anwendung von Sorgfaltspflichten und zwar sowohl für die Staaten selbst als auch für die Verpflichteten. Diese Änderungen sind im Kontext des verstärkten risikoorientierten Ansatzes zu lesen. Da die Anwendung der verschieden intensiven Sorgfaltspflichten stärker am individuellen Risiko auszurichten ist, mussten die Pflichten zur Risikoerkennung entsprechend verschärft werden.[823]

Das Verhältnis des Geldwäscherechts zum Datenschutz wurde im Vorfeld der vierten Richtlinie schwerpunktmäßig diskutiert.[824] Dass sich der europäische Gesetzgeber der Datenproblematik bewusst war, ergibt sich allein daraus, dass er das Richtlinienkapitel V in „Datenschutz, Aufbewahrung von Aufzeichnungen und statistische Daten", Art. 40-44 der 4. GWRL, umbenannt hatte. Am Umfang der Aufbewahrungspflicht, Art. 40 Abs. 1 der 4. GWRL, hatte sich aber faktisch nicht geändert. Lediglich die Weitergabe der Informationen war auf die Zwecke der „Verhinderung, Aufdeckung und Ermittlung möglicher Geldwäsche oder Terrorismusfinanzierung durch die zentrale Meldestelle oder andere zuständige Behörden" beschränkt.

823 Vgl. *Tonnara* in Siclari (Hrsg.), Anti-Money-Laundering, 2016, S. 57 (61 f.); *Mitsilegas/Vavoula* Maastricht J. of EU and Comp. Law 23 (2016), 261 (267 f.).

824 *Rößler*, WM 2015, 1405 (1411 f.).

hh. Das Geldwäschegesetz 2017

Das vierte Geldwäschegesetz wurde im Juni 2017 durch eine Neufassung des GwG in deutsches Recht umgesetzt.[825] Da die Grundstruktur des GwG – insbesondere der Inhalt und die Systematik der für diese Arbeit relevanten Regelungen – seitdem kaum geändert wurden, soll hier in überschaubarem Umfang über die wesentlichen Änderungen referiert werden. Eine umfangreiche Darstellung des aktuellen GwG erfolgt an späterer Stelle (s. III. 2. b.).

Die Änderungen betrafen zunächst die FIU, die nun nicht mehr Zentralstelle *für Verdachtsmeldungen,* sondern *für Finanztransaktionsuntersuchungen* hieß. Sie wurde vom BKA ausgelöst und beim Zollkriminalamt angesiedelt, § 5a FVG, arbeitete jedoch ausdrücklich als eigenständige, unabhängige Organisationseinheit, als „Behörde in der Behörde"[826], im Geschäftsbereich des Bundesministeriums und war von der Fachaufsicht zumindest partiell befreit, §§ 27 Abs 2, 28 Abs. 2 GwG 2017. [827]

Neben dieser strukturellen Änderung wurden auch die Aufgaben und Aktivitäten der FIU in Umsetzung der Richtlinie neu organisiert. Nach § 28 GwG 2017 hatte die FIU die *„Aufgabe der Erhebung und Analyse von Informationen im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung und der Weitergabe dieser Informationen an die zuständigen inländischen öffentlichen Stellen zum Zwecke der Aufklärung, Verhinderung oder Verfolgung solcher Taten.*" Die Maßnahmen, mit denen die FIU dieser Aufgabe nachzukommen hat, wurden in § 28 Abs. 1 S. 2 GwG 2017 katalogisiert und in den §§ 29 ff. GwG 2017 ausgebreitet. Ihre neuen Kompetenzen gingen deutlich über jene des BKAs und der Strafverfolgungsbehörden hinaus.[828]

Insbesondere wird die Arbeit der FIU nicht auf die Aufklärung und Verhinderung von Geldwäsche beschränkt. Sie hat nach § 28 Abs. 3 GwG 2017 auch hinsichtlich der allgemeinen Gefahrenabwehr und Strafverfolgung

825 Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen vom 23. Juni 2017 (BGBl. I, S. 1822).

826 BT-Drs. 18/11555, S. 90.

827 Hierzu *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (224); *Spoerr/Roberts*, WM 2017, 1142 (1143); zur Kritik *Da Barreto Rosa* in Herzog GwG, § 27 GWG Rn. 7.

828 *Spoerr/Roberts*, WM 2017, 1142 (1148).

mit den hierfür zuständigen Behörden zusammenzuarbeiten.[829] Das zeigt sich insbesondere in § 32 Abs. 3 Nr. 2 GwG, nach dem die FIU auch zur *Aufklärung sonstiger Gefahren und die Durchführung von anderen Strafverfahren* (die nicht im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung stehen) Daten auf Ersuchen bestimmter Sicherheitsbehörden übermitteln soll.

Aufgrund dieser Regelungen war nun zweifelhaft, ob der FIU weiterhin lediglich eine *Filterfunktion* zukam,[830] oder ob sie nicht eher als eine Art *Finanzgeheimdienst* eingestuft werden müsste (dazu ausf. Kap. G. III. 3. b. bb.).[831]

Neu war auch das aufgrund des Art. 30 der 4. GeldwäscheRL einzuführende Transparenzregister in den §§ 18 ff. GwG 2017. In dieses waren nunmehr Informationen über den wirtschaftlichen Berechtigten einzutragen, und zwar nicht nur von den Verpflichteten nach § 2 GwG 2017, sondern von allen juristischen Personen des Privatrechts, § 20 Abs.1 GwG 2017.[832] Das Transparenzregister schuf somit eine zentrale Schnellübersicht über sämtliche juristische Personen des Privatrechts, in der die wichtigsten Basisinformationen sowie alle geldwäscherelevanten Daten gebündelt hinterlegt wurden. Zur Einsichtnahme, soweit dies zu deren Aufgabenerfüllung erforderlich war, wurden insbesondere die FIU, die Strafverfolgungsbehörden und die Gefahrenabwehrbehörden ermächtigt, § 23 GwG 2017.

Auf das Transparenzregister wurde in der deutschsprachigen Literatur besonders kritisch reagiert.[833] Dabei wurde insbesondere auch ein konkreter Zusammenhang mit der Rechtsprechung des EuGH zur Vorratsdatenspeicherung (von TK-Verkehrsdaten) hergestellt. Da das Register keinerlei Differenzierungen enthalte, stelle es anlasslos private Daten für sämtliche staatliche Behörden inklusive Sicherheitsbehörden zur Verfügung.[834] Es greife daher in unverhältnismäßiger Weise in Art. 7, 8 EU-GRC ein.[835] Die-

829 s.a. *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (224 f.).
830 So BT-Drs. 18/11555, S. 90
831 Vgl. *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (249 f.); *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21.
832 Hierzu *Diller/Brauneisen/Hütten* NZA 2017, 1512 (1513).
833 *N. Müller*, NZWiSt 2017, 87 (91 ff.) *dies*., NZWiSt 2017, 121; *Escher-Weingart/M. Stief*, WM 2018, 693 (697 ff.); *Spoerr/Roberts*, WM 2017, 1142 (1148).
834 *N. Müller*, NZWiSt 2017, 121 (122).
835 Idem, (122).

ser Auffassung hat sich der EuGH jüngst angeschlossen und die Regelungen als grundrechtswidrig und nichtig erklärt.[836]

ii. Die fünfte Geldwäscherichtlinie, EU-FinanzinformationsRL und das aktuelle GwG

Die GWRL wurde im Juli 2018 zuletzt geändert. Aktuell liegt sie somit in der fünften Fassung vor,[837] wobei kein völlig neuer Gesetzestext geschaffen, sondern nur die 4. GWRL in Teilen geändert bzw. ergänzt wurde.

Die aus sicherheitsrechtlicher Perspektive bedeutsamste Änderung lag in der Einführung des Art. 32 Abs. 9 GWRL. Nach dieser Vorschrift kann *jede zentrale Meldestelle im Rahmen ihrer Aufgaben unbeschadet des Artikels 34 Absatz 2 von jedem Verpflichteten Informationen für (sic) den in Absatz 1 genannten Zweck anfordern, einholen und nutzen, selbst wenn keine vorherige Meldung gemäß Artikel 33 Absatz 1 Buchstabe a oder Artikel 34 Absatz 1 erstattet wurde.* Damit sah die GWRL erstmals ausdrücklich eine umfangreiche Zugriffsmöglichkeit der FIUs auf Informationen der Verpflichteten vor, die konkrete Anforderungen sowohl in materieller als auch formeller Hinsicht vermissen ließ.

Aufgrund der Richtlinie wurde das GwG im Dezember 2019 novelliert.[838] Eine Umsetzung des 32 Abs. 9 GWRL war nicht notwendig, da in § 30 Abs. 3 GwG bereits eine entsprechende Zugriffsnorm enthalten war.

Zu einer wichtigen Änderung kam es aber im Rahmen des Erlasses der EU-Finanzinformationsrichtlinie (FinanzinformationsRL). [839] In dieser

836 EuGH, Urt. v. 22.11.2022 – C-37/20, C-601/20 (WM ua/Luxembourg Business Registers) = NJW 2023, 199.

837 Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU, ABl. 2018, L 156/43.

838 Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie vom 12. Dezember 2019, BGBl. I 2602; hierzu *Glaab/Neu/Scherp* BB 2020, 322; *Feiler/J.-W. Kröger*, CCZ 2019, 262.

839 Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten und zur Aufhebung des Beschlusses 2000/642/JI des Rates, ABl. 2019, L 186/122.

wurden die Mitgliedstaaten verpflichtet, Vorschriften zu erlassen, die es den nationalen Sicherheitsbehörden erleichtern sollten, auf die Daten der FIU zur Bekämpfung schwerer Kriminalität zuzugreifen, also nicht nur zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung.[840] Aus dieser Zielsetzung ergab sich, dass der europäische Gesetzgeber offenbar bislang davon ausgegangen war, dass die auf Grundlage der GWRL erhobenen Informationen ausschließlich für diese Zwecke möglich war.[841]

Ausgehend von Art. 3 FinanzinformationsRL soll eine solche Übermittlung aber nur an ausdrücklich benannte Behörden zulässig sein. Darüber hinaus sieht die Richtline eine Reihe von Anforderungen, Art. 5, und Verfahrensvorschriften vor, etwa eine Protokollpflicht, Art. 6.

In Deutschland ist eine Umsetzung der FinanzinformationsRL durch die Einführung des § 32 Abs. 3a GwG erfolgt.[842] Als Behörde wurde das BKA benannt, § 3 Abs. 2a S. 2 BKAG. Weiterhin aber ist nach § 32 Abs. 3 Nr. 2 GwG eine Übermittlung auch zur Aufklärung sonstiger Gefahren und Bekämpfung sämtlicher Strafverfahren an die in § 32 Abs. 3 S. 1 GwG benannten Behörden (Strafverfolgungsbehörden, Bundesverfassungsschutz, BND und MAD) möglich. In Deutschland kann also keine Rede davon sein, dass erst im Rahmen der FinanzinformationsRL eine Übermittlung zu anderen Zwecken als der Bekämpfung von Geldwäsche und Terrorismusfinanzierung ermöglicht wurde.

Diese Diskrepanz weckt ernsthafte Zweifel an der Unionsrechtsmäßigkeit der Übermittlungsregeln des GwG (dazu Kap. G. III. 2. c. cc.).

840 Vgl. BT-Drs. 19/28164, S. 30.

841 Vgl. Erwägungsgrund Nr. 15, FinanzinformationsRL.

842 Gesetz zur europäischen Vernetzung der Transparenzregister und zur Umsetzung der Richtlinie 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Nutzung von Finanzinformationen für die Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstigen schweren Straftaten (Transparenzregister- und Finanzinformationsgesetz) vom 25.06.2021 (BGB I, S. 2083); dazu BT-Drs. 19/28164, S. 54.

jj. Ein Blick in die Zukunft

Noch während der Bearbeitung dieser Arbeit, am 20. Juli 2021, hat die Kommission eine Vorlage für eine Geldwäscheverordnung vorgelegt.[843] Diese soll die GeldwäscheRL aber nur teilweise ablösen. [844] Die GeldwäscheRL soll stattdessen in Form der 6. GWRL ebenfalls neu gefasst werden.[845] Die Regeln zu den Verpflichteten und deren Sorgfaltspflichten sollen zukünftig in der Geldwäscheverordnung – GWVO geführt werden. Die Richtlinie enthält dann noch die allgemeinen Vorgaben zur supra- und nationalen Risikoanalyse sowie zu den verschiedenen Registern – außerdem die Vorgaben zu den FIUs.

Darüber hinaus will die Kommission die Grundlage für eine eigene EU-Behörde bzw. FIU mit dem Namen *Authority for Anti-Money Laundering and Countering the Financing of Terrorism* (AMLA) schaffen.[846] Auf diese sollen die Kompetenzen der Europäischen Bankenaufsichtsbehörde im Bereich der Geldwäsche- und Terrorismusfinanzierung übertragen werden.[847]

Die GeldtransferVO soll ebenfalls erneuert, allerdings nicht neu gefasst, sondern nur ergänzt werden.[848] Die Ergänzung erweitert den Anwendungsbereich der Verordnung auf den Transfer bestimmter Kryptowährungen.

Inhaltliche Änderungen der Überwachungs- oder der Aufzeichnungs- und Aufbewahrungspflicht finden sich in den Gesetzesvorschlägen nicht. Die Regelung der Überwachungspflicht als allgemeine Sorgfaltspflicht in

843 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, 20. Juli 2021, COM(2021) 420 final, 2021/0239 (COD).

844 Übersicht bei *Europäische Kommission,* Anti-money laundering and countering the financing of terrorism legislative package, 20.07.2021, https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en, zuletzt aufgerufen am 12.01.2025; dazu *Brian/Frey/Pelz*, CCZ 2021, 209.

845 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die von den Mitgliedstaaten einzurichtenden Mechanismen zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Aufhebung der Richtlinie (EU) 2015/849, 20. Juli 2021, COM(2021) 423 final, 2021/0239 (COD),

846 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung der Behörde zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010, 20. Juli 2021, COM(2021) 421 final, 2021/0240 (COD).

847 Idem, S. 29.

848 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte (Neufassung), 20. Juli 2021, COM(2021) 422 final, 2021/0241 (COD).

Art. 13 Abs. 1 lit. c) GWRL soll in Art. 16 Abs. 1 lit. (d) GWVO fast wortgleich übernommen werden. Die Änderungen sind redaktioneller Natur. Dem Umfang der Überwachungspflicht soll sich zwar künftig ein eigener Art. 21 GWVO widmen. Dieser betrifft aber vor allem die genauen Umstände über die Pflicht zur Aktualisierung der Kundendaten. Auf den Ablauf des Monitorings soll er sich offensichtlich nicht auswirken. Auch die Vorschrift des Art. 13 Abs. 3 GWRL, der eine Mindestpflicht zur Überwachung bei Anwendung vereinfachter Sorgfaltspflichten vorsieht, soll beibehalten werden und findet sich im neuen Art. 27 Abs. 1 UABs. 2 GWVO.

Die verstärkte Überwachungspflicht, bislang in Art. 18 Abs. 2 GWRL geregelt, bleibt ebenfalls erhalten, die risikoorientierte Anwendung wird aber spezifiziert. Im vorgeschlagenen Art. 28 Abs. 4 GWVO findet sich ein Katalog an Maßnahmen, die von den Verpflichteten in den Situationen, die eine verstärkte Sorgfaltspflicht auslösen, angewandt werden können. Der Wortlaut „apply any of these measures" impliziert dabei aber, dass nicht alle Maßnahmen kumuliert ergriffen werden müssen, sondern zur Auswahl der Verpflichteten stehen. Insoweit könnte die Pflicht zur verstärkten Überwachung abgeschwächt werden. Allerdings werden die verstärkten Sorgfaltspflichten bei Korrespondenzbankbeziehungen und PEP in eigene Artikel ausgegliedert (Art. 31 und 32) und sehen weiterhin strikt anzuwendende, verstärkte Sorgfaltspflichten vor.

Die Aufzeichnungs- und Aufbewahrungspflicht des Art. 40 GWRL ist wortgleich in Art. 56 GWVO enthalten.

Soweit sich aus dem aktuellen Anti-Geldwäscherecht eine umfassende Pflicht zur Speicherung von Kontoinhaltsdaten ergibt, ist also auch von den Gesetzesvorschlägen keine Änderung zu erwarten. Sie unterscheiden sich insofern nicht von dem aktuellen Regelwerk, das im folgenden Abschnitt erläutert werden soll.

b. Die Sorgfaltspflichten als Leitsystem des GwG: insbesondere *kontinuierliche Überwachung*

Der Kern des deutschen Anti-Geldwäscherechts ist (noch) das GwG. Ziel des GwG ist die Verhinderung von *Geldwäsche* und *Terrorismusfinanzierung*. Diese Begriffe werden in § 1 Abs. 1, 2 GwG legaldefiniert. Hinsichtlich der Geldwäsche wird auf § 261 StGB verwiesen. Dort findet sich der entsprechende Straftatbestand.

Die Terrorismusfinanzierung ist nach § 89c StGB ebenfalls strafbewehrt, allerdings geht die Definition des GwG über diesen Straftatbestand hinaus. So gilt nach § 1 Abs. 2 GwG nicht bloß die *Begehung einer Tat nach § 89c StGB* als Terrorismusfinanzierung, sondern auch das „*Bereitstellen oder Sammeln von Vermögensgegenständen mit dem Wissen oder in der Absicht, dass diese Vermögensgegenstände ganz oder teilweise dazu verwendet werden oder verwendet werden sollen*" eine Tat nach §§ 129a, 129b StGB oder Art. 3, 5-10 und 12 der Terrorismusbekämpfungsrichtlinie 2017[849] zu begehen.

Trotz mancher Divergenzen sind sämtliche in dieser Richtlinie aufgeführten Taten nach den §§ 89c, 129a, 129 StGB strafbewehrt, allerdings nicht immer explizit als terroristische Straftaten.[850] Durch den Verweis in § 1 Abs. 2 Nr. 1 lit. b) GwG auch auf die Terrorismusbekämpfungsrichtlinie wird der Begriff der Terrorismusfinanzierung mithin erweitert.[851] Auf die strafrechtlichen Feinheiten soll indes hier nicht eingegangen werden. Aufgrund der Verweisungen ist § 1 Abs. 2 GwG jedenfalls so weitreichend, dass sämtliche vollendete oder versuchte Vermögensabflüsse im Zusammenhang mit einer terroristischen Tat (im deutschen oder EU-Sinne) unter Terrorismusfinanzierung gefasst werden können.[852] Um diese Vermögensflüsse aufzudecken und somit Straftaten ermittelt oder verhindert werden können, versucht das GwG, den Geldfluss transparent zu machen, indem es die unmittelbar am Geldfluss Beteiligten zu bestimmten Maßnahmen verpflichtet.[853] Es handelt sich also um eine sicherheitsrechtliche Begrenzung der Heimlichkeit bestimmter wirtschaftlicher Vorgänge und somit der informationellen Selbstbestimmung (zur bisherigen Diskussion s. Kap. F. II.).[854]

Im vorangegangenen Abschnitt wurde die Entwicklung des GwG beschrieben. Dabei wurde an mancher Stelle bereits deutlich gemacht, dass

---

849 Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. 2017, L 88/6.

850 *Engelstätter*, GSZ 2019, 95 (97 ff.).

851 „konturenlos" nach *Häberle* in Erbs/Kohlhaas Nebengesetze, GWG § 1 Rn. 3.

852 *Stegmann/Meuer* in Bürkle (Hrsg.), Compliance, 3. Aufl. 2020, § 12 Rn. 6.

853 *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 179.

854 Allg. zu diesem Spannungsverhältnis *Herzog/Achtelik* in Herzog GwG, Einl. Rn. 162 ff.; *Werner,* Geldwäsche, 1996, S. 94 ff.; *Kirchhof* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 79 (88 f.); *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95; *Häberle* in Erbs/Kohlhaas Nebengesetze, GWG, Vor. § 1 Rn. 1.

sich aus dem GwG eine umfangreiche Pflicht für Banken und andere Institute zur Speicherung von Kontoinhaltsdaten ergibt. Um diese Speicherpflicht einem verfassungs- und europarechtlichen Vergleich zu unterziehen, muss sie in ihrer aktuellen Fassung aber detaillierter erörtert werden. Daher soll in diesem Abschnitt die Wirkweise des zum Zeitpunkt der Bearbeitung gültigen GwG[855] beschrieben werden. Weiterhin liegt der Fokus dieser Arbeit auf der Betrachtung persönlicher Kontoinhaltsdaten, insbesondere Kontobewegungen. Das GwG soll daher sinnvollerweise nicht vollumfänglich, sondern nur in diesem Kontext erläutert werden.

Dreh- und Angelpunkt[856] des Gesetzes sind die in § 10 ff. GwG geregelten Sorgfaltspflichten. Diese basieren auf einem risikoorientierten Ansatz, dem „Risk-Based-Approach" und dem „Know-Your-Customer (KYC)"-Prinzip. Gemäß dem Risk-Based-Approach gilt, dass nicht alle Geschäftsbeziehungen oder Transaktionen gleich gefährlich sind. Dies ist abhängig von den betreffenden Umständen – etwa den beteiligten Personen, der Höhe des transferierten Betrages, dem Ziel der Transaktion etc.[857] Dieser am Risiko orientierte Ansatz setzt voraus, dass Risiken überhaupt erst erkannt werden. Um eine solche Analyse anzustellen, sind die Beteiligten darauf angewiesen, irreguläre Vorgänge zu identifizieren.[858] Dies gelingt nur, wenn sie ihre Kunden und deren reguläres Verhalten kennen. Insofern ergänzen sich der Risk-Based-Approach und das KYC-Prinzip.

Die risikoabhängigen Transparenzerfordernisse zeigen sich zunächst in einer Trichotomie von Sorgfaltspflichten, die die in § 2 GwG normierten Verpflichteten zu erfüllen haben. So gibt es vereinfachte Sorgfaltspflichten, § 14 GwG, allgemeine Sorgfaltspflichten, §§ 10-13 GwG und verstärkte Sorgfaltspflichten, § 15 GwG.

Diese Pflichten sollen im Folgenden nicht extensiv, sondern schwerpunktmäßig in Bezug auf die Pflicht zur kontinuierlichen Überwachung untersucht werden.

---

855 Geldwäschegesetz vom 23. Juni 2017 (BGBl. I S. 1822), zuletzt geändert durch Gesetz vom 10. August 2021 (BGBl. I S. 3436) geändert worden ist.

856 Vgl. schon *Achsnich/Mende/Mülhausen ua.* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 39 Rn. 30.

857 *Sotiriadis/Heimerdinger*, BKR 2009, 234 (234); *Costanzo* in Unger (Hrsg.), HdB Money Laundering, 2013, S. 349; *Gürkan,* Geldwäscheprävention, 2019, 95 ff.; *Herzog/Achtelik* in Herzog GwG, Einl. Rn. 86, 157; *Ross/Hannan*, J. of Money Laundering Control 10 (2007), 106 (107 ff.).

858 *Tuba/van der Westhuizen*, Int. J. of Public Law and Policy 4 (2014), 53 (59); *Spoerr* in BeckOK Datenschutzrecht, Grundlagen Syst. J. Rn. 150; *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 209.

aa. Allgemeine Sorgfaltspflichten nach §§ 10 ff. GwG

Den Regelfall stellen die allgemeinen Sorgfaltspflichten nach § 10 GwG[859] dar. Diese werden nach dem Katalog des § 10 Abs. 1 Nr. 1-5 GwG im Einzelnen aufgeführt. Sie umfassen nach § 10 Abs. 1 Nr. 1 GwG die Pflicht, den Vertragspartner zu identifizieren; nach Nr. 2 die Pflicht abzuklären, ob hinter dem Vertragspartner ein abweichender wirtschaftlicher Berechtigter steht, der gegebenenfalls zu identifizieren ist; nach Nr. 3 die Pflicht, Informationen über den Zweck und die Art der angestrebten Geschäftsbeziehung einzuholen; nach Nr. 4 die Pflicht zur Feststellung, ob es sich bei dem Vertragspartner um eine politisch exponierte Person handelt bzw. ein Familienmitglied oder eine ihr nahestehende Person, und schließlich nach Nr. 5 die Pflicht zur kontinuierlichen Überwachung der Geschäftsbeziehung einschließlich der in ihrem Verlauf durchgeführten Transaktionen. Diese Pflicht steht im Zentrum dieser Untersuchung.

(1). Pflichtauslösende Umstände

Wann diese Sorgfaltspflichten zu erfüllen sind, bestimmt sich nach § 10 Abs. 3 Nr. 1-3 GwG. Dabei dürfte § 10 Abs. 3 Nr. 1 GwG – die Begründung einer Geschäftsbeziehung – den in der Praxis bedeutendsten Auslöser darstellen.[860] Er begründet die Pflicht zur Einhaltung von Sorgfaltspflichten gegenüber den Vertragskunden der Verpflichteten. Sorgfaltspflichten gegenüber Bank- insbesondere Girokunden müssen also nach § 10 Abs. 3 Nr. 1 GwG eingehalten werden.[861]

§ 10 Abs. 3 Nr. 2 GwG betrifft hingegen Gelegenheitskunden der Verpflichteten, die keine dauerhafte Rechtsbeziehung zu den Verpflichteten eingehen, sondern nur einzelne bare oder unbare Überweisungen vornehmen.[862] Die im regelmäßigen Geschäftsverkehr typische Transaktion, die über ein bestehendes Geschäftskonto abgewickelt wird, ist von § 10 Abs. 3 Nr. 2 GwG also nicht umfasst, sondern fällt unter § 10 Abs. 3 Nr. 1 GwG.[863]

859 Umsetzung von Art. 13 Abs.1 der 4. Geldwäscherichtlinie, s. BT-Drs. 18/11555, S. 116

860 Vgl. *Stegmann/Meuer* in Bürkle (Hrsg.), Compliance, 3. Aufl. 2020.

861 *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 26.

862 *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Z. 9; *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017; *Höche/Rößler*, WM 2012, 1505 (1507).

863 *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Z. 9.

Zu den Begriffen des § 10 Abs. 3 Nr. 1 GwG bedarf es einiger Ausführungen. Die Formulierung „*bei der Begründung einer Geschäftsbeziehung*" ist nicht eindeutig.

Sie könnte so verstanden werden, dass die Sorgfaltspflichten nur *im Moment der Begründung* einer Geschäftsbeziehung umgesetzt werden müssen. Das wäre jedenfalls hinsichtlich der Identifizierungspflicht auch erst einmal sinnvoll. Die kontinuierliche Überwachungspflicht erstreckt sich aber nach § 10 Abs. 1 Nr. 5 GwG ausdrücklich auch auf Transaktionen, die *im Verlauf der Geschäftsbeziehung* getätigt werden. Gleichzeitig werden nach § 1 Abs. 4 GwG nur auf eine gewisse Dauer angelegte Geschäftsbeziehungen unter § 10 Abs. 3 S. 1 GwG subsumiert, wodurch sich diese von den gelegentlichen Transaktionen i. S. v. § 10 Abs. 3 S. 2 GwG abgrenzen. Bei dauerhaften Geschäftsbeziehungen, etwa einem Girovertrag, finden Transaktionen auch nicht im Moment der Begründung, sondern im späteren Verlauf statt. Schon aus der Überwachungspflicht ergibt sich deshalb, dass § 10 Abs. 3 S. 2 GwG nicht regelt, wann die Sorgfaltspflichten einzuhalten sind, sondern ab wann.[864]

Was unter *Begründung* der Geschäftsbeziehung verstanden wird, ergibt sich aus § 11 Abs. 1 GwG. Da § 11 Abs. 1 GwG die Identifizierungspflicht im Regelfall *vor* der Begründung verlangt, kommt als frühester Punkt nur der Vertragsschluss in Betracht, nicht die Zeit unmittelbar davor.[865]

(2). Kontinuierliche Überwachung nach §§ 10 Abs. 1 Nr. 5 GwG, 25h Abs. 2 KWG

Nach § 10 Abs. 1 Nr. 5 GwG haben die Verpflichteten ihre Geschäftsbeziehungen, einschließlich der in ihrem Verlauf durchgeführten Transaktionen, kontinuierlich zu überwachen. Im engen Zusammenhang mit dieser Vorschrift steht § 25h Abs. 2 KWG, wonach *Kreditinstitute unbeschadet der Überwachungspflicht aus § 10 Abs. 1 Nr. 5 GwG Datenverarbeitungssysteme zu betreiben und zu aktualisieren haben, mittels derer sie in der Lage sind, Geschäftsbeziehungen und einzelne Transaktionen im Zahlungsverkehr zu erkennen, die relativ gesehen, besonders komplex oder groß sind, ungewöhnlich ablaufen oder ohne offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck erfolgen*. Die Vorschriften können gemeinschaftlich als Pflicht, insbe-

864 *Ackermann/Reder*, WM 2009, 158 (166).; s.a. BT-Drs. 16/9038, S. 34
865 *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 451 f.

sondere für Banken, gelesen werden, die Transaktionen ihrer Kunden mit Datenverarbeitungssystemen zu überwachen.[866]

Was genau unter *Überwachung* verstanden werden soll, ergibt sich aus dem Gesetz nur unzureichend und sorgt beim ersten Zugriff für einige Verwirrung. Da § 15 GwG für bestimmte Fälle eine verstärkte Überwachung vorsieht, also einen qualitativen oder quantitativen Unterschied einfordert, könnte man annehmen, dass bei weniger riskanten Situationen nicht alle Transaktionen erfasst werden müssen.

Um Auslegungsproblemen des Geldwäscherechts zu begegnen, erlassen die Europäischen Finanzaufsichtsbehörden nach Art. 17, 18 Abs. 4 der 4. GWRL und Art. 16, 56 der ESA-Verordnungen[867] Leitlinien zu den Risikofaktoren, die die Verpflichteten im Rahmen der Sorgfaltspflichten zu beachten haben.[868] Diese werden von der BaFin grundsätzlich übernommen.[869]

In der aktuellen Leitlinie[870] heißt es in lfd. Mr. 4.7 lit. e), dass die Verpflichteten darlegen sollen, „welches Maß an Überwachung unter welchen Umständen Anwendung findet" und zwar nach lfd. Nr. 4.10 lit a) in Abhän-

866 Vgl. BT-Drs. 17/9038, S. 49 f.; BT-Drs. 18/11555, S. 176; *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d; *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 343; *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18; *Vollmuth,* Geldwäscheprävention, 2020, 168 f; 171 ff.; *Ackermann/Reder*, WM 2009, 158 (164); *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (456).

867 Verordnungen über die Gründung der Europäischen Aufsichtsbehörden (European Supervisory Authorities – ESAs): Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission, ABl. 2010, L 331/12; Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission, ABl. 2010, L 331/48; Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission; ABl. 2010, L 331/84.

868 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung).

869 *BaFin,* Leitlinien und Q&As der ESA, https://www.bafin.de/DE/RechtRegelungen/Leitlinien_und_Q_and_A_der_ESAs/Leitlinien_und_Q_and_A_der_ESAs_node.html, zuletzt aufgerufen am 12.01.2025.

870 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung).

gigkeit des jeweiligen Risikos. Demnach variiert die Überwachungspflicht offenbar in ihrem Umfang.

Mit diesem Umfang setzen sich lfd. Nr. 4.72 ff. auseinander. Lfd. Nr. 4.73 legt zunächst fest, dass die Transaktionsüberwachung ermöglichen soll, ungewöhnliche oder verdächtige Transaktionen oder Transaktionsmuster zu erkennen. Das entspricht dem Wortlaut der § 25h Abs. 2 KWG und § 14 Abs. 2 S. 2 GwG. Gleichzeitig soll der Umfang der Überwachung nach lfd. Nr. 4.72 aber *angemessen* sein. Was angemessen ist, hängt nach lfd. 4.74 wiederum vom jeweiligen Risiko ab. So sollen die Verpflichteten nach lfd. Nr. 4.74 lit. a) etwa entscheiden können, ob und wann sie Transaktionen in Echtzeit überwachen und wann nur nachträglich.

Aus der Möglichkeit der Echtzeitüberwachung ergibt sich eine erste entscheidende Erkenntnis: Unter Überwachung versteht das GwG nicht nur die Vorgänge, die eine bestehende Datenbasis voraussetzen, sondern die Anlegung neuer Daten in Folge von Beobachtung. Dies bedarf einer vertieften Betrachtung:

§ 10 Abs.1 Nr. 5 GwG ließe sich zunächst so verstehen, dass das GwG vom Bestehen einer entsprechenden Datengrundlage *a priori* ausgeht und die Anlegung dieser Grundlage nicht der Pflicht zur Überwachung unterfällt. Ein solches Verständnis könnte man darauf stützen, dass die Verpflichteten sämtliche Transaktionen ohnehin wahrnehmen, denn sie sind es, die diese digital oder manuell ausführen. Auch Speicherpflichten bestehen außerhalb des GwG zur Genüge (zu den Speicherpflichten außerhalb des GwG siehe oben Kap. D. II).

Die *Überwachung* i. S. d. geldwäscherechtlichen Vorschriften erschöpfte sich nach diesem Verständnis in der nachträglichen Kontrolle der vorliegenden Daten, was die BaFin in Abgrenzung zum Screening (= Echtzeitüberwachung) als Monitoring bezeichnet.[871] Eine solche Kontrolle – ob mittels EDV oder individuell – könnte auch in verschiedenen Intensitätsstufen erfolgen, womit sich wiederum erklären lässt, dass im GwG verschiedene Intensitätslevel der Überwachungspflicht veranlagt sind.

Wenn aber die Auslegungshinweise von der Möglichkeit einer Echtzeitüberwachung[872] ausgehen, muss auch die Datenanlage bzw. die Wahrneh-

871 *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14.

872 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.74 lit. a); *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14.

mung der Transaktion von der Überwachungspflicht mitumfasst sein. Auch die DK-Hinweise sehen sowohl das „laufende Monitoring" als auch die „konkrete, anlassbezogene Transaktionskontrolle" von § 25h Abs. 2 KWG umfasst.[873] Dies impliziert, dass die Wahrnehmung aller Transaktionen zur Überwachungspflicht dazugehört und diese nicht auf die nachträgliche Kontrolle reduziert ist. Überwachung ist demnach Screening *und* Monitoring.

Insbesondere im digitalen Massenverkehr dürfen also keine automatisierten Transaktionsvorgänge etabliert werden, die dem Monitoringsystem verborgen bleiben. Unabhängig von der technischen Ausgestaltung ist auf abstrakter Basis zu verlangen, dass die Verpflichteten Kenntnis aller im Rahmen ihrer Geschäftsbeziehungen durchgeführten Transaktionen erhalten. Schon im Moment der Transaktion setzt somit die Überwachungspflicht an.[874]

Verstünde man die Überwachungspflicht hingegen ausschließlich als nachträgliche Kontrolle einer Datenbasis, von deren Bestehen man *a priori* ausgeht, folgte aber ohnehin aus der Aufzeichnungspflicht i. S. d. § 8 Abs. 1 Nr. 1 GwG auch eine Pflicht zur Wahrnehmung der Transaktionen. In § 8 Abs. 1 Nr. 1 GwG wird festgelegt, dass auch die *zur Erfüllung der Sorgfaltspflicht eingeholten Informationen* aufzuzeichnen sind. Da auch die Überwachung im Sinne einer bloß nachträglichen Transaktionskontrolle eine Datenbasis bedingt, ergibt sich die Pflicht zur Transaktionserkennung und Speicherung jedenfalls aus § 8 Abs. 1 Nr. 1 GwG .[875]

Die Pflicht zur Speicherung der Transaktionsdaten ist also unabhängig von der Frage, ob die Überwachung i. S. d. § 10 Abs.1 Nr. 5 GwG eine Pflicht zur Wahrnehmung der Transaktionen oder nur eine Pflicht zur nachträglichen Kontrolle enthält.

Überzeugend ist es, schon die Datenanlegung bzw. die Erstwahrnehmung etwaiger Transaktionen unter den Überwachungsbegriff zu subsumieren. Allerdings ist der Begriff damit nicht erschöpft. Nach lfd. Nr. 4.74 lit. c) der ESA-Leitlinien sollen die Verpflichteten schließlich die Häufigkeit der Transaktionsüberwachung bestimmen. Schon hier wird klar, dass mit *Überwachung* nicht mehr nur das reine Erfassen der Transaktion gemeint

873 *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86 lit. d) S. 69 f.

874 Vgl. *Degen,* Geldwäsche, 2009, 206 f.

875 So etwa *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (463.); wohl auch *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18.

sein kann, denn ohne dies wäre auch ein nachträgliches Überwachen nicht möglich.

Der Überwachungsprozess gliedert sich vielmehr in mehrere graduelle Schritte auf. Am Anfang steht die Erfassung sämtlicher Transaktionen, also die Anlegung der Datenbasis. Danach erfolgt die Kontrolle dieser Daten, typischerweise durch einen automatisierten Abgleich mit bestehenden Daten. Dies geschieht teilweise im Rahmen einer Echtzeitüberwachung und teilweise nur im Rahmen einer nachträglichen, automatisierten Kontrolle. Die ausschließlich nachträgliche Überprüfung einer Transaktion auf Auffälligkeiten stellt in der Praxis den Standard dar.[876] Anstelle der ständigen Prüfung einzelner Transaktionen nimmt sich die Software einen ganzen Transaktionsverlauf eines Kunden in längeren, periodischen Abständen vor.[877]

Dass die Überwachung in jedem Fall eine Kontrolle der Daten beinhaltet, folgt aus § 25h Abs. 2 KWG und § 14 Abs. 2 S. 2 GwG. Dort wird festgelegt, dass selbst bei der geringsten Überwachungspflicht sämtliche Auffälligkeiten nachvollziehbar bleiben müssen. Soweit Leitlinie 4.74 lit. c) der ESA-Leitlinien von einer Reduzierung der Überwachungshäufigkeit spricht, ist nur die Quantität oder Qualität der nachträglichen Kontrolle gemeint, nicht der Umfang der Datenanlegung. Andernfalls würde eine Reduzierung der Häufigkeit dazu führen, dass bestimmte Transaktionen gar nicht registriert werden. Das Erkennen von Unregelmäßigkeiten i. S. d. § 25h Abs. 2 KWG und § 14 Abs. 2 S. 2 GwG wäre in diesem Fall nicht ständig gewährleistet.

Wenn im GwG bzw. dem Geldwäscherecht von *Überwachung* gesprochen wird, ist zusammenfassend also ein komplexer Prozess gemeint, der mehrere Einzelvorgänge von der digitalen Wahrnehmung bis zur manuell-individuellen Kontrolle von Transaktionen umfasst. Das prinzipielle Erfassen sämtlicher Transaktionen und die Durchführung eines regelmäßigen Abgleichs, zumindest digital, ist dabei das unterste Maß der Überwachung und muss immer gewährleistet sein. Keine Transaktion darf den Verpflichteten – etwa wegen der Verwendung automatisierter Systeme – verborgen bleiben. Auch im Rahmen des risikobasierten Ansatzes gilt folglich, unabhängig von der präzisen Einordnung im Gesetzestext, dass die Monitoring-

876 *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (455 f.).

877 *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 57.

systeme der Verpflichteten sämtliche Transaktionsvorgänge wahrnehmen und in gewissen Abständen rastern müssen.[878] Dies ist für das Verständnis der unterschiedlichen Ausprägungen der Überwachungspflicht, insbesondere i. R. d. verstärkten Sorgfaltspflichten, höchst bedeutsam. Wenn also im Folgenden vom risikoorientierten Umfang der Sorgfaltspflichten bzw. der Überwachung gesprochen wird, darf nicht übersehen werden, dass sich dies nur auf die individuelle Überwachung bzw. Kontrolle – etwa durch Mitarbeiter – nicht auf das generelle Erfassen der Transaktionsdaten bezieht.

(3). Risikobasierter Umfang

Der konkrete Umfang der Sorgfaltspflichten bestimmt sich nach § 10 Abs. 2[879] GwG – ganz dem Risk-Based-Approach folgend[880] – nach dem jeweiligen Risiko einer Geschäftsbeziehung oder einzelnen Transaktion. Diese Vorschrift geht Hand in Hand mit § 5 GwG, der die Verpflichteten allgemein zur Risikoanalyse im Rahmen ihrer geldwäscherechtlichen Aufgaben verpflichtet, wobei die nationale Risikoanalyse[881] i. S. d. § 3a Abs. 2 GwG gem. § 5 Abs. 1 S. 2 GwG zu berücksichtigen ist. Bei der Risikobestimmung kommt den einzelnen Unternehmen ein Ermessenspielraum zu.[882]

Für Verpflichtete, die unter das KWG fallen, ergibt sich dieser Ermessensspielraum auch aus dem insoweit ergänzenden §§ 25h Abs. 1 KWG, der ein *angemessenes* Risikomanagement verlangt.[883] Um dieses Risiko zu bestimmen, enthält das GwG in den Anlagen 1 und 2 eine nicht abschließende Liste an Faktoren, die für ein potenziell niedriges oder erhöhtes Risiko sprechen. Stellen die Verpflichteten ein solches niedriges oder erhöhtes

878 BT-Drs. 16/9038, S. 50; *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 15; *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d; *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18; *Vollmuth,* Geldwäscheprävention, 2020, 168 f; 171 ff.; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (462).

879 Umsetzung von Art. 13 Abs. 2 – 5 der 4. Geldwäscherichtlinie, s. BT-Drs. 18/11555, S. 116

880 *Figura* in Herzog GwG, §10 Rn. 38.

881 Zuletzt *Bundesministerium der Finanzen,* 1. Nationale Risikoanalyse 2018/19.

882 BT-Drs. 16/9038, S. 35 zu § 3 Abs. 4 GwG aF; *Stegmann/Meuer* in Bürkle (Hrsg.), Compliance, 3. Aufl. 2020, § 13 Rn. 179.

883 *Figura* in Herzog GwG, § 10 Rn. 40.

Risiko fest, haben sie in Anwendung der §§ 14, 15 GwG vereinfachte oder verstärkte Sorgfaltspflichten anzuwenden.

bb. Vereinfachte Sorgfaltspflichten nach § 14 GwG

Im Falle eines niedrigen Risikos gelten nach § 14 GwG vereinfachte Sorgfaltspflichten. Ob ein niedriges Risiko besteht, haben die Verpflichteten nach § 5 Abs. 1 GwG im Rahmen ihrer Risikoanalyse unter Anwendung anerkannter Risikofaktoren zu bestimmen – insbesondere der in Anlage 1 und 2 aufgeführten Kriterien. Die in den Anlagen 1 und 2 genannten Risikofaktoren sind nach § 14 Abs. 1 S. 2 GwG aber nur Indikatoren für ein gewisses Risiko und nicht abschließend zu verstehen[884]. Die Verpflichteten müssen im konkreten Fall auch stets das tatsächliche Bestehen eines geringen Risikos der Geldwäsche oder Terrorismusfinanzierung feststellen.

Eine schematische Anwendung findet i. R. d. § 14 GwG nicht statt. Einen Katalog mit Regelbeispielen zu Situationen, in denen vereinfachte Sorgfaltspflichten gelten, sucht man im Gesetz heute vergeblich (zur alten Gesetzeslage s. o. III. 2. a.). Vielmehr ist die Anwendung vereinfachter Sorgfaltspflichten immer denkbar, wenn es der Einzelfall denn zulässt.[885]

§ 14 GwG ist heute so ausgestaltet, dass er nicht mehr die grundsätzliche Anwendung der Sorgfaltspflichten entbehrlich macht, sondern nur den Umfang der in § 10 GwG aufgeführten Pflichten beschränkt. Wie diese Beschränkung im Einzelfall ausgestaltet werden soll, schreibt die Norm auch nicht vor, sondern überlässt es in § 14 Abs. 2 Nr. 1 GwG grundsätzlich den Verpflichteten, eine *angemessene* Reduzierung vorzunehmen. Die Verpflichteten sind bei der Reduzierung des Pflichtenumfangs aber nicht gänzlich sich selbst überlassen. Sie werden mit Auslegungshinweisen versorgt. In den ESA-Leitlinien sind beispielhaft Möglichkeiten aufgezählt, wie sich die allgemeinen Sorgfaltspflichten reduzieren lassen.[886] Das GwG selbst verweist zwar nicht auf die Art. 16, 56 ESA-Verordnungen bzw. dem hier-

884 BT-Drs. 18/11555, S. 63; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 59.

885 *Ruppert*, DStR 2012, 100 (101 f.).

886 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.41.

nach erlassenen Leitlinien. Allerdings stellt die Gesetzesbegründung (zum GwG 2017) den Bezug ausdrücklich her.[887]

So kann insbesondere die Häufigkeit und Intensität der Transaktionsüberwachung reduziert werden, indem die überwachten Transaktionen von einem gewissen Schwellenwert abhängig gemacht werden.[888] Dabei ist jedoch § 14 Abs. 2 S. 2 GwG zu beachten, nach dem die Verpflichteten in jedem Fall die Überprüfung von Transaktionen und die Überwachung von Geschäftsbeziehungen in einem Umfang sicherstellen, der es ihnen ermöglicht, ungewöhnliche oder verdächtige Transaktionen zu erkennen und zu melden. Dies setzt voraus, dass jede Transaktion zumindest grundsätzlich von den digitalen Sicherungsmechanismen erfasst wird und kontrolliert werden kann.[889]

cc. Verstärkte Sorgfaltspflichten nach § 15 GwG

Das Gegenstück zu den vereinfachten Sorgfaltspflichten stellen die verstärkten Sorgfaltspflichten dar, die in § 15 GwG geregelt sind. Sie sind nach § 15 Abs. 2 GwG anzuwenden, falls die Verpflichteten unter Berücksichtigung der in den Anlagen 1 und 2 genannten Faktoren ein *höheres Geldwäscherisiko* festgestellt haben – und zwar entweder im Rahmen ihrer Risikoanalyse i. S. d. § 5 Abs. 1 GwG oder im Einzelfall. Neben diesem generalklauselartigen Auslöser gibt § 15 Abs. 3 GwG einen Katalog bestimmter Fälle vor, in denen von einem erhöhten Risiko *insbesondere* auszugehen ist. Die Aufzählung ist im Zeichen des Risk-Based-Approach nicht abschließend zu verstehen.[890]

(1) Auslösende Umstände und allgemeiner Umfang

Schon aus § 15 Abs. 2 GwG ergibt sich, dass die Anwendung verstärkter Sorgfaltspflichten sich nicht nur generell aus bestimmten Umständen eines

887 BT-Drs. 18/11555, S. 120.

888 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.41 lit. e).

889 *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d; *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18; *Vollmuth,* Geldwäscheprävention, 2020, 168 f; 171 ff.; *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 11, 13.

890 Vgl. *Ackermann/Reder*, WM 2009, 200 (202); *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 455.

Kunden ergeben, sondern auch von Umständen einzelner Transaktionen ausgelöst werden kann. Dieser Befund spiegelt sich auch im Beispielkatalog des § 15 Abs. 3 GwG wider.

§ 15 Abs. 3 Nr. 1 GwG etwa stellt allgemein auf den Kunden ab. Handelt es sich bei diesem oder dessen wirtschaftlich Berechtigtem um eine politisch exponierte Person (PEP), ein Familienmitglied einer PEP oder auch nur um eine Person, die einer PEP nahesteht, so sind stets verstärkte Sorgfaltspflichten anzuwenden.[891]

§ 15 Abs. 3 Nr. 2 GwG hingegen stellt auf Geschäftsbeziehungen oder Transaktionen ab und nimmt damit sowohl allgemeine Umstände einer Geschäftsbeziehung als auch Einzelumstände von Transaktionen in den Blick. Die Norm betrifft Vorgänge mit Beteiligung eines geldwäscheriskanten Drittstaats. Diese Drittstaaten „mit hohem Risiko" werden nach Art. 9 Abs. 2, 64 GWRL in einem Rechtsakt der Kommission bestimmt. Dies geschah erstmals im Jahr 2016 im Rahmen der Delegierten-Verordnung (EU) 2016/1675.[892] Die Liste wurde zuletzt im Jahr 2020 aktualisiert.[893]

Bei der Bestimmung orientiert sich die Kommission an den Erkenntnissen der FATF. Diese überwacht und bewertet in Kooperation mit regionalen FATF-ähnlichen Organisationen weltweit die Effizienz der Geldwäschebekämpfung in über 200 Staaten.[894]

Staaten mit erhöhtem Risiko werden in der Liste *„jurisdictions under increased monitoring"*[895] geführt. Staaten mit hohem Geldwäscherisiko, in denen ein unzureichendes Anti-Geldwäscheregime festgestellt wurde, kommen auf die sogenannte *black list (High-Risk Jurisdictions subject to a Call*

891 Zur Entwicklung *Herzog/Hoch*, WM 2007, 1997; *Kunz/Schirmer* BB 2015, 2435 (2439 f.).

892 Delegierte Verordnung (EU) 2016/1675 der Kommission vom 14. Juli 2016 zur Ergänzung der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates durch Ermittlung von Drittländern mit hohem Risiko, die strategische Mängel aufweisen, ABl. 2016, L 254/1; konsolidierte Fassung vom 07.02.2021: Document 02016R1675-20210207.

893 Delegierte Verordnung (EU) 2021/37 der Kommission vom 7. Dezember 2020 zur Änderung der Delegierten Verordnung (EU) 2016/1675 zur Ergänzung der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates im Hinblick auf die Streichung der Mongolei aus der Tabelle unter Nummer I des Anhangs; ABl. 2021, L 14/1.

894 *FATF,* Annual Report 2019/2020, 37 ff.

895 Aktuelle Liste unter *dies.,* Jurisdictions under Increased Monitoring, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2021.html, zuletzt aufgerufen am 12.01.2025

for Action).[896] Auf diese *black list* stellt § 15 Abs. 8 GwG ab, nach dem die BaFin über § 15 Abs. 4 GwG hinausgehende Maßnahmen erforderlich machen kann.[897] Ähnliches sieht § 15 Abs. 5a GwG vor, der aber nicht auf die FATF-Listen abstellt, sondern für alle von der Kommission festgelegten Drittstaaten im Einzelfall besonders intensive Pflichten vorsieht. Ausgehend von § 15 Abs. 5a GwG hat die BaFin für Nordkorea und den Iran Gebrauch gemacht und eine Meldepflicht für Geschäftsbeziehungen und Transaktionen mit dort ansässigen Personen angeordnet.[898]

Allein auf die Umstände einer einzelnen Transaktion, unabhängig vom jeweiligen Kunden, stellt § 15 Abs. 3 Nr. 3 GwG ab. Danach sind verstärkte Sorgfaltspflichten bei Transaktionen anzuwenden, die im Vergleich zu ähnlichen Fällen besonders komplex oder ungewöhnlich groß sind (lit. a), einem ungewöhnlichen Transaktionsmuster folgen (lit. b) oder keinen offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck haben (lit. c). Außerdem sind verstärkte Sorgfaltspflichten nach § 15 Abs. 3 Nr. 4 GwG bei Transaktionen von bestimmten Verpflichteten auszuüben, insbesondere Transaktionen von Kreditinstituten an deren Korrespondenzinstitute, wenn sich die Korrespondenzinstitute in einem Drittstaat oder in einem Staat des Europäischen Wirtschaftsraums befinden.

Wie auch bei den vereinfachten Sorgfaltspflichten gilt der Risk-Based-Approach ebenso bei den verstärkten Sorgfaltspflichten. So haben nach § 15 Abs. 1 S. 2 GwG die Verpflichteten prinzipiell selbst den konkreten Umfang der verstärkten Sorgfaltspflichten zu bestimmen. Anders als bei den vereinfachten Sorgfaltspflichten sehen § 15 Abs. 4 – 8 GwG aber für verschiedene Fälle nur Mindestpflichten vor, die zwar alle über die allgemeinen Sorgfaltspflichten hinausgehen, aber in unterschiedlicher Schärfe. Auf eine abschließende Aufzählung der Maßnahmen wurde bewusst verzichtet.[899]

---

896 Derzeit nur Nordkorea und Iran, *dies.,* High-Risk Jurisdictions, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2021.html, zuletzt aufgerufen am 12.01.2025.

897 Dazu *BaFin,* Rundschreiben 01/2019 (GW), 15.02.2019; Rundschreiben 03/2020 (GW), 13.05.2020, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2020/rs_03-2020_laenderliste_gw.html, zuletzt aufgerufen am 12.01.2025.

898 *BaFin,* Allgemeinverfügung zur Anordnung einer Meldepflicht bei Geschäftsbeziehungen und Transaktionen mit Bezug zur Demokratischen Volksrepublik Korea (Nordkorea), GZ: GW 1-GW 2002-2020/0002, 13.05.2020; *BaFin,* Allgemeinverfügung zur Anordnung einer Meldepflicht bei Geschäftsbeziehungen und Transaktionen mit Bezug zu Iran, GZ: GW 1-GW 2002-2020/0002, 13.05.2020.

899 *Zentes/Glaab* BB 2017, 67 (70).

Die Intensität der verstärkten Sorgfaltspflichten ist also nur nach oben hin unbegrenzt[900] und steht auch nur insoweit tatsächlich im Ermessen der Verpflichteten.

(2) Verstärkte kontinuierliche Überwachung

Auf die einzelnen Mindestpflichten, die § 15 Abs. 4-7 GwG für die verschiedenen auslösenden Situationen statuiert, soll nur kurz eingegangen werden. Da die kontinuierliche Überwachung der Geschäftsbeziehungen schon aufgrund der allgemeinen Sorgfaltspflichten gilt, ist sie natürlich erst recht im Rahmen der hochriskanten Situationen des § 15 GwG einzuhalten. Die verstärkten Sorgfaltspflichten intensivieren die Überwachungspflicht aber an einigen Stellen. Die Pflichten des § 15 Abs. 4-7 GwG in Bezug auf die Überwachung zeigen insofern, dass der Überwachungsbegriff im GwG uneinheitlich ist bzw. verschiedene Handlungen mitumfasst.

Für Geschäftsbeziehungen und Transaktionen, an denen PEP beteiligt sind, sehen etwa § 15 Abs. 4 Nr. 2 und 3 GwG vor, dass durch angemessene Maßnahmen die Herkunft der transferierten Vermögenswerte bestimmt wird und die Geschäftsbeziehung einer *verstärkten* kontinuierlichen Überwachung unterzogen wird. Hier wird deutlich, dass es im Rahmen der verstärkten Sorgfaltspflicht nicht ausreichend sein kann, dass sämtliche Transaktionen von der EDV erfasst und irgendwann einmal kontrolliert werden. *Überwachung* ist hier also nicht gleichbedeutend mit dem allgemeinen EDV-Monitoring. Vielmehr werden sich die Verpflichteten aktiv und individuell bzw. durch Einsatz ihrer Mitarbeiter mit den einzelnen Vorgängen regelmäßig beschäftigen müssen.[901] Der genaue Rahmen der Intensität ergibt sich aus dem Gesetz aber nicht.[902]

Die Verpflichteten sind insofern auf die Auslegungshinweise des ESA angewiesen. Dort heißt es: „*Die Unternehmen sollten nach Anzeichen für ungewöhnliche Transaktionen suchen und die ihnen vorliegenden Daten regelmäßig überprüfen, um sicherzustellen, dass alle neuen oder aufkommenden Informationen mit potenziellen Auswirkungen auf die Risikobewertung*

900 Vgl. *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (193 ff.).

901 *Achtelik* in Herzog GwG, § 15 Rn. 25; *Stegmann/Meuer* in Bürkle (Hrsg.), Compliance, 3. Aufl. 2020, § 12 Rn. 244.

902 Schon *Herzog/Hoch*, WM 2007, 1997 (1998).

zeitnah identifiziert werden. Die Häufigkeit der Überprüfungen im Rahmen der fortlaufenden Überwachung sollte sich nach dem Risikograd der betreffenden Geschäftsbeziehung richten."[903] Die sektorspezifischen Leitlinien zur Unternehmensfinanzierung stellen daneben ausdrücklich fest: „*In diesem Zusammenhang* (der Unternehmensfinanzierung) *sollten Unternehmen, die automatisierte Transaktionsüberwachung einsetzen, diese mit den Kenntnissen und dem Fachwissen des die Tätigkeit ausübenden Personals kombinieren. Diese verstärkte Überwachung sollte zu einem klaren Verständnis führen, weshalb ein Kunde eine bestimmte Transaktion oder Tätigkeit durchführt; für diesen Zweck sollten Unternehmen dafür Sorge tragen, dass sein Personal sein Wissen über den Kunden, und was unter den gegebenen Umständen zu erwarten wäre, einsetzt, um ungewöhnliche oder potenziell verdächtige Transaktionen und Tätigkeiten zu erkennen.*[904]

Daraus ergibt sich doch recht eindrücklich, dass eine *verstärkte Überwachung* nur durch eine qualitative und/oder quantitative[905] Ausweitung der individuellen Kontrollen ausgeübt werden kann.

Die unterschiedliche Verwendung des Überwachungsbegriffs zeigt sich denn auch in § 15 Abs. 6 GwG, der die Pflichten bei Hochrisikotransaktionen i. S. d. § 15 Abs. 3 Nr. 3 GwG bestimmt. Nach § 15 Abs. 6 Nr. 1 GwG haben die Verpflichteten zunächst Informationen zu der Transkation einzuholen, um sodann das Risiko der Transkation oder Geschäftsbeziehung einschätzen und überwachen zu können. Nach § 15 Abs. 6 Nr. 2 GwG soll weiter, *wenn die Transaktion aus einer Geschäftsbeziehung stammt, die Geschäftsbeziehung verstärkt überwacht werden, um das Geldwäsche- oder Terrorismusfinanzierungsrisiko zu bestimmen und bei höherem Risiko zu überwachen.*

Mit dieser undankbaren Formulierung ist Folgendes gemeint: Zunächst soll also das Transaktionsverhalten im Rahmen der Geschäftsbeziehung individuell bzw. manuell erfasst und in angemessener Regelmäßigkeit überwacht werden. Daran anknüpfend soll die Risikoeinstufung im weiteren Verlauf, die wiederum für das Maß der individuellen Überwachung verantwortlich ist, regelmäßig und individuell kontrolliert werden. Die Überwachung des Risikos ist keine Überwachung im Sinne der Wahrnehmung bestimmter Vorgänge, sondern ein Kontrollvorgang hinsichtlich der eigenen

903 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.50. d).
904 Idem, lfd. Nr. 20.7. h).
905 Nur knapp *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 62.

Kundeninformationen. Sie baut aber auf der eigentlichen Überwachung bestimmter Vorgänge auf. Die Verwendung des Begriffs der „Überwachung" in § 15 Abs. 6 Nr. 2 GwG ist dahingehend undifferenziert.

dd. Ergebnis: Überwachung prinzipiell unabhängig von Sorgfaltspflichten

Es lässt sich damit feststellen, dass die Pflicht zur kontinuierlichen Überwachung prinzipiell unabhängig von den einschlägigen Sorgfaltspflichten besteht. Lediglich das Maß der *Überwachung* ändert sich.

Im Rahmen vereinfachter Sorgfaltspflichten besteht die Pflicht zur Überwachung, die es ermöglicht, ungewöhnlich hohe Transaktionen zu erkennen, § 14 Abs. 1 S. 2 GwG. Eine ungewöhnlich hohe Transaktion kann im Einzelfall verstärkte Sorgfaltspflichten auslösen, § 15 Abs. 3 Nr. 3 GwG.[906] Eine individuelle Überwachung der Transaktionen im Rahmen vereinfachter Sorgfaltspflichten wird nicht regelmäßig stattfinden müssen, sondern kann von Schwellenwerten abhängig gemacht werden.[907]

Dementsprechend geht die Praxis bei der Überwachung von Kunden so vor, dass sie grundsätzlich alle Transaktionen des Kunden in das Monitoring miteinbezieht.[908] Bei den vereinfachten Sorgfaltspflichten beschränkt sich die Überwachungspflicht also minimal darauf, dass ein EDV-System die Transkationen des Kunden registriert, speichert und im Rahmen bestehender Geschäftsbeziehungen mit den Transaktionsmustern des Kunden regelmäßig abgleicht. Bei Kunden mit geringem oder moderatem Risiko rastern die EDV-Systeme in gewissen Abständen die Transaktionsverläufe blockweise, anstatt sich jede Transaktion einzeln „anzusehen".[909] Bestimmte Transaktionsmuster werden jedoch automatisch eine individuelle Echtzeit- oder Nachprüfung einleiten, indem z. B. die Überweisungsmasken

906 *Vollmuth,* Geldwäscheprävention, 2020, S. 173; *Achtelik* in Herzog GwG, § 25h KWG Rn. 11 f.

907 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.41 lit. e).

908 *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (463).

909 Vgl. *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020 mit Verweis auf *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86 lit. d).

beim Online-Banking auf bestimmte Namen oder Länderkennungen reagieren.[910]

Diese Praxis erscheint sachgerecht und ist notwendig. Denn § 25h Abs. 2 KWG und § 14 Abs. 1 S. 2 GwG verlangen, dass auf der niedrigsten Risikostufe zumindest Abweichungen vom Risikoprofil registriert werden können. Die unter das KWG fallenden Institute kommen der vereinfachten Sorgfaltspflicht somit bereits durch den Einsatz ausreichender EDV-Systeme nach. Manuelle Prüfungen finden nur statt, wenn die EDV-Systeme bei einer Transaktion *anschlagen,*[911] und deshalb verstärkte Sorgfaltspflichten zu beachten sind.

c. Verdachtsmeldungen

Wenn die Verpflichteten im Rahmen der Ausführung ihrer Sorgfaltspflichten verdächtige Transaktionen oder andere Umstände aufspüren, müssen sie diese an die FIU melden, § 43 Abs. 1 GwG. Die Meldungen sind der Zweck der Überwachungsmaßnahmen der Verpflichteten[912] und stehen ganz im Zentrum der Geldwäschebekämpfung.[913]

Anders als etwa die Vorratsdatenspeicherung von TK-Verkehrsdaten nach § 176 TKG wurde und wird die Beobachtung der Finanzströme durch private Akteure nicht primär als Instrument zum Datensammeln und Bereithalten für staatliche Behörden verstanden. Vielmehr verwenden die Verpflichteten diese Daten selbst – zumindest im ersten Zugriff. Die Verpflichteten sollen selbstständig Verdachtsmomente aus dem Massengeschäft filtern und melden. Von Kritikern des Anti-Geldwäschesystems werden sie deshalb als „Erfüllungsgehilfen“[914], „verlängerter Arm der Staatsanwaltschaft“[915] oder gar als „Hilfssheriffs“ [916] bezeichnet.

910 Zum Prozess ausf. *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 40 ff; 54 ff.
911 Idem, Rn. 47, 54 ff.
912 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (204).
913 Vgl. nur. *Barreto da Rosa* in Herzog GwG, § 43 Rn. 1; *Greite* in Zentes/Glaab GWG, § 43 Rn. 2.
914 *Dahm/Hamacher*, wistra 1995, 206 (207).
915 *L. Schuster,* Geldwäsche, 1994, S. 21.
916 *Griebel* NZM 2012, 482.

Wie sich ihre Stellung in der Geldwäschebekämpfung rechtlich einsortieren lässt, war und bleibt umstritten.[917] Nach Ansicht des Gesetzgebers erfüllen die Verpflichteten schlicht eine gewerberechtliche Pflicht und sind weder Verwaltungshelfer noch Beliehene oder sonst hoheitlich ermächtigt.[918]

Dass die Sicherheitsbehörden im ersten Schritt der Geldwäschebekämpfung eine passive Funktion haben, zeigt sich schon im Wortlaut der geldwäscherechtlichen Vorschriften. Sowohl in der GWRL als auch dem GwG wird die FIU als zentrale *Melde*stelle bzw. als Zentralstelle für Finanztransaktionsuntersuchungen bezeichnet.[919] Schon dem Namen nach ist die FIU also auf eine passive Tätigkeit ausgerichtet, die auf ein proaktives Handeln der verpflichteten Akteure aufbaut. Die FIU selbst beschreibt ihre Tätigkeit auf ihrer Homepage als das *Entgegennehmen, Sammeln und Auswerten von Meldungen über auffällige Finanztransaktionen.*[920] Ob diese Selbsteinschätzung vor dem Hintergrund ihrer, zumindest auf dem Papier bestehenden, weiten rechtlichen Befugnisse überzeugen kann, ist zu bezweifeln.[921] (s. Kap. G. III. 3. b. bb.).

aa. Rechtsnatur und Verdachtsschwelle

Die Rechtsnatur der Verdachtsmeldungen ist bis heute nicht ganz klar.[922] Gemäß dem Gesetzgeber soll es sich jedenfalls nicht um Strafanzeigen i. S. d. § 158 StPO handeln,[923] sondern um eine *gewerberechtliche* Meldeverpflichtung.[924] Die Rechtswissenschaft scheint dies akzeptiert zu haben, wenngleich weiterhin auf die Gemeinsamkeiten der Verdachtsmeldung zur

917 Ausführlich hierzu *Degen,* Geldwäsche, 2009, S. 128 ff.
918 BT-Drs. 18/11928, S. 26; *Kaetzler*, CCZ 2008, 174 (174).
919 Der Begriff wird auch in dem Entwurf für eine EU-GeldwäscheVO verwendet, COM/2021/420 final
920 *Zoll,* Financial Intelligence Unit, https://www.zoll.de/DE/Der-Zoll/Aufgaben-des-Zolls/Schutz-fuer-Mensch-Wirtschaft-und-Umwelt/FIU-Aufgaben/fiu-aufgaben_node.html , zuletzt aufgerufen am 12.01.2025.
921 Dazu *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (249 f.); krit. auch *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21.
922 *Barreto da Rosa* in Herzog GwG, § 43 Rn. 5.
923 BT-Drs. 17/6804, S. 21, 35.; *Findeisen* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. II, 3. Auflage 2017, § 85 Rn. 62; anders noch *Herzog* in Herzog GWG, 1. Aufl. 2010, § 11 Rn. 20, 32.
924 BT-Drs. 18/11928, S. 26.; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 76.

Strafanzeige hingewiesen wird.[925] Im Hintergrund dieser Frage steht offenbar der Verdachtsgrad, der im Rahmen des § 43 Abs. 1 GwG erreicht werden muss.[926]

(1) Keine Ableitung der Verdachtsschwelle aus der Rechtsnatur

In der Literatur wurde versucht, aus der Einordnung der Verdachtsmeldungen als Strafanzeige Erkenntnisse über die Verdachtsschwelle zu gewinnen.[927] Der Gesetzgeber stellte deshalb in der Begründung zum Geldwäscheoptimierungsgesetz aus dem Jahr 2011[928] fest, dass die Verdachtsmeldungen keinen Anfangsverdacht i. S. d. § 152 Abs. 2 StPO benötigen, *da sie keine Strafanzeigen darstellen*[929]. In der Begründung zum Gesetz zur Umsetzung der 4. GWRL wurde wiederum festgehalten, *dass der Verdachtsgrad, auf Basis dessen der Verpflichtete eine Meldung abgibt, unterhalb dem einer Strafanzeige liegt.*[930] Damit stellte der Gesetzgeber sich allgemein gegen eine stark vertretene Meinung in der Literatur, die unabhängig von der Frage der Rechtsnatur, den Verdachtsgrad des § 152 Abs. 2 StPO auf die Verdachtsmeldepflicht übertragen wollte.[931]

Die Ausführungen in den Gesetzesbegründungen zur Verquickung von Rechtsnatur und Verdachtsgrad der Strafanzeige irritieren. Die Strafanzeige nach § 158 StPO kennt überhaupt keine materiellen Voraussetzungen bzw. einen Verdachtsgrad, ab dem sie obligatorisch würde. Sie ist lediglich eine (private) Aufforderung an die Staatsanwaltschaft, einen Sachverhalt strafrechtlich zu prüfen.[932]

925 *Barreto da Rosa* in Herzog GwG, § 43 Rn. 5, der von einer Pflicht „sui generis" ausgeht.: zust. *Lenk*, JR 2020, 103 (105 Fn 15).

926 Dazu *Höche/Rößler*, WM 2012, 1505 (1509 f.).

927 In diese Richtung jedenfalls *Barreto da Rosa* in Herzog GwG, § 43 Rn. 5 ff.; *Herzog/Achtelik* in Herzog GwG, 2. Aufl. 2014, Rn. 16; dazu krit. *Findeisen* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. II, 3. Auflage 2017, § 85 Rn. 62.

928 Gesetz zur Optimierung der Geldwäscheprävention vom 22.12.2011 (BGBl. I, S. 2595).

929 BT-Drs. 17/6804, S. 21, 35.

930 BT-Drs. 18/11555, S. 144.

931 *Krais,* Geldwäsche, 2018, Rn. 510; *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (68); *ders.* in Herzog GWG, 1. Aufl. 2010, § 11 Rn. 18 ff.; *Klugmann*, NJW 2012, 641 (644); *Carl/Klos*, wistra 1994, 161 (162); *Bülte*, NZWiSt 2017, 276 (280 f.); *Degen,* Geldwäsche, 2009, S. 127 f.

932 *Köhler* in Meyer-Goßner/Schmitt StPO, § 158 Rn. 2.

Mit wenigen Ausnahmen, etwa Anzeigen von bekannten Querulanten und oder „Geistesgestörten“[933], ist die Staatsanwaltschaft grundsätzlich zur Prüfung verpflichtet.[934] Die Anzeigen werden registriert und sodann in den sogenannten „Vorermittlungen“ darauf geprüft, ob sie die Verdachtsschwelle des § 152 Abs. 2 StPO erreichen.[935] So dies der Fall ist, muss die Strafverfolgungsbehörde mit den formellen Ermittlungen beginnen, § 152 Abs. 2 StPO. Nicht die Strafanzeige, sondern nur die Reaktion der Staatsanwaltschaft hängt also von einem Verdachtsgrad ab.

Die primäre Folge der Anzeige ist also immer deren Prüfung, unabhängig von etwaigen Voraussetzungen. Die Umstände der Anzeige können aber dennoch weite Folgen nach sich ziehen. Wer leichtfertig eine objektiv unwahre Anzeige abgibt, muss die Kosten des – auch außergerichtlichen – Verfahrens und Auslagen des Beschuldigten tragen, § 469 Abs. 1 StPO. Im Falle der vorsätzlich erstatteten Falschanzeige kommt auch eine Strafbarkeit wegen falscher Verdächtigung nach § 164 StGB in Betracht bzw. ein darauf gestützter zivilrechtlicher Schadensersatzanspruch nach § 823 Abs. 2 BGB.[936]

Der Vergleich der Verdachtsmeldung mit der Strafanzeige sagt somit über die Verdachtsschwelle der Pflicht zur Verdachtsmeldung nicht unmittelbar etwas aus, da für den Strafanzeigenden eine solche Schwelle gar nicht existiert. Selbst wenn die Meldung analog zur Strafanzeige behandelt werden müsste, könnte man aus den §§ 152 Abs. 2, 160 Abs. 1 StPO nur ableiten, ab wann die FIU aufgrund der Meldung weitere Schritte einleiten muss, denn die FIU stellt im geldwäscherechtlichen Meldesystem das Pendant zur Staatsanwaltschaft im Rahmen der §§ 152 ff. StPO dar.

Wenn in den Gesetzesbegründungen und der Literatur um den Verdachtsgrad gestritten wird, kann es daher nicht darum gehen, ob der Verdachtsgrad für die meldenden Verpflichteten niedriger ist als der Verdachtsgrad eines Strafanzeigenden, sondern niedriger ist als der Grad, ab dem die Strafverfolgungsbehörden auf Grundlage einer Anzeige tatsächlich ermitteln muss. Dieser wiederum wird in § 152 Abs. 2 StPO bestimmt, wonach Ermittlungen eingeleitet werden *müssen*, wenn *zureichende tatsächli-*

933 Dazu *Kockel/Vossen-Kempkens*, NStZ 2001, 178.
934 *Köhler* in Meyer-Goßner/Schmitt StPO, § 158 Rn. 2.
935 *Kölbel* in MüKo StPO, § 158 Rn. 26.
936 Etwa AG Bremen, NJW-RR 2014, 207.

che Anhaltspunkte (bzgl. einer Straftat) vorliegen. Der Verdachtsgrad des § 152 Abs. 2 StPO ist im Übrigen der niedrigste, den die StPO kennt.[937]

(2) Konturen der Verdachtsschwelle

§ 43 GwG ist ähnlich formuliert wie § 152 Abs. 2 StPO. Ausweislich des hier abgekürzten Wortlauts sind Verdachtsmeldungen vorzunehmen, *wenn Tatsachen vorliegen, die darauf hindeuten, dass ein Vermögensgegenstand aus einer Vortat der Geldwäsche stammt, oder ein solcher Gegenstand, ein Geschäftsvorfall oder eine Transaktion im Zusammenhang mit Terrorismusfinanzierung steht.* Außerdem *wenn Tatsachen vorliegen, die darauf hindeuten, dass ein Geschäftspartner seinen wirtschaftlich Berechtigten, so er existiert, nicht offenbart hat.*

Die Voraussetzung erschöpft sich also in „hindeutenden Tatsachen". Diese Formulierung wird gemeinhin als ein Weniger zum strafprozessualen Anfangsverdacht i. S. d. § 152 Abs. 2 StPO verstanden[938], für den zwar ebenfalls schon „konkrete Anhaltspunkte" ausreichen sollen,[939] aber eben in Bezug auf das Vorliegen einer Straftat. Das soll bei den Verdachtsmeldungen gerade nicht mehr die Schwelle sein. Da es sich bei den Verpflichteten nicht um eine Strafverfolgungsbehörde handelt, müssten diese nicht die Vorstellung haben, dass möglicherweise eine Straftat begangen wurde oder begangen wird. Insbesondere sollen sie nicht den § 261 StGB tatbestandlich prüfen, sondern nur kontrollieren, ob die nach dem GwG erforderlichen Tatsachen vorliegen.[940] Das wiederum sei dann der Fall, wenn nach der subjektiven Ansicht des Verpflichteten bzw. dessen Mitarbeiter eine Ungewöhnlichkeit oder Auffälligkeit im spezifischen geschäftlichen Kontext

937 *Frister* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. F Rn. 122; *Herzog* in Herzog GWG, 1. Aufl. 2010, § 11 Rn. 19 ff.

938 BT-Drs. 17/6804, S. 35; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72; Findeisen in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. II, 3. Auflage 2017, Rn. 62; *Klugmann*, NJW 2012, 641 (644); *Greite* in Zentes/Glaab GWG, § 43 Rn. 10 ff.

939 Hierzu *B. Schmitt* in Meyer-Goßner/Schmitt StPO, § 152 Rn. 4; *Roxin/Schünemann,* Strafverfahrensrecht, 29. Aufl. 2017, § 39 Rn. 15 mwN.

940 *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72; *Bundesministerium der Finanzen,* Auslegunsghinweise Verdachtsmeldewesen, 06. November 2014, S. 3; OLG Frankfurt a.M., Hinweisbeschluss vom 17. Dezember 2012 - 19 U 210/12; *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (202).

vorliegt – etwa, weil ein ungewöhnlich großer oder unnötig komplexer Vorgang stattfindet.[941] Für die Verpflichteten besteht also ein Beurteilungsspielraum, der allerdings begrenzt sein kann, wenn bestimmte Indikatoren vorliegen.[942]

Diese Indikatoren kann nach § 43 Abs. 5 GwG die FIU bestimmen. Als die FIU noch beim BKA angesiedelt war, wurden diese Indikatoren in Newslettern veröffentlicht – etwa in dem Papier „Anhaltspunkte Geldwäsche"[943], auf das die BaFin noch heute hinweist.[944] Es finden sich aber auch Indikatoren in den ESA-Leitlinien.[945]

Der Beurteilungsspielraum erlaubt es den Verpflichteten nicht, den Sachverhalt durch eigene Nachforschungen eigens aufzuklären.[946]

Mit den Anforderungen an die Verdachtsmeldungen hat sich jünger auch das BVerfG kurz beschäftigt.[947] Anlass war eine Wohnungsdurchsuchung wegen Verdachts einer Geldwäschehandlung. Dieser ging eine Verdachtsmeldung voraus. Es fehlten im konkreten Fall aber Anhaltspunkte dafür, dass die transferierten Beträge, die in der Tat auffällig waren, aus einer Katalogtat des damaligen § 261 Abs. 1 StGB stammten. Nach Ansicht des Generalbundesanwalts waren solche Anhaltspunkte nicht nötig, da es im Rahmen der Verdachtsmeldepflicht i. R. d. § 43 Abs. 1 GwG auch nicht darauf ankäme.[948] Gegen diese Übertragung stellte sich das BVerfG und hob die Unterschiede zwischen strafprozessualem Anfangsverdacht und § 43 Abs. 1 GwG hervor. Im Rahmen der geldwäscherechtlichen Verdachtsanzeige sei es danach ausreichend, wenn *objektiv erkennbare Anhaltspunkte dafür sprechen, dass durch eine Transaktion illegale Gelder dem Zugriff*

941 BT-Drs. 17/6804, S. 35; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72 f.; *Bundesministerium der Finanzen,* Auslegunsghinweise Verdachtsmeldewesen, 06. November 2014, S. 3.

942 *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72.

943 Die Newsletter werden nicht mehr auf der Website der FIU veröffentlich, vgl. *Krais,* Geldwäsche, 2018, Rn. 507, zuletzt online aber hier verfügbar: *FIU,* Anhaltspunktepapier - Newsletter 11/2014, August 2014, https://geldwaesche-beauftragte.de/wp-content/uploads/2017/04/FIU_Newsletter_Ausgabe_Nr._11_-August_2014.pdf, zuletzt aufgerufen am 12.01.2025; zusammengefasst bei *Diergarten* in Hauschka/Moosmayer/Lösler (Hrsg.), Hdb. Haftungsvermeidung, 3. Aufl. 2016, § 34 Rn. 392; *Krais,* Geldwäsche, 2018, Rn. 717.

944 *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72.

945 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 2.16 ff.

946 OLG Frankfurt, NStZ 2020, 173 (175).

947 BVerfG, NJW 2020, 1351 (1353, Rn. 43).

948 Ibid.

der Strafverfolgungsbehörden entzogen oder die Herkunft illegaler Vermögenswerte verdeckt werden sollen und ein krimineller Hintergrund im Sinne des § 261 StGB nicht ausgeschlossen werden kann.[949] Die vom Gesetzgeber vorgestellte Verdachtsschwelle unterhalb der Anforderungen des § 151 Abs. 2 StPO kann daher als akzeptiert angesehen werden.

(3) Kritische Würdigung

Die niedrige Verdachtsschwelle ist nicht ohne Kritik geblieben. Auf die dogmatische Nähe zur Strafanzeige wurde gerade eingegangen. Da jedoch für die Strafanzeige keine materiellen Voraussetzungen gelten, lässt sich aus der Frage der Rechtsnatur für den Verdachtsgrad des § 43 GwG nichts ableiten.

Aber auch unabhängig von der Rechtsnatur ist eine Übertragung des § 152 Abs. 2 StPO nicht einzusehen. Banken sind keine Ermittlungsbehörden und sollen es auch nicht sein. Das Geldwäscherecht soll die strafprozessuale Ermittlung nicht ersetzen, sondern die Informationen liefern, auf denen die Ermittlungen aufbauen können.[950]

Die Verdachtsmeldungen der Verpflichteten bzw. die Maßnahmen, mit denen diese Meldungen erst vorbereitet werden, stellen also *Vorfeldermittlungen*[951] dar. Ihr Sinn liegt (noch) nicht in einer strafrechtlichen Prüfung eines Sachverhalts, sondern der aktiven Gewinnung von Verdachtssituationen[952]. Diese sollen dann von den Strafverfolgungsbehörden auf einen Anfangsverdacht hin untersucht werden, wobei eine operative Analyse als Zwischenschritt durch die FIU erfolgt, § 28 Abs. 1 Nr. 2 GwG (zu deren Rechtsnatur unten Kap. E II. 2. c. bb. (2)).

Die Beurteilung dieser Pflicht als „gewerberechtlich" überzeugt indes nicht.[953] Es ist schon nicht klar, was hiermit überhaupt gemeint sein soll. Dass (auch) Gewerbebetriebe von der Pflicht erfasst sind, ändert nichts an

949 Idem, mit Verweis auf OLG Frankfurt a.M., Hinweisbeschluss vom 17. Dezember 2012 - 19 U 210/12.

950 *Werner,* Geldwäsche, 1996, S. 141; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72.

951 Ausf. *Weßlau,* Vorfeldermittlungen, 1989, S. 25 ff.; Abgrenzung zu „Vorermittlungen": *Zöller,* Informationssysteme, 2002, S. 127 ff.; *Rogall*, ZStW 1991, 907 (945 ff.); *Roxin/Schünemann,* Strafverfahrensrecht, 29. Aufl. 2017, § 39 Rn. 17 f.

952 *Böse*, ZStW 2007, 848 (866 ff.).

953 *Barreto da Rosa* in Herzog GwG, § 43 Rn. 7 f.

deren Funktion. Dass private Betriebe für staatliche Aufgaben eingesetzt werden, an denen sie nur mittelbar und mehr zufällig auch ein Eigeninteresse haben, ist der springende Punkt der Inpflichtnahme. Sie unterscheidet sich von anderen Spielarten der *Criminal Compliance* dadurch, dass die jeweiligen Unternehmen nicht bloß ihre unternehmensinternen Risiken bekämpfen sollen, sondern dass die spezifische Nähe bestimmter Wirtschaftsteilnehmer zu externen Gefahrenlagen (wie etwa Kreditinstitute zur Finanzkriminalität) ausgenutzt werden soll (s. o. Kap B. II. 2. B. b. (a)).[954] Die Motivation des Staates liegt nicht darin, von den Unternehmen ausgehende Risiken einzudämmen, sondern die Unternehmen zur Bekämpfung von Drittrisiken zu utilisieren. Dementsprechend muss sich der Staat auch die Handlungen dieser in die Pflicht genommenen Unternehmen als eigene Eingriffe gegenüber Dritten zurechnen lassen.[955]

Gerade im Bereich der Verdachtsgewinnung durch Massenüberwachung ist dieses Vorgehen mittlerweile typisch. Da der Staat selbst im Sicherheitsrecht grundsätzlich reaktiv handeln muss, lagert er die Vorermittlungen an Private aus und grenzt dann lediglich die Übermittlung der entsprechenden Informationen ein.

Die Bezeichnung der geldwäscherechtlichen Meldepflicht als „gewerberechtlich" kann nur als Versuch gedeutet werden, von der Tatsache abzulenken, dass es sich um eine massenhafte Verdachtsgewinnung i. R. d. Sicherheitsgewährleistung handelt. Tatsächlich sind die Maßnahmen der Verpflichteten primär sicherheitsrechtlich motiviert. Die reaktiven (Mindest-)Eingriffsschwellen bestimmter Sicherheitsbehörden sollen unterlaufen werden.[956]

In letzter Konsequenz dienen die Meldungen dabei faktisch vor allem der Ahndung von Strafdelikten, wenngleich die ermittelten Informationen auch zur Gefahrenabwehr genutzt werden können. Diese Frage hängt aber primär davon ab, wie die Aufgaben der FIU charakterisiert werden (s. Kap. E II. 2. c. bb. (2)).

Jedenfalls ist die Herabsetzung der Verdachtsschwelle mitnichten von der Entlastung der Verpflichteten motiviert, denen keine strafverfahrensrechtli-

954 Weiter Begriff der Criminal Compliance bei *Hilgendorf* in Rotsch (Hrsg.), Compliance Zukunft, 2013, S. 19 (21).

955 BVerfGE 125, 260 (310) – Vorratsdatenspeicherung; dazu *Durner* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 154 ff. mwN.; aA. *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 2 Rn. 30.

956 *Krais,* Geldwäsche, 2018, Rn. 510; *Lenk*, JR 2020, 103 (107 f., insb, Fn 51); *Böse*, ZStW 2007, 848 (861, 866 ff.).

chen Pflichten – es fehlte ihnen auch die meist die Expertise – aufgebürdet werden sollen. Vielmehr ergibt sich aus der niedrigen Schwelle eine große Menge an Verdachtsmomenten und somit eine breitflächige Vorfeldermittlung[957], die der Staat wohl eigenständig weder vornehmen könnte noch dürfte.

Berechtigt sind im Übrigen auch die Einwände, die die praktischen Nachteile der niedrigen Schwelle betonen. Nach § 56 Abs. 1 Nr. 69 GwG handelt ordnungswidrig, wer entgegen § 43 GwG eine Verdachtsmeldung nicht abgibt. Das Erreichen des Verdachtsgrads führt also zu einer bußgeldbewährten Meldepflicht, der nachzukommen im finanziellen Interesse der Verpflichteten liegt. Dies hat wohl zwangsläufig den Effekt, dass ein Absenken des Verdachtsgrads zu einer Steigerung der Menge der gemeldeten Fälle führt.[958] Mit der zunehmenden Zahl an Verdachtsmeldungen geht aber keine steigende Anzahl erfolgreicher Strafverfahren einher.[959] In der Literatur wird dieses Phänomen mit „Masse statt Klasse" überschrieben und kritisch hervorgehoben.[960]

In der Tat wächst die Menge der Verdachtsmeldungen seit Jahren rasant. Waren es im Jahr 2009 noch knapp 10.000, gingen 2019 schon etwa 115.000 Meldungen bei der FIU ein.[961] Der Umstand, dass diese mit der Menge an Verdachtsmeldungen kaum zurechtkommt, zieht mittlerweile beträchtliche politische Kreise und hat sowohl im Rahmen des Wirecard-Skandals als auch im Wahlkampf zur Bundestagswahl 2021 eine (fragwürdige) Rolle gespielt.[962]

957 zum Begriff ausf. Weßlau, Vorfeldermittlungen, 1989, S. 25 ff.; Abgrenzung zu „Vorermittlungen": Zöller, Informationssysteme, 2002, S. 127 ff.; Rogall, ZStW 1991, 907 (945 ff.); Roxin/Schünemann, Strafverfahrensrecht, 29. Aufl. 2017, § 39 Rn. 17 f.

958 So auch *FIU*, (BKA), Jahresbericht, 2011, S. 11.

959 *T. Fischer,* StGB, 69. Aufl. 2021, § 261 Rn. 4 c; *FIU,* Jahresbericht, 2019, S. 21 bemerkt eine Steigerung zum Vorjahr von gerade einmal 2%, trotz immenser Steigerung der Meldungen von 2018 zu 2019, siehe dort S. 15.

960 *Höche/Rößler*, WM 2012, 1505 (1509 f.); *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 501; *Herzog* in Herzog GWG, 1. Aufl. 2010, § 11 Rn. 16; vgl. auch *Hein* in Schwark/Zimmer, KMRK, 4. Aufl. 2010, WpHG § 10 Rn. 21.

961 *FIU,* Jahresbericht, 2019, S. 15.

962 *Bartz/Böcking/Diehl ua.* – Deutschland, ein Paradies für Geldwäscher, Der Spiegel vom 27.08.2021, Ausgabe 35/2021.

bb. Form der Meldung

Die Meldung muss seit Juni 2016 gem. § 45 Abs. 1 S. 1 GwG elektronisch eingereicht werden. Die Verpflichteten müssen sich außerdem unabhängig von der Abgabe einer Meldung gem. § 45 Abs. 1 S. 2 GwG bei der FIU online registrieren. Eine Meldung auf dem Postweg ist nach § 45 Abs. 2 GwG nur in Ausnahmefällen möglich oder nach § 45 Abs. 1 S. 3 GwG, wenn die elektronische Datenübermittlung gestört ist.

Ein elektronisches Meldesystem hat die FIU, mit einiger Verzögerung[963], zum Februar 2018 durch die Bereitstellung des Meldeportals „goAML" implementiert.[964] Bei goAML handelt es sich um eine Software, die vom Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC) entwickelt wurde und den FIUs der UNO-Mitglieder bereitgestellt wird.[965] Laut Angaben des UNODC wird goAML aktuell von 56 FIUs verwendet.[966]

Im goAML-Webportal können sich die Verpflichteten registrieren und auf zwei verschiedene Arten Meldungen einreichen. Sie können entweder eine XML-Datei mit vorgeschriebenen Elementen[967] hochladen oder eine Webmaske ausfüllen[968].

cc. Umfang der Meldepflicht

Gemeldet werden müssen alle i. S. d. § 43 Abs. 1 GwG verdächtigen baren und unbaren Transaktionen sowie andere Vermögensverschiebungen,

963 *Barreto da Rosa* in Herzog GwG, § 45 Rn. 1; *Greite* in Zentes/Glaab GWG, § 45 Rn. 3 ff.; bis zum Februar 2018 galt eine Übergangslösung, siehe *FIU,* Schreibem vom 09.01.2018, GZ: SV 6002-2018.RUN.800002-DVIII.D.12, verfügbar unter https://web.archive.org/web/20220522191027/https://www.coburg.ihk.de/media/merkblatt_der_generalzolldirektion.pdf, zuletzt aufgerufen am 12.01.2025 (Original-Link zuletzt aufgerufen im Mai 2022).

964 *FIU,* goAML Web, https://goaml.fiu.bund.de/Home, zuletzt aufgerufen am 12.01.2025; s.a. *FIU,* Handbuch goAML Web Portal, https://www.zoll.de/DE/FIU/Software-goAML/Publikationen/publikationen_node.html, Stand 01.02.2024, https://www.zoll.de/DE/FIU/Software-goAML/Publikationen/publikationen_node.html, zuletzt aufgerufen am 12.01.2025

965 *UNODC,* goAML, https://unite.un.org/goaml/, zuletzt aufgerufen am 12.01.2025.

966 Ibid.

967 *FIU,* XML-Schema Dokumentation, Stand 20.08.2018.

968 Hierzu ausf. *FIU.,* Handbuch goAML Web Portal, Stand 27.01.2020.

unabhängig von ihrer Höhe und unabhängig davon, ob sie schon durchgeführt wurden, noch bevorstehen oder nach § 46 GwG abgelehnt wurden.[969] Für verdächtige Geschäftsbeziehungen gilt dasselbe. Sie sind auch dann meldepflichtig, wenn sie sich erst anbahnen.[970]

Die Meldung muss nicht nur den konkreten Vorgang, sondern auch die wesentlichen Umstände enthalten, aus denen sich das Verdachtsmoment ergibt. Bei einer ungewöhnlichen Transaktion, etwa einer sehr hohen Bargeldeinzahlung, müssen der Meldung deshalb Begleitinformationen beigefügt werden, aus denen sich die Auffälligkeit ableiten lässt, z. B. vergangene Umsätze.[971] In der Praxis wird außerdem der Sachverhalt in Form einer schriftlichen Begründung präsentiert, wobei sich der Gutachtenstil bewährt haben soll.[972]

Die konkreten Details der Meldung ergeben sich in der Praxis zwangsläufig aus der goAML-Webmaske bzw. den Anforderungen an die XML-Datei. Sämtliche der folgenden zusammengefassten Angaben sind dem Handbuch zur goAML-Webmaske[973] entnommen.

Bei der Meldung sind zunächst Informationen über den meldenden Verpflichteten wie Name, Adresse etc. und des meldenden Mitarbeiters einzutragen sowie die unmittelbaren Umstände der Meldung, etwa das Datum, das Aktenzeichen, der Meldungstyp und der Grund der Meldung. Sodann sind sämtliche Informationen über die Transaktion anzugeben, d. h. der Betrag, die Währung, die handelnde Person, interne Referenznummer, das Transaktionsverfahren, Datum, Ort (z. B. Filiale), Verwendungszweck sowie sonstige Informationen als Kommentar.

Hinsichtlich der ausführenden Person sind alle persönlichen Daten inklusive Legitimationsdokumente (etwa die Ausweisnummer) und – soweit vorhanden – die E-Mail-Adresse anzugeben. Bei Überweisungen sind sinnvollerweise all diese Informationen auch bzgl. des Empfängers und der beteiligten Personen und Institutionen anzugeben. Steht die Transaktion mit Gütern im Zusammenhang, sind alle verfügbaren Informationen über die entsprechenden Sachen anzugeben, wie z. B. Identifikationsnummern oder bei Immobilien die Adresse des Objekts.

969 *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 71 f.
970 Idem, S. 72.
971 Idem, S. 76.; s.a. *FIU,* Handbuch goAML Web Portal, Stand 27.01.2020, S. 77 f.
972 *Täubner* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 377 (394);
973 *FIU,* Handbuch goAML Web Portal, Stand 27.01.2020, S. 30 ff.

Geht die Transaktion von einem Bankkonto aus, sind die Kontoinformationen anzugeben. Dazu zählen u. a. die Kontonummer, der Name, das Institut, BLZ oder BIC/Swift, die Kontoart, der Kontostand und die Berechtigten.

dd. Eingang, Speicherung und Verbleib der Meldung bei der FIU

Die Meldung geht bei der FIU ein, die sie nach § 30 Abs. 1 Nr. 1 GwG entgegennehmen und verarbeiten muss. Das weitere Schicksal der Meldung bestimmen die §§ 30 ff. GwG.

Die Grundaufgabe der FIU besteht darin, die Meldungen auf ihren Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung zu analysieren, § 30 Abs. 2 GwG, und dann nach § 32 ff. GwG an die zuständigen Stellen weiterzuleiten. Dies gilt prinzipiell für alle nach § 30 Abs. 1 GwG entgegenzunehmenden Meldungen. Der Datenverarbeitungsprozess der FIU hängt also prinzipiell nicht von der Art der Meldung bzw. von der Person des Verpflichteten ab.[974]

Aufgrund der Fülle der Verdachtsmeldungen (s. o. III. 2. c. aa. (3)) ist es praktisch nicht denkbar, dass die Meldungen kurzfristig oder gar in Echtzeit bzw. unmittelbar nach deren Eingang bearbeitet werden. Laut einer Antwort der Bundesregierung auf eine kleine Anfrage von Abgeordneten und der Fraktion Bündnis90/Die Grünen werden zwar alle Meldungen umgehend erstbewertet – insbesondere, um Fristfälle nach § 46 GwG herauszufiltern, Angaben zur Dauer der Bearbeitung der nicht-priorisierten Fälle konnte die Bundesregierung machen.[975]

Grundsätzlich werden sämtliche Verdachtsmeldungen zunächst gespeichert, unabhängig davon, ob sie zeitnah weitergegeben werden.[976] Die Ermächtigung der FIU zur Speicherung ergibt sich aus § 29 Abs. 1 GwG, der als Generalklausel zur Verarbeitung von Daten[977] im Rahmen ihrer Aufgaben nach § 28 GwG dient.[978]

974 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (226).
975 BT-Drs. 19/2263, S. 4.
976 BT-Drs. 18/11928, S. 26; *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 11; *Barreto da Rosa* in Herzog GwG, § 32 Rn. 26, § 37 Rn. 19.
977 i. S. d. §§ 3, 46 Nr. 2 BDSG bzw. Art. 4 Nr. 2 DSGVO, vgl. BT-Drs. 18/11555, S. 140; zur Identität der Legaldefinitionen *M. Lang* in Taeger/Gabel DSGVO - BDSG, § 3 BDSG Rn. 18.
978 Vgl. BT-Drs. 18/11555, S. 140.

Die Daten sind nach §§ 37 Abs. 2, 38 Abs. 2 GwG eigentlich zu löschen, sobald *die Kenntnis dieser Daten für die Aufgabenerfüllung nicht mehr erforderlich ist.* Grundsätzlich wäre dies nach Abschluss der operativen Analyse der Fall. Es sei denn, es bestehen Anhaltspunkte, dass die Daten in der Zukunft noch relevant werden.[979] Die Bundesregierung argumentiert jedoch für das Bestehen starrer Löschfristen unabhängig von der Notwendigkeit der Daten und beruft sich dabei auf §§ 37 Abs. 2-4, 39 Abs. 1 GwG.[980] Personenbezogene Daten, die durch die FIU bearbeitet wurden, obgleich sie weitergeleitet wurden oder nicht, werden hiernach erst drei Jahre nach Beendigung der operativen Analyse automatisch gelöscht.[981]

Diese Praxis könnte auf einem falschen Verständnis der Speicher- und Löschpflichten nach §§ 37 ff. GwG beruhen. § 39 Abs. 1 GwG regelt die Errichtung automatisierter Dateien bei der FIU, die jeweils einer Anordnung bedürfen. Der Anordnung muss das Bundesinnenministerium zustimmen, § 39 Abs. 1 S. 2 GwG. Welche Dateien die FIU bislang errichtet hat, bzw. wie sie sortiert sind, unterliegt der Geheimhaltung.[982]

Die Bundesregierung bezieht sich in ihrer oben angesprochenen Antwort, in der sie von starren Löschfristen ausgeht, überraschenderweise nicht auf § 39 Abs. 2 GwG. Diese Vorschrift müsste aber korrekterweise mitzitiert werden. Dort erst wird unter Nr. 8 festgelegt, dass auch Fristen in der Anordnung aufgeführt werden müssen, in denen die in der Datei gespeicherten Daten überprüft werden müssen. § 39 Abs. 2 GwG stellt somit auf § 37 Abs. 4 GwG ab, der besagt, dass die FIU ihre gespeicherten Daten bei der Einzelfallbearbeitung und in festgesetzten Fristen, die im Gesetz aber nicht im Einzelnen dargelegt werden, prüfen muss, *ob gespeicherte personenbezogene Daten zu berichtigen, zu löschen oder in der Verarbeitung einzuschränken sind.*

§ 37 Abs. 4 und § 39 Abs. 2 GwG stehen also in einem gemeinsamen Kontext. Sie regeln aber nicht das Eintreten der Löschpflicht, sondern das Mindest-Überprüfungsintervall der gespeicherten Daten. Die Löschpflicht tritt grundsätzlich unmittelbar nach der operativen Analyse mit negativem Ausgang ein – spätestens aber, wenn die Daten nicht mehr zur Aufgabenerfüllung notwendig sind, § 37 Abs. 2 GwG.

979 *C. Lang* in Zentes/Glaab GWG, § 37 Rn. 7 mit Verweis auf BVerwG, NJW 1994, 2499.
980 BT-Drs. 19/2263, S. 8 f.
981 Ibid.
982 *Barreto da Rosa* in Herzog GwG, § 29 Rn. 2.

§ 37 Abs. 4, § 39 Abs. 2 GwG beziehen sich also nur auf die Fälle, in denen nach der Analyse noch von einer Notwendigkeit ausgegangen wird, die Daten deshalb gespeichert werden und die Notwendigkeit dann zu einem späteren Zeitpunkt entfällt. Diese „Datenleichen" sind das Ziel der turnusmäßigen Überprüfung.

Die von der Bundesregierung geschilderte Praxis einer Speicherung sämtlicher bearbeiteten Meldungen für drei Jahre kann nur damit erklärt werden, dass die FIU nach jeder Analyse einfach prinzipiell annimmt, dass die Daten eventuell noch gebraucht werden, und sie deshalb speichert. Da die erste Kontrolle dann erst nach drei Jahren erfolgt, kommt es für diesen Zeitraum zu einer indifferenten Speicherung auch nicht notwendiger Daten. Die in § 37 Abs. 4 GwG eigentlich auch nach der Einzelfallbearbeitung vorgesehene Prüfung der Löschpflicht wird von der Bundesregierung ignoriert.

Für den Fall, dass die FIU im Rahmen der Analyse zu einem positiven Ergebnis gelangt, sie also von einem Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung ausgeht und den Fall weiterleitet, werden die gemeldeten Daten für fünf Jahre nach dem Abschluss der Analyse aufgehoben.[983]

ee. Ergebnis: Speicherung gefilterter Finanzdaten bei der FIU.

Wie soeben dargestellt, enthält jede Verdachtsmeldung eine Fülle an Finanzinformationen, da sie nicht nur die konkreten Umstände des verdächtigen Vorfalls enthalten, sondern auch jene, aus denen sich die Ausfälligkeit ergibt. Hierzu gehört insbesondere das Transaktionsverhalten bei Bankkunden, weshalb den Verdachtsmeldungen regelmäßig Umsatzlisten beigefügt werden dürften.[984] Jedenfalls im Rahmen der Verdachtsmeldungen wird also eine große Menge an sensiblen[985] persönlichen Daten verarbeitet.[986] Der Bundesregierung wurde im Rahmen einer kleinen Anfrage im Jahr 2018 die Frage gestellt, wie viele unterschiedliche Dateien die FIU

983 BT-Drs. 19/2263, S. 9.

984 *FIU,* Handbuch goAML Web Portal, Stand 27.01.2020, S. 78; *Täubner* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 377 (S. 395).

985 Vgl. BVerfGE 120, 274 (346 ff.) [2008] – Online-Durchsuchung.

986 Übersicht bei *Täubner* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 377 (393 ff.); umfänglich *FIU,* Handbuch goAML Web Portal, Stand 27.01.2020, S. 30 ff.

führt, und wie viele Personen je Datei geführt werden. Die Antwort fällt knapp aus. Es würden aktuell in den Dateien der FIU unter Nutzung von goAML *149.285 natürliche und juristische Personen gespeichert.*[987] Ob es sich bei all diesen Personen um eigene Verdachtsmeldungen handelt, oder wie viele Meldungen im Schnitt auf diese Personen entfallen, bleibt unbeantwortet. Da in den Meldungen regelmäßig eine ganze Fülle an Personen genannt wird (ausführende Person, Empfänger, wirtschaftlich Berechtigter, beschäftigte Mitarbeiter etc.), lässt sich aus der Antwort der Bundesregierung nicht abschätzen, wie viele Daten bzw. einzelne Vorgänge oder Verdächtige gespeichert sind. Es ist noch nicht einmal klar, ob alle diese Daten aus Verdachtsmeldungen stammen. Aus der Antwort ergibt sich nur, dass die FIU von *149.285 verschiedenen* Personen, inklusive juristischen Personen, irgendwelche Daten besitzt.

Wenngleich diese Daten dazu bestimmt sind, einem sicherheitsrechtlichen Zweck zu dienen und insofern von den Verpflichteten vorgefiltert werden, ist die Schwelle, ab der diese Daten übermittelt werden, sehr niedrig. Sie wird unterhalb dem strafprozessualen Anfangsverdacht eingeordnet (s.o.). Gleichzeitig regt das Compliance System des GwG die Verpflichteten dazu an, möglichst umfangreich zu melden (s. o.), da sie sich anderenfalls bußgeldpflichtig machen können.[988]

Durch die Verdachtsmeldungen entsteht bei der FIU daher ein gewaltiger Datenpool, der sich aus sämtlichen Meldungen und den hierzu eingeholten Informationen speist.[989] Ausweislich von Angaben der Bundesregierung werden die Meldungen für mindestens drei Jahre gespeichert, da die eigentlich unmittelbar einsetzenden Löschpflichten erst im Rahmen der turnusmäßigen Datenprüfungen umgesetzt werden.[990] Es besteht damit ein Normenregime, das den Umgang mit diesen Daten einigermaßen streng reglementieren könnte, faktisch aber nicht angewandt wird.

Das GwG sieht aber nicht nur eine Speicherpflicht für die vorgefilterten Meldedaten bei der FIU nach §§ 29, 39 GwG vor, sondern auch eine umfassende Aufzeichnungs- und Aufbewahrungspflicht der Verpflichteten. Auf diese soll im folgenden Abschnitt eingegangen werden.

987 BT-Drs. 19/2263, S. 3.
988 Bspw. OLG Frankfurt, NStZ 2020, 173 (175).
989 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (228).
990 BT-Drs. 19/2263, S. 8 f.

d. Aufzeichnungs- und Aufbewahrungspflicht nach § 8 GwG

Die nach § 2 GwG Verpflichteten müssen gem. § 8 Abs. 1 GwG bestimmte Informationen aufzeichnen und aufbewahren. Das GwG verpflichtet insbesondere Banken und Zahlungsinstitute zur Vorhaltung massenhafter Kontoinhaltsdaten ihrer Kunden. Nicht nur Verdachtsmeldungen sind zu speichern, auch alle unauffälligen Transaktionsdaten unterfallen § 8 Abs. 1 GwG.

aa. Verdachtsmeldungen

Nicht nur die FIU, auch die Verpflichteten haben die Verdachtsmeldungen zu speichern. Nach § 8 Abs. 1 Nr. 4 GwG sind die *Erwägungsgründe und eine nachvollziehbare Begründung des Bewertungsergebnisses eines Sachverhalts hinsichtlich der Meldepflicht nach § 43 Abs.1 GwG* aufzuzeichnen und aufzubewahren. Diese Pflicht betrifft alle Fälle, in denen konkret geprüft wurde, ob eine Pflicht zur Meldung bestehen könnte – also auch jene, in denen von einer Meldung abgesehen wurde.[991] Ziel ist es, für die Aufsichtsbehörden nachvollziehbar zu halten, ob die Beurteilung sachgerecht erfolgt ist, bzw. auf richtigen Tatsachen und allgemeingültigen Bewertungsmaßstäben beruht.[992] Die Erwägungsgründe umfassen daher sinnvollerweise sämtliche Informationen, die im Rahmen der Verdachtsmeldung an die FIU übermittelt wurden, da auch im Rahmen der Verdachtsmeldung die Hintergründe der Auffälligkeit dargelegt werden müssen (s. o.). Der Datenbestand der Verdachtsmeldungen bei den Verpflichteten wird also im Falle einer erstatteten Meldung regelmäßig identisch mit der übermittelten Meldung sein, jedenfalls aber nicht dahinter zurückstehen. Die Aufbewahrungspflicht läuft in diesen Fällen letztlich darauf hinaus, dass sowohl bei der FIU als auch bei den Verpflichteten die Meldung aufbewahrt wird. Unterschiede bestehen allenfalls hinsichtlich der Frist (dazu unten).

991 BT-Drs. 18/11555, S.114; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 74 f.; *Täubner* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 377 (393).

992 *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 74 f.

bb. Allgemeine Transaktionsdaten aufgrund der Überwachungspflicht

Neben dieser immerhin von einem gewissen Verdachtsmoment geprägten Dokumentationspflicht enthält § 8 GwG in Abs. 1 Nr. 1 GwG eine generell formulierte Pflicht zur Aufzeichnung und Aufbewahrung *aller Informationen, die von den Verpflichteten im Rahmen der Erfüllung ihrer Sorgfaltspflichten erhoben oder eingeholt werden.*

Das betrifft nach § 8 Abs. 1 Nr. 1 lit. a) GwG zunächst die Informationen, die im Rahmen der Identifizierungspflicht i. S. d. § 10 Abs. 1 Nr. 1, §§ 11, 12 GwG eingeholt wurden. Insbesondere sind nach § 8 Abs. 2 S. 1 GwG die Art, die Nummer und die Behörde, die das zur Überprüfung der Identität vorgelegte Dokument ausgestellt hat, aufzuzeichnen. Von den vorgelegten Identifikationspapieren – insbesondere Ausweispapieren – müssen die Verpflichteten nach § 8 Abs. 2 S. 2 GwG Kopien anfertigen.

Auch wenn diese umfangreiche Speicherung von Identifikationsdaten, gerade auch in Kombination mit der Kontobestandsabfrage nach § 24c KWG, schon einen beachtlichen vorgehaltenen Datenbestand darstellt, soll der hier angelegte Fokus doch auf § 8 Abs. 1 Nr. 1 lit. b) GwG liegen. Dieser beinhaltet eine Aufzeichnungs- und Aufbewahrungspflicht für Informationen *über Geschäftsbeziehungen und Transaktionen, insbesondere Transaktionsbelege, soweit sie für die Untersuchung von Transaktionen erforderlich sein können*, die im Rahmen der Erfüllung der Sorgfaltspflichten erhoben und eingeholt werden.

(1) Überwachung als anfängliche Pflicht zum Erfassen aller Transaktionen

§ 8 Abs. 1 Nr. 1 lit. b) GwG muss im Kontext mit der Überwachungspflicht des § 10 Abs. 1 Nr. 5 GwG verstanden werden. Das GwG selbst beinhaltet keine präzisen Aussagen zum Umfang der Überwachungspflicht, geschweige denn, wie die *Überwachung* ausgestaltet werden soll. Erst der Blick auf § 25h Abs. 2 KWG und § 14 Abs. 1 S. 2 GwG bringt i. V. m. mit den ESA-Leitlinien die erhellende Erkenntnis, dass die Überwachungspflicht eine originäre Pflicht zur Wahrnehmung sämtlicher Transaktionen beinhaltet. Aus den Leitlinien ergibt sich,[993] dass die Verpflichteten in Abhängigkeit von den jeweiligen Umständen zwischen einer Echtzeit- oder einer nach-

993 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.74, 4.75.

träglichen Überwachung wählen können. Beides ist nur möglich, wenn die Sicherungsmaßnahmen der Verpflichteten zumindest alle Transaktionen wahrnehmen können. Das GwG kann also nicht davon ausgehen, dass die Datenbasis für die Transaktionsüberwachung ohnehin vorliegt, um sodann nur deren nachträgliche, verschiedentlich intensive Überprüfung anzuordnen. Ein solches Verständnis würde die Echtzeitüberwachung ausschließen. Vielmehr ist schon die Anlage dieser Datenbasis, auch wenn sie zwangsweise ohnehin entsteht, eine Pflicht des Geldwäscherechts (s. o. 2. b. aa. (2)).

Jedenfalls aber ist die Datenbasis in Form aller durchgeführten Transaktionen für die Überwachungspflicht unabdinglich. Sie kann deswegen auch aus der Aufzeichnungspflicht des § 8 Abs. 1 Nr. 1 GwG konstruiert werden, wenn man die Überwachungspflicht auf die Kontrollpflicht einer schon existierenden Datenbasis reduziert. Dies ergibt sich aus der Pflicht, sämtliche Transaktionen zu prüfen. Hierfür müsste der gesamte Datenbestand bzgl. der Kundentransaktionen als *Information einbezogen* werden und wäre folglich nach § 8 Abs. 1 Nr. 1 GwG in vollem Umfang aufzuzeichnen (s. o. 2. b. aa. (2)).[994]

(2) Unabhängige Pflicht zur Speicherung von Transaktionsbelegen in der GWRL und dem Auslegungsmaterial

Zu diesem Verständnis, dass sämtliche Transaktionsbelege im Rahmen einer Geschäftsbeziehung aufbewahrt werden müssen, gelangt man auch zwingend, wenn man zur Auslegung des § 8 Abs. 1 Nr.1 GwG den Art. 40 Abs. 1 lit. b) der GWRL heranzieht. Dessen Wortlaut enthält hinsichtlich der Aufbewahrungspflicht für Transaktionsbelege, anders als § 8 Abs. 1 Nr. 1 GwG, von vorneherein keine Anknüpfung an die Sorgfaltspflichten.

Stattdessen heiß es dort schlicht: „*Die Mitgliedstaaten schreiben vor, dass die Verpflichteten die nachstehenden Dokumente und Informationen im Einklang mit dem nationalen Recht für die Zwecke der Verhinderung, Aufdeckung und Ermittlung möglicher Geldwäsche oder Terrorismusfinanzierung durch die zentrale Meldestelle oder andere zuständige Behörden aufbewahren: a)… b) die Transaktionsbelege und -aufzeichnungen (…) für die Dauer von fünf Jahren nach Beendigung der Geschäftsbeziehung mit dem Kunden oder nach dem Zeitpunkt einer gelegentlichen Transaktion.*“

994 Für ein solches Verständnis etwa *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (462), wohl auch *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18.

Die ESA-Leitlinien bestätigen dieses Bild. Dort wird in verschiedenen Bullet Points aufgeführt, dass Aufzeichnungen geführt werden müssen für: „*a) die für die Sorgfaltspflichten gegenüber Kunden relevanten Informationen; b) ihre Risikobewertungen; und c) Transaktionen.*"[995] Somit wird klargestellt, dass Transaktionsaufzeichnungen immer geführt werden müssen, unabhängig von der Frage, ob man sie auch als *zur Erfüllung der Sorgfaltspflichten notwendige Informationen* subsumieren könnte.

Auch die FATF-Empfehlungen[996] sind in dieser Hinsicht eindeutig. Unter der lfd. Nr. 11 wird im ersten Absatz verdeutlicht, dass alle notwendigen Transaktionsdaten aufbewahrt werden sollen, um Auskunftsersuchen staatlicher Stellen nachkommen zu können. Diese Aufbewahrungen müssen ausreichend sein, um individuelle Transaktionen rekonstruieren zu können. In einem weiteren eigenen Absatz wird sodann festgestellt, dass die Finanzinstitute alle Aufzeichnungen über Transaktionen aufbewahren sollen, die sie im Rahmen der Sorgfaltspflichten erlangt haben. Selbst wenn man die FATF-Empfehlungen nun so liest, dass sie aus der Erfüllung der Sorgfaltspflichten noch keine Pflicht zur Aufzeichnung sämtlicher Transaktionsdaten ableiten, so stellen sie dennoch ganz ausdrücklich klar, dass sämtliche Transaktionsbelege aufbewahrt werden müssen.

Das Geldwäschegesetz, das der Umsetzung der EU-Geldwäsche RL und mittelbar den FATF-Empfehlungen dient, muss also, ähnlich wie die §§ 25a KWG, 257 HGB, 22 UStG, 147 AO, eine Pflicht zur Speicherung sämtlicher Transaktionsdaten vorsehen.[997] Obwohl dies in der Literatur zum GwG nicht deutlich zum Ausdruck kommt, ergibt sich dies dort daraus, dass

995 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 5.1.

996 *FATF,* Recommendations 2012, konsolidierte Fassung März 2022.

997 Bzgl. Art. 40 Abs. 1 li.t b) 4. EU-GeldwäscheRL: *C. Kaiser,* Privacy in Financial Transactions, 2018, 102 ff. und *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (118 f; 123); vgl. auch *Article 29 Data Protection Working Party,* Opinion 14/2011 relating Money Laundering, 13.06.2011, Annex Nr. 28, 29, S. 22 ff.; ohne konkreten Normbezug: *Ioannides,* Money Laundering, 2016, S. 135; *Flores/Angelopoulou/Self* J. of Internet Services & Information Security 3 (2013), 101 (111); vgl. auch *Basel Committee on Banking Supervision*, (Bank of Internationational Settlements), Guidelines AML, January 2014 (rev. July 2020), S. 11; offen gelassen bei *B. Vogel* in Vogel/

auf die unterschiedlichen Fristen der Transaktionsaufbewahrungspflichten aufmerksam gemacht wird.[998]

Auch der historische Gesetzgeber ließ erkennen, dass er den Umfang der Speicherpflicht erkannt hat. In der ersten Form des GwG anno 1993 wurde noch auf eine Aufbewahrungspflicht für Transaktionsbelege verzichtet. In der Gesetzesbegründung wurde dies ausdrücklich damit erklärt, dass eine solche Pflicht ja schon in § 257 HGB enthalten sei.[999] Man ging also davon aus, dass eine geldwäscherechtliche Aufbewahrungspflicht der Pflicht nach § 257 HGB inhaltlich entsprechen würde und deswegen obsolet wäre. Dieses Verständnis trägt noch immer. § 8 Abs. 1 GwG und § 257 HGB sind gleichlaufend. Sie sehen eigenständig eine umfangreiche Pflicht zur Aufbewahrung sämtlicher Transaktionsdaten (in Form von Kontoauszügen) vor.

(3) Umfang, Form und Speicherfrist – „Big Data".

Die Transaktionsbelege müssen ausreichend sein, um die geldwäscherechtlichen Pflichten zu erfüllen.[1000] Sie enthalten dazu mindestens den Kundennamen, die Kontonummer, Empfangs- und Versendungsinstitut, Empfangs- und Versendungsland, das Transaktionsdatum, den Betrag und die Währung sowie den Verwendungszweck.[1001]

Die Aufbewahrungspflicht für alle nach § 8 GwG notwendigen Aufbewahrungen beträgt gem. § 8 Abs. 4 S. 1 GwG fünf Jahre unbeschadet anderer gesetzlicher Vorschriften. Es handelt sich somit um eine Mindestfrist.[1002] Jedenfalls nach zehn Jahren sind die Unterlagen zu vernichten, § 8 Abs., 4 S. 2 GwG. Die Frist beginnt nach § 8 Abs. 4 S. 4 GwG für Transaktionsbelege mit Ablauf des Jahres, in dem die Angabe festgestellt wurde, d. in dem Jahr, in dem die Transaktion durchgeführt wurde.

Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (990); aA. *Krais,* Geldwäsche, 2018, S. 284.

998 *Herzog* in Herzog GwG, § 8 Rn. 1, 18; *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 438; Diergarten/Fraulob GWG, S. 228; *Stegmann/Meuer* in Bürkle (Hrsg.), Compliance, 3. Aufl. 2020, § 12 Rn. 230.

999 BT-Drs. 12/2704, S. 16.

1000 Vgl. *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86 lit. d) S. 71.

1001 *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 53; *Fiedler/Krumma/Zanconato ua.,* Geldwäscherisiko Glücksspiel, 2017, S. 38.

1002 Hierzu krit. *Article 29 Data Protection Working Party,* Opinion 14/2011 relating Money Laundering, 13.06.2011, Annex Nr. 29.

Für Informationen, die zur Erfüllung der Pflichten nach § 10 Abs. 3 S. 1 GwG (insbesondere Identifizierung bei Begründung der Geschäftsbeziehung) eingeholt werden, beginnt die Pflicht hingegen erst mit dem Schluss des Kalenderjahres, in dem die Geschäftsbeziehung endet, § 8 Abs. 4 S. 3 GwG.

Zwischen Mindest- und Maximaldauer der Speicherung entscheiden die Verpflichteten nach Ermessen.[1003] Der Gesetzgeber ging davon aus, dass durch die mögliche Verlängerung (bis zu zehn Jahre) eine Angleichung an die §§ 257 Abs. 5 HGB, 147 Abs. 4 AO stattfinden sollte.[1004]

Bei den Transaktionsbelegen kommt es insofern zu einem Gleichlauf der Fristen. §§ 257 Abs. 5 HGB, 147 Abs. 4 AO sehen für Kontoauszüge eine Aufbewahrungspflicht von zehn Jahren vor[1005] und zwar, wie auch § 8 Abs. 4 S. 4 GwG, ab Ende des Kalenderjahres, in dem die Dokumente entstanden sind. Das Ermessen i. R. v. § 8 Abs. 1 GwG wird bei Kontoauszügen also leerlaufen.[1006]

Die aufbewahrungspflichtigen Daten können nach § 8 Abs. 3 GwG digital gespeichert werden, wenn sie mit den festgestellten Informationen übereinstimmen, während der Frist verfügbar bleiben und jederzeit in angemessener Zeit lesbar gemacht werden können. Im Hinblick auf die Feststellung, dass die Banken sämtliche Informationen über die Transaktionen ihrer Kunden archivieren müssen, ist diese Möglichkeit wohl auch kaum wegzudenken. Jedenfalls bei den größeren Banken, insbesondere den am Privatkundenmarkt beteiligten, liegen immense Datenmengen vor, deren Verwendung unter dem Stichwort „Big Data" auch in der IT-Wissenschaft diskutiert wird.[1007] Die Speicherung erfolgt längst nicht mehr nur in den Rechenzentren der Verpflichteten, sondern vermehrt in Kooperation mit großen Anbietern von Online- bzw. Cloud-Speichern.[1008] Transaktionsda-

1003 *Brian/Krais* in BeckOK GwG, § 8 Rn. 38.

1004 BT-Drs. 19/13827, S. 76.

1005 Vgl. *Schober*, BC 2013, 528 (532).

1006 *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 438.

1007 Etwa *Skyrius/Giriūnienė/Katin ua.* in Srinivasan (Hrsg.), Big Data, 2018, S. 451 (452 ff., 458 ff.); *Turner/Schroeck/Shockley*, (IBM Institute for Business Value, Saïd Business School at the University of Oxford), IBM Paper Big Data, 2013; *Deutsche Bank*, Big Data Whitepaper, 2014; Sapozhnikova/*Gayanova/Vulfin ua.* in, ITNT, IV INT, 2018, S. 228 (229 f.); *Westermeier*, Information, Communication & Society 23 (2020), 2047 (2051 f.).

1008 Die Deutsche Bank hat eine große Kooperation mit Google angekündigt, siehe *Deutsche Bank,* Deutsche Bank & Goolge Cloud partnership, 4. Dezember, 2020,

ten dürften bei diesen Datenbeständen einen großen Anteil ausmachen[1009] und sollen laut einem der größeren Anbietern von Cloud-Speichern insbesondere zum Erkennen von Geldwäsche verwendet werden.[1010]

3. Zusammenfassend: Speicherung von Inhaltsdaten bei FIU und Privaten

In diesem Kapitel wurde dargestellt, wie sich aus der GeldtransferVO und dem GwG, das die GWRL umsetzt, eine Pflicht zur Speicherung von Kontoinhaltsdaten ergibt. Es konnten zwei Datenpools identifiziert werden, die als taugliches Objekt einer Untersuchung aus dem Blickwinkel der Rechtsprechung zur Vorratsdatenspeicherung infrage kommen.

a. Speicherung von Verdachtsmeldungen bei der FIU, §§ 28 ff., 43 Abs. 1 GwG

Zunächst agiert die Zentralstelle für Finanztransaktionsuntersuchungen bzw. Financial Intelligence Unit – FIU als Sammelstelle für Verdachtsmeldungen bzgl. Geldwäsche und Terrorismusfinanzierung nach § 28 Abs. 1 Nr.1, § 30 Abs. 1, 2, § 43 Abs. 1 GwG. Um dieser Aufgabe nachzukommen, darf sie persönliche Daten verarbeiten, § 29 GwG.

Die Verdachtsmeldungen werden unterhalb eines strafprozessualen Verdachtsgrads[1011] von privaten Akteuren an die FIU übermittelt. Die Verpflichteten werden danach nicht selbst als Strafverfolger oder Verfassungsschützer tätig, sondern lediglich als Lieferanten von Informationen, die

---

https://www.db.com/news/detail/20201204-deutsche-bank-and-google-cloud-sign-pioneering-cloud-and-innovation-partnership?language_id=1, zuletzt aufgerufen am 12.01.2025.

1009 *Turner/Schroeck/Shockley*, (IBM Institute for Business Value, Saïd Business School at the University of Oxford), IBM Paper Big Data, 2013, S. 6.

1010 *Stackowiak et al.*, (Oracle Corp.), Big Data in Financial Services and Banking, 2015, S. 7.

1011 BT-Drs. 18/11928, S. 26.; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72; *Bundesministerium der Finanzen,* Auslegunsghinweise Verdachtsmeldewesen, 06. November 2014, S. 3; *Greite* in Zentes/Glaab GWG, § 43 Rn. 10 ff.; *Findeisen* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. II, 3. Auflage 2017, § 85 Rn. 62; krit.; *Barreto da Rosa* in Herzog GwG, § 43 Rn. 5 ff., 24 ff.; *Degen,* Geldwäsche, 2009, 127 f.; *Krais,* Geldwäsche, 2018, Rn. 510 f.; *Klugmann*, NJW 2012, 641 (644); *Bülte*, NZWiSt 2017, 276 (280 f.).

eventuell, ausgehend von einer weiteren Analyse, durch die FIU an verschiedene Sicherheitsbehörden weitergeleitet werden können. Im Moment der Meldung ist somit gerade nicht klar, ob die an die FIU übermittelten Informationen eine sicherheitsrechtliche Relevanz aufweisen. Sie sind allenfalls *auffällig* im geldwäscherechtlichen Sinne.[1012]

Die FIU prüft die Meldungen nach Aussagen der Bundesregierung zwar umgehend, d. h. spätestens am Folgetag des Eingangs, allerdings nur sehr oberflächlich.[1013] Aufgrund des mittlerweile gewaltigen Meldeaufkommens[1014] wäre eine intensive Prüfung unmittelbar nach der Übermittlung auch nicht denkbar. Die Meldungen werden stattdessen von der FIU gespeichert und in einer Datei, für die nach § 39 GwG eine Errichtungsanordnung gilt, abgelegt. Dort liegen sie, nach Aussage der Bundesregierung, für mindestens drei Jahre nach Bearbeitung, auch wenn sie nicht weitergeleitet wurden.[1015] Bei der FIU liegen also massenhaft Kontoinhaltsdaten vor, bei denen unklar ist, ob sie sicherheitsrechtlich relevant sind, oder nicht.

b. Speicherung von Verdachtssachverhalten und Transaktionsdaten bei den Verpflichteten

Die noch weitaus größere Datensammlung, die im Rahmen der geldwäscherechtlichen Vorschriften angelegt werden muss, findet sich aber unmittelbar und dezentralisiert bei den Verpflichteten.

aa. Art. 16 GeldtransferVO

Die an einem Geldtransfer beteiligten Institute müssen schon nach Art. 16 Abs. 1, S. 2 GeldtransferVO alle Angaben, die nach den Art. 4-7, 11 Geld-

1012 BT-Drs. 18/11928, S. 26.; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72; *Bundesministerium der Finanzen,* Auslegunsghinweise Verdachtsmeldewesen, 06. November 2014, S. 3; *FIU,* Anhaltspunktepapier - Newsletter 11/2014, August 2014, https://geldwaesche-beauftragte.de/wp-content/uploads/2017/04/FIU_Newsletter_Ausgabe_Nr._11_-August_2014.pdf, zuletzt aufgerufen am 12.01.2025; Die FIU-Indikatoren für Auffälligkeit zusammengefasst bei zusammengefasst bei *Diergarten* in Hauschka/Moosmayer/Lösler (Hrsg.), Hdb. Haftungsvermeidung, 3. Aufl. 2016, § 34 Rn. 392; *Krais,* Geldwäsche, 2018, Rn. 717.

1013 BT-Drs. 19/2263, S. 4.

1014 *FIU,* Jahresbericht, 2019, S. 15 ff.

1015 BT-Drs. 19/2263, S. 8 f.

transferVO für den entsprechenden Geldtransfer bereitgestellt werden, fünf Jahre lang aufbewahren (s. o. 1. d.). Bei diesen Angaben handelt es sich um die entscheidenden Umstände eines Transfervorgangs – also die Namen der Beteiligten sowie die Kontonummern, außerdem die Anschrift des Auftraggebers, die Nummer eines Ausweisdokuments oder das Geburtsdatum und der Geburtsort des Auftraggebers. Die GeldtransferVO dient insofern ausdrücklich dem Nachvollzug der „Papierspur"[1016] unbarer Zahlungen.

Der Anwendungsbereich der Verordnung ist aber mit Blick auf das Massengeschäft überschaubar. Nach Art. 5 GeldtransferVO sind nämlich Zahlungen innerhalb der EU von den Übermittlungsanforderungen weitgehend ausgenommen. Es müssen lediglich die Konto- bzw. die Transaktionsnummern, bei Transaktionen außerhalb einer Geschäftsbeziehung (Einmalzahlungen), übermittelt werden. Die übrigen Daten können zwar vom Dienstleister des Begünstigten proaktiv abgefragt werden. Dieses Anfragerecht ist aber bei Transaktionen unterhalb von 1.000,00 € begrenzt auf die Namen von Auftraggeber und Begünstigten sowie die Konto- bzw. Transaktionsnummern nach Art. 5 Abs. 2 lit. b) GeldtransferVO. Außerdem sind Bareinzahlungen generell vom Anwendungsbereich gem. Art. 2 Abs. 2, 4 lit. a) GeldtransferVO ausgenommen.

bb. § 8 Abs. 1 Nr. 2 GwG (Art. 40 Abs. 1 lit. b) GWRL)

Brisanter als die GeldtransferVO hinsichtlich der Speicherung von Kontoinhaltsdaten sind daher § 8 Abs. 1 Nr. 2 GwG i. V. m. § 10 Abs. 1 Nr. 5 GwG und § 25h Abs. 2 S. 1 KWG.

Die in § 10 Abs. 1 Nr. 5 GwG, § 25h Abs. 2 S. 1 KWG vorgesehene kontinuierliche Überwachungspflicht wird in der Praxis obligatorisch durch ein umfassendes Kontenmonitoring und Einzelfall*screening* umgesetzt.[1017] Ins-

1016 *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25g KWG Rn. 3; *Schatz* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 525 (527); vgl. auch Erwägungsgrund 9, EU-GeldtransferVO.

1017 BT-Drs. 16/9038, S. 50; *DK*, Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d; *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18; *ders.* in Herzog GwG, § 25h Rn. 12 ff.; *Vollmuth,* Geldwäscheprävention, 2020, 168 f; 171 ff.; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (462); *Jahn*, ZRP 2002, 109 (110); *Herzog/Christmann*, WM 2003, 6 (11).

besondere Banken, die sich am privaten Massenverkehr beteiligen, müssen hierfür ausdrücklich spezielle EDV-Systeme etablieren.[1018]

Die Überwachungspflicht setzt nach dem hier vorgetragenen Verständnis die Datenbasis in Form aller Transaktionen aller Kunden nicht einfach voraus, sondern konstituiert deren Anlegung. *Überwachen* bedeutet also nicht nur, dass die Banken ihre bestehenden Daten regelmäßig kontrollieren, sondern dass sie alle Transaktionen zumindest digital wahrnehmen und speichern. Es muss von der EDV an diesem Punkt nicht immer eine Auffälligkeit registriert werden, es kann auch eine nachträgliche Kontrolle erfolgen.[1019] Die abstrakte Pflicht zur Anlegung dieser Datenbasis bleibt vom Zeitpunkt der Rasterung aber unberührt.

Aus § 8 Abs. 1 Nr. 2 GwG folgt im Anschluss die Pflicht zur Aufbewahrung dieses Datensatzes. Selbst wenn man ausschließlich von Überwachung in Form einer nachträglichen Kontrolle ausgehen würde, müsste aber ohnehin eine Speicherung erfolgen, denn § 8 Abs. 1 GwG schreibt auch die Aufbewahrung solcher Informationen vor, die *zur* Erfüllung der Sorgfaltspflichten eingeholt wurden.[1020] Da das Kontenscreening bzw. -monitoring[1021] sämtliche Transaktionen erfasst[1022], muss die gesamte Transaktionsdatenbasis herangezogen werden und fällt spätestens jetzt unter die Aufbewahrungspflicht. Dieses Ergebnis wird vom Wortlaut des Art. 40

1018 BT-Drs. 16/9038, S. 50; dazu *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d.; *Langweg* in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006, § 14 GWG Rn. 105; *Achtelik* in Herzog GwG, § 25h KWG Rn. 11 ff.; *ders.* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h KWG Rn. 16 ff.; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (456 f.); *Mülhausen* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 43 Rn. 50 ff.

1019 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.74 a); zur Praxis: *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 57; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (455 f.).

1020 So etwa *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h KWG Rn. 18; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (463).

1021 Begriffe nach *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14.

1022 BT-Drs. 16/9038, S. 50; *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d; *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 4 Rn. 11; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (463); *Degen,* Geldwäsche, 2009, S. 206.

Abs. 1 lit. b) der 4. GWRL und den Auslegungsmaterialen[1023] gestützt, die unabhängig von den Sorgfaltspflichten eine Aufbewahrung der Transaktionsbelege anordnen.

§ 8 Abs. 1 Nr. 2 GwG reiht sich somit ein in die Vorschriften des Zahlungs-, Aufsichts-, Handels- und Privatrechts, die ebenfalls eine Pflicht zur Speicherung von Kontotransaktionsdaten etablieren. Wenngleich er aufgrund der inhaltlichen Überschneidung mit diesen Vorschriften faktisch nicht zu mehr gespeicherten Daten führt, ergänzt § 8 Abs. 1 Nr. 2 GwG aber doch die Zwecke der Speicherung um einen sicherheitsrechtlichen Aspekt.

Die Vorschrift begründet also durchaus, wie die Opposition im Bundestag schon im Jahr 2008 befürchtet hatte[1024], nichts Geringeres als die unbegrenzte Pflicht für Banken und andere geldwäscherechtlich Verpflichteten zur Speicherung sämtlicher Transaktionsdaten ihrer Kunden.[1025]

1023 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 5.1; *FATF,* Recommendations 2012, konsolidierte Fassung März 2022, lfd. Nr. 11.

1024 BT-Drs. 16/9647, S. 3.

1025 Vgl. *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 101 ff; 493 ff.; *Milaj/C. Kaiser* Int. Data Privacy Law 7 (2017), 115 (123); *Article 29 Data Protection Working Party,* Opinion 14/2011 relating Money Laundering, 13.06.2011, Annex Nr. 28. 29, S. 22 ff.; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (462); offen gelassen bei *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (990); aA. *Krais,* Geldwäsche, 2018, Rn. 284.