Datenschutzrecht

Wolff / Brink

2. Auflage 2022
ISBN 978-3-406-78990-8
C.H.BECK

Art. 7 Rn. 61; gegen eine Differenzierung nach besonderer Angewiesenheit Hacker, Datenschutzprivatrecht 2020, 143 f. mit Verweis auf Erwägungsgrund 42 zur DS-GVO).

Zwar enthält Art. 7 Abs. 4 DS-GVO kein echtes und striktes „Koppelungsverbot" (so auch Buchner DuD 2016, 155 (158) und Kühling/Martini EuZW 2016, 448 (451)). Richtig ist aber, darin eine starke „Tendenz" zu sehen, dass bei Take-it-or-leave-it-Konstellationen die Freiwilligkeit sorgfältig zu prüfen ist. Art. 7 Abs. 4 DS-GVO bringt somit eine auf die Rechtsanwendung bezogene Berücksichtigungspflicht zum Ausdruck, was schon der Wortlaut („in größtmöglichem Umfang Rechnung getragen") belegt. Einwilligungsbasierte Lösungen sind auch deshalb in den Fällen fragwürdig, in denen die Datenverarbeitung für die Durchführung des Geschäfts objektiv erforderlich ist (so auch EDSA, Leitlinien 5/2020, Rn. 31). **48**

Mit den genannten, gegenüber der allgemeinen Rechtsgeschäftslehre erhöhten Anforderungen an eine wirksame Einwilligung werden **AGB-rechtliche Einwilligungen** problematisch. Die Kreditwirtschaft hat hierauf reagiert, indem sie, entgegen langjähriger Regelungstradition die Bankauskunft in den AGB Banken 01/2018 bei **natürlichen** Personen von einer **gesonderten** Einwilligung abhängig gemacht hat. Nr. 2 Abs. 3 AGB Banken 07/2018 lautet nun: „Die Bank ist befugt, über juristische Personen und im Handelsregister eingetragene Kaufleute Bankauskünfte zu erteilen, sofern sich die Anfrage auf ihre geschäftliche Tätigkeit bezieht. Die Bank erteilt jedoch keine Auskünfte, wenn ihr eine anderslautende Weisung des Kunden vorliegt. Bankauskünfte über andere Personen, insbesondere über Privatkunden und Vereinigungen, erteilt die Bank nur dann, wenn diese generell oder im Einzelfall ausdrücklich zugestimmt haben…". **49**

Im Anwendungsbereich der PSD II wird in der Literatur diskutiert, wie das Einwilligungserfordernis aus Art. 94 Abs. 2 PSD II bzw. § 59 Abs. 2 ZAG zu verstehen ist, wonach Zahlungsdienstleister die für das Erbringen ihrer Zahlungsdienste notwendigen personenbezogenen Daten nur mit der ausdrücklichen Zustimmung des Nutzers – „explicit consent" – verarbeiten dürfen (vgl. Störing in Casper/Terlau, ZAG, 2. Aufl. 2020, ZAG § 59 Rn. 26 ff.; Indenhuck/Stein BKR 2018, 136; Sander BKR 2019, 66 (70 f.)). Da der Wortlaut darauf hindeutet, dass von den sechs Erlaubnistatbeständen aus Art. 6 Abs. 1 DS-GVO im Anwendungsbereich des Zahlungsdiensterechts allein die Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO in Betracht kommt, wird die Norm teilweise als zugleich europarechtswidrig und verfassungswidrig angesehen (Sander BKR 2019, 66 (70 f.)). Mit dem Europäischen Datenschutzausschuss ist davon auszugehen, dass mit der Einwilligung iSv Art. 94 Abs. 2 PSD II keine Einwilligung iSv Art. 6 Abs. 1 lit. a DS-GVO gemeint ist (EDSA, Leitlinien 6/2020, Rn. 34 ff.). Es handelt sich nicht um einen selbstständigen Rechtfertigungsgrund nach Art. 6 Abs. 1 DS-GVO, sondern um eine besondere datenschutzrechtliche Vertragserklärung (s. EDSA, Leitlinien 6/2020, Rn. 35 f.; zusammenfassend Störing in Casper/Terlau, ZAG, 2. Aufl. 2020, ZAG § 59 Rn. 27). Rechtsgrundlage bleibt Art. 6 Abs. 1 lit. b DS-GVO (Vertragserfüllung), zusätzlich muss der Zahlungsdienstleister sicherstellen, dass der Nutzer im Rahmen des zugrundeliegenden Zahlungsdienstevertrags – getrennt von den übrigen Bestandteilen des Vertrags – der Datenverarbeitung zu konkret genannten Zwecken zustimmt (EDSA, Leitlinien 6/2020, Rn. 36; Störing in Casper/Terlau, ZAG, 2. Aufl. 2020, ZAG § 59 Rn. 27; Heinson, HdbEudDSR, 2019, Rn 56 ff.). **50**

2. Vertragserforderliche Datenverarbeitung (Art. 6 Abs. 1 lit. b DS-GVO)

Viele Datenverarbeitungsvorgänge bei Banken und Zahlungsdienstleistern sind zur Erfüllung eines Vertrages (oder auf Anfrage des Betroffenen zur Durchführung vorvertraglicher Maßnahmen) erforderlich (dazu EDSA, Leitlinien 6/2020, Rn. 14–19). **51**

Neben der Einwilligung beruht auch dieser Rechtmäßigkeitstatbestand auf betätigter Privatautonomie, da Verträge die Folge privatautonomer Entscheidungen darstellen (dezidiert Hacker, Datenschutzprivatrecht, 2020, 196 ff.) Der Begriff „Vertrag" umfasst hier somit Abschluss, Änderung, Abwicklung und Beendigung von sowohl rechtsgeschäftlichen sowie rechtsgeschäftsähnlichen Schuldverhältnissen als auch vertragsähnlichen Konstellationen (→ Art. 6 Rn. 28 ff.). **52**

Der Vertrag muss mit der betroffenen und nicht einer dritten Person bestehen, ansonsten kommt eine Verarbeitung nur auf Grundlage von lit. a, c und f (→ Rn. 71 ff.) in Betracht (NK-DatenschutzR/Schantz Art. 6 Rn. 20). Bei vernetzten Verträgen – wie für den Zahlungsverkehr typisch – dürften auch nicht nur Daten des „eigenen" Vertragspartners, sondern auch Daten der zum Vertragsnetz verbundenen (dazu grundlegend Grundmann AcP 207 (2007), 718 ff.) Betroffenen vertragserforderliche Daten iSd Art. 6 Abs. 1 lit. b DS-GVO sein. Auch die Person des Verantwortlichen und die des Vertragspartners können auseinanderfallen, solange die Verarbeitung durch den Dritten zur Erfüllung des Vertrages erforderlich ist (→ Art. 6 Rn. 30). **53**

54 Die Erforderlichkeit ist für jede im Vertrag enthaltene Dienstleistung separat zu beurteilen (EDSA, Leitlinien 6/2020, Rn 17 f.). Unerheblich sind vertragliche Bestimmungen darüber, ob eine Datenverarbeitung zur Vertragserfüllung erforderlich ist oder nicht (EDSA, Leitlinien 6/2020, Rn. 16, 18). Intensiv diskutiert wird, welche Anforderungen aus dem Tatbestandsmerkmal der Erforderlichkeit folgen. Einigkeit besteht weitgehend, dass eine Datenverarbeitung nicht erst erforderlich ist, wenn sie unverzichtbar ist (näher hierzu mit verschiedenen Kriterien EDSA, Leitlinien 2/2019, Rn. 33). Es wird aber teilweise ein unmittelbarer Zusammenhang mit dem konkreten Zweck des Vertrages (Gola/Schulz Art. 6 Rn. 38) verlangt oder gelehrt, vertragserforderlich könne es nicht sein, wenn die Datenverarbeitung ein „Geschäftsmodell" sei (NK-DatenschutzR/Schantz DS-GVO Art. 6 Abs. 1 Rn. 33; Kühling/Buchner/Buchner/Petri Rn. 41 ff.). Richtiger Weise sind solche Einbrüche in die freie Selbstbestimmung der Verbraucherinnen und Verbraucher jenseits des privatrechtlichen, nicht harmonisierten Schutzes unnötig und von der DS-GVO nicht gedeckt (grundlegend Hacker, Datenschutzprivatrecht, 2020, 198 f.).

55 Eine Datenverarbeitung im vorvertraglichen Bereich fällt nur unter Art. 6 Abs. 1 lit. b DS-GVO, soweit sie auf Anfrage des Betroffenen durchgeführt wird, wie etwa im Rahmen einer Bonitätsprüfung; im Falle eines Scheiterns des Vertragsabschlusses entfällt die Erforderlichkeit ex nunc (→ Art. 6 Rn. 33). Die Daten müssen dann gelöscht werden, aber erst, wenn sie nicht mehr für handelsrechtliche oder andere rechtlich gebotene Dokumentationszwecke gebraucht werden. Dies kann typisierend in einem Löschungskonzept festgelegt werden.

56 Die Vertragserfüllung von Finanz- und Zahlungsdienstleistern ist informationell vielfältig durch Rechtsvorschriften determiniert, die teilweise auch im öffentlichen Interesse auferlegt sind. Hier stellt sich die Frage nach dem Verhältnis zur Rechtfertigung aus lit. c, lit. e und lit. f.

57 Hier dürfte häufig der Fall einer Kumulation vorliegen. Beispielsweise ist die Erhebung der KYC-Daten des Vertragspartners rechtlich verpflichtend, bevor eine Geschäftsbeziehung begründet wird (→ Rn. 190 ff.). Sie ist damit für die Vertragserfüllung erforderlich und dient zugleich einer rechtlichen Verpflichtung; die hier oft ebenfalls einbezogenen Daten dritter Betroffener können allerdings nicht nach Art. 6 Abs. 1 lit. b erhoben und verarbeitet werden; hier bleiben Art. 6 Abs. 1 lit. c und lit. f DS-GVO. Da das Kreditinstitut auf die Datenerhebung angewiesen ist, um seine regulatorischen Pflichten zu erfüllen, überwiegen auch die Interessen.

58 Jedenfalls im Zahlungsverkehr und bei anderen, auf Authentifizierung basierenden Verfahren bei Finanzdienstleistungen ist auch die Betrugs- und Missbrauchserkennung zur Vertragserfüllung erforderlich (anders allg., aber nicht spezifisch auf Zahlungsdienstleistungen bezogen EDSA, Leitlinien 2/2019, Nr. 50).

3. Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DS-GVO)

59 Eine große Bedeutung hat wegen der ausgeprägten Regulierung und Inpflichtnahmen des Finanzsektors die Erfüllung rechtlicher Verpflichtungen des Verantwortlichen. Art. 6 Abs. 1 lit. c DS-GVO ist nicht deckungsgleich mit § 4 Abs. 1 BDSG aF, der noch jegliche Verarbeitungen für rechtmäßig erachtet hat, die durch Gesetz „erlaubt" waren (vgl. → Art. 6 Rn. 34 f.).

60 Im Gegensatz zu lit. a und b flankiert Art. 6 Abs. 1 lit. c DS-GVO keine privatautonome Entscheidung, sondern eine gesetzliche Verpflichtung aus Unionsrecht oder nationalem Recht. Dieser Erlaubnistatbestand ist als grundsätzliche Subsidiarität des Datenschutzrechts gedeutet worden; das präventive Verbot der Verarbeitung personenbezogener Daten befreie demnach nicht von anderen gesetzlichen Pflichten, vielmehr überlagerten letztere dieses (HK-DS-GVO/Reimer Art. 6 Rn. 22). Das wird allerdings der Systematik des DS-GVO nur bedingt gerecht. Der Anschein einer Durchsetzungsschwäche der DS-GVO gegenüber gesetzlichen Verpflichtungen ist allerdings im konzeptionellen Ausgangspunkt nicht berechtigt, da – soweit kein gleichrangiges Unionsrecht vorgeht – einerseits über Art. 6 Abs. 3 S. 4 DS-GVO, andererseits durch eine unmittelbare, nicht über die Erforderlichkeitsprüfung mediatisierte Anwendung europäischer oder nationaler Grundrechte die Wirksamkeit der DS-GVO auch gegenüber gesetzlichen Pflichten sicherzustellen ist. Im Finanzwesen ist dies aber noch nicht wirklich zu praktischer Wirksamkeit gebracht worden.

61 Heute beruhen die meisten rechtlichen Verpflichtungen von Finanz- und Zahlungsdienstleistern unmittelbar oder mittelbar auf Unionsrecht. Gewährt zB ein Zahlungsdienst einem Kontoinformationsdienst Zugang zu personenbezogenen Daten, kann er sich dazu auf das Art. 67 Abs. 1 PSD II umsetzende nationale Gesetz stützen (§§ 50–52 ZAG) und damit auf Art. 6 Abs. 1 lit. c DS-GVO berufen (s. EDSA, Leitlinien 6/2020, Rn. 25 ff.). Bei den typischen Datenverarbeitungsvorgängen des Risikomanagements, die nicht in gesetzlich spezifischer Form konkret, sondern nur über eine allgemeine Programm- oder Finalvorgabe determiniert sind, ist allerdings diskutabel, ob anstelle Art. 6 Abs. 1 lit. c DS-GVO eher Art. 6 Abs. 1 lit. f DS-GVO einschlägig ist. Das gilt

auch und insbesondere da, wo Datenverarbeitungsvorgänge – wie typisch in der Finanzindustrie – multifinal sind und den Eigeninteressen des Unternehmens, der Erfüllung des Vertrages und zugleich der Erfüllung regulatorischer oder geldwäschepräventiver Pflichten im öffentlichen Interesse dienen oder, noch komplexer, eine teilweise Multifinalität vorliegt.

Zu den rechtlichen Verpflichtungen gehören selbst geschaffene, also vertragliche Pflichten grundsätzlich nicht. Etwas Anderes kann dann zu erwägen sein, wenn die vertraglichen Pflichten ein gesetzlich verpflichtendes Handlungsprogramm ausgestalten. **62**

4. Lebenswichtiges Interesse (Art. 6 Abs. 1 lit. d DS-GVO)

Der Schutz personenbezogener Daten muss hinter dem Schutz lebenswichtiger Interessen zurücktreten. Diese Ansicht wird in Art. 6 Abs. 1 lit. d DS-GVO zum Ausdruck gebracht. Der Begriff der Lebenswichtigkeit ist objektiv zu bestimmen und erfasst insbesondere die körperliche Unversehrtheit und das Leben (vgl. Erwägungsgrund 112 S. 2 zur DS-GVO). Aus Erwägungsgrund 46 S. 2 zur DS-GVO ergibt sich, dass der Erlaubnistatbestand als subsidiär gegenüber den anderen aufgezählten Tatbeständen zu sehen ist. Für das Finanzwesen wird er in individuellen Ausnahmefällen von Relevanz sein, etwa, wenn mit Zahlungstransaktionsdaten eine Gefahr für Leib oder Leben abgeklärt werden kann. **63**

5. Aufgabe im öffentlichen Interesse oder Ausübung hoheitlicher Gewalt (Art. 6 Abs. 1 lit. e DS-GVO)

Die intensive, auf öffentliche Interessen ausgerichtete Regulierung des Finanzsektors, mehr noch seine Inpflichtnahmen etwa bei der Zahlungsverkehrstransparenz, Geldwäscheprävention und fiskalischer Transparenz werfen die Frage auf, ob punktuell auch eine Berufung auf Art. 6 Abs. 1 lit. e DS-GVO in Betracht kommt, der zwei Varianten hat: einerseits die Wahrnehmung einer Aufgabe im öffentlichen Interesse und andererseits die Wahrnehmung einer Aufgabe in Ausübung öffentlicher Gewalt. **64**

Wie Art. 6 Abs. 1 lit. c kann auch lit. e DS-GVO nur in Verbindung mit einer Rechtsgrundlage im Unionsrecht oder nationalen Recht Geltung beanspruchen. Die Erforderlichkeit im Rahmen dieses Erlaubnistatbestandes ist gleichzeitig auch Schnittstelle für die Verhältnismäßigkeit bei einer Einschränkung der Grundrechte der Betroffenen aus Art. 7 und 8 GRCh (→ Art. 6 Rn. 42 ff.). **65**

Das Spektrum der gesetzlich induzierten Verarbeitungsvorgänge in der Finanzindustrie reicht von klassisch wirtschaftsaufsichtlichen über allgemein-generell vorgegebenen Pflichten bis hin zu sehr konkreten Inpflichtnahmen. Typischer Weise wird bei solchen Inpflichtnahmen nach deutschem Verständnis keine Hoheitsaufgabe und schon keine Hoheitsbefugnis übertragen, wie es für die Beleihung charakteristisch ist, vielmehr werden dem Privaten gesetzliche Aufgaben auferlegt, mit denen er öffentliche Interessen verwirklichen oder sichern soll, oder der staatliche Vollzug wird teilweise auslagert. Das reicht jedenfalls für Art. 6 Abs. 1 lit. e Alt. 1 DS-GVO. **66**

Die Begriffe des Art. 6 Abs. 1 lit. e DS-GVO sind unionsrechtlich autonom auszulegen, sodass keine Bindung an Begrifflichkeiten des nationalen Rechts besteht. seine Anwendung nicht steuern können. Unionsrechtlich autonom ist die Erforderlichkeit (→ Art. 6 Rn. 44) auszulegen. Grund hierfür ist vor allem das Ziel der Herstellung eines unionsweiten gleichwertigen Schutzniveaus bzgl. der Verarbeitung personenbezogener Daten (EuGH BeckRS 2008, 71329 Rn. 50, 52, noch bezugnehmend auf die Vorgängerregelung des Art. 7 lit. e Datenschutz-RL). **67**

Art. 6 Abs. 1 lit. e DS-GVO ist somit einschlägig, wenn die jeweilige Vorgabe dem Verantwortlichen den informationellen Eingriff in klar bestimmter Weise auferlegt und dieser dabei unmittelbar öffentliche Interessen wahrnimmt. **68**

Beispiele sind damit die Bereitstellung von Kontendaten beim Abruf durch die Finanzverwaltung und andere konkrete Meldepflichten in Besteuerungsverfahren sowie insbesondere die Erhebung von Abzugssteuern. **69**

Demgegenüber ist Art. 6 Abs 1 lit. e bei den typischen aufsichtlich induzierten Verarbeitungsvorgängen wie denen des Kredit- und Missbrauchsrisikomanagements nicht einschlägig, da hier nicht unmittelbar öffentliche Fremdinteressen wahrgenommen werden. **70**

Nicht ganz eindeutig ist es, ob auch die vielfältigen Verarbeitungsvorgänge der Geldwäscheprävention, soweit sie sich auf reguläre Geschäftsdaten beziehen, von Art. 6 Abs. 1 lit. e DS-GVO gedeckt sind. Dass die Geldwäscheprävention eine Angelegenheit von öffentlichem Interesse ist, legt das Unionsrecht bereits fest. Damit ist Art. 6 Abs. 1 lit. e zumindest einschlägig, wenn die Verarbeitungspflicht konkret bestimmt und determiniert ist, bspw. die Pflicht zu Verdachtsanzeigen. Wird wie in Art. 94 Abs. 1 S. 1 PSD II bzw. § 59 Abs. 1 ZAG hingegen nur eine Befugnis erteilt, aber keine Pflicht begründet, sind die Normen nicht als Vorschriften iSd Art. 6 Abs. 1 lit. **71**

e, Abs. 2, 3 DS-GVO, sondern dahingehend zu verstehen, dass Zahlungsdienste in diesen Fällen ein berechtigtes Interesse iSd Art. 6 Abs. 1 lit. f DS-GVO haben (so auch Weichert BB 2018, 1161 (1164); aA Störing in Casper/Terlau, ZAG, 2. Aufl. 2020, ZAG § 59 Rn. 7).

6. Überwiegendes Interesse des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 lit. f DS-GVO)

72 Art. 6 Abs. 1 lit. f DS-GVO enthält die in der Praxis wichtige zentrale Interessenabwägungsklausel der DS-GVO und regelt damit den Ausgleich zwischen den Datenschutzinteressen des Betroffenen und den Interessen des Verantwortlichen oder des Dritten (Gola/Schulz Art. 6 Rn. 56).

73 Soweit **staatlich** gehandelt wird, ist Art. 6 Abs. 1 lit. f DS-GVO in Deutschland nicht ohne weiteres anwendbar, da hier zusätzlich der verfassungsrechtliche Gesetzesvorbehalt greift. Zur Verhinderung eines Unterlaufens des Vorbehalts des Gesetzes können sich Behörden bei der Erfüllung ihrer Aufgaben gem. Art. 6 Abs. 1 S. 2 DS-GVO nicht auf die Interessenabwägung nach lit. f stützen. Die Interessenabwägung nach lit. f hat somit als einziger der Erlaubnistatbestände aus Art. 6 Abs. 1 DS-GVO einen beschränkten persönlichen Anwendungsbereich (HK-DS-GVO / Reimer Art. 6 Rn. 52). Hieraus ergibt sich die besondere Problematik, wenn die Erfüllung öffentlicher Aufgaben im öffentlichen Interesse privaten Akteuren als Pflichtaufgabe übertragen wird. Hier sind dann unbestimmte Eingriffsermächtigungen möglich, die nicht gesetzlich verantwortet werden, sondern sich erst in einer Interessensabwägung im Einzelfall konkretisieren.

74 Als berechtigte Interessen sind jedenfalls die vernünftigen Erwartungen der betroffenen Person zu sehen, die auf der Beziehung zu dem Verantwortlichen gründen (vgl. Erwägungsgrund 47 S. 1 zur DS-GVO). Das Vorliegen eines berechtigten Interesses auf Seiten des Verarbeitenden ist normativ zu bestimmen; hierzu zählen nicht nur rechtliche, sondern auch wirtschaftliche und ideelle Interessen. In Erwägungsgrund 47 S. 2, 6 und 7 sowie Erwägungsgrund 49 zur DS-GVO werden als berechtigte Interessen bspw. die Betrugsprävention (Erwägungsgrund 47 S. 6), Direktwerbung (Erwägungsgrund 47 S. 7) und auch Maßnahmen zur Verbesserung der Sicherheit von IT-Systemen (Erwägungsgrund 49) aufgezählt.

75 Die Abwägung der beiderseitigen Interessen sowie die Bestimmung dieser selbst hat stets im Einzelfall und unter Berücksichtigung der Intensität der Einschränkung zu erfolgen (Gola/Schulz Art. 6 Rn. 67). Kritisiert worden ist, dass die Formulierung von Art. 6 Abs. 1 lit. f DS-GVO die Beweislast dem Betroffenen überlässt. Hierüber kann nur das jederzeitige Widerspruchsrecht nach Art. 21 Abs. 1 DS-GVO hinweghelfen, wonach sodann der Verantwortliche seine zwingenden schutzwürdigen Interessen nachweisen muss (→ Art. 6 Rn. 45 ff.).

76 Wenn aufsichtlich und gesetzlich induzierte Pflichten nicht schon auf Art. 6 Abs. 1 lit. a, b, d oder e gestützt umgesetzt werden, so ist an lit. f zu denken. Die **allgemeine** Rechtspflicht des Verantwortlichen ist ein Belang von Gewicht, auch wenn sie nicht ohne Weiteres auf der Beziehung zu den Betroffenen gründen. Hier stellen sich aber im Einzelnen noch ungelöste Fragen der Verhältnisse der lit. f zu lit. c und lit. e.

77 Art. 6 Abs. 1 lit. f DS-GVO kommt zudem als Rechtsgrundlage in Betracht, wenn Zahlungsdienste zur Erfüllung ihres Vertrags mit dem Zahlungsdienstenutzer personenbezogene Daten Dritter – sog. „silent party" – verarbeiten (s. EDSA, Leitlinien 6/2020, Rn. 44 ff.; Sander BKR 2019, 66 (72)). Das ist zB der Fall, wenn ein Kontoinformationsdienst zur Erbringung seiner Dienstleistung auf Transaktionsdaten zugreift, die die Kontonummer und den überwiesenen Betrag eines Dritten offenbaren. Dabei hat der Verantwortliche (technisch) sicherzustellen, dass die Gewährleistung der Datenschutzgrundsätze aus Art. 5 Abs. 1 DS-GVO – insbesondere das Zweckbindungs- und das Transparenzgebot sowie das Gebot der Datenminimierung – auch im Hinblick auf den Dritten durch entsprechende Schutzmaßnahmen abgesichert ist. Insbesondere dürfen die personenbezogenen Daten des Dritten, vorbehaltlich ausdrücklicher gesetzlicher Vorgaben der EU oder der Mitgliedstaaten, nicht für andere Zwecke als zur Vertragserfüllung (im Beispiel zur Erbringung des Kontoinformationsdienstes) verarbeitet werden (ausführlich dazu EDSA, Leitlinien 6/2020, Rn. 48 f.). Unklar ist, welche Rechtsgrundlage heranzuziehen ist, wenn die personenbezogenen Daten des Dritten einer der besonderen Kategorien von Daten aus Art. 9 Abs. 1 DS-GVO zuzuordnen sind. Von den Ausnahmetatbeständen aus Art. 9 Abs. 2 DS-GVO wird regelmäßig keiner greifen (so auch Sander BKR 2019, 66 (73)).

78–87 Derzeit nicht belegt.

E. Unternehmerisches und aufsichtlich gebotenes Risikomanagement als Einfallstor von Eingriffen in die informationelle Selbstbestimmung

Kreditinstitute sind zur Sicherung ihrer Risikotragfähigkeit (Kapitalausstattung) und Liquidität verpflichtet, interne Sicherungsmaßnahmen gegen Kreditausfälle zu ergreifen und ein Risikomanagement zu etablieren. Hierzu gehört ua die Überprüfung der Kreditwürdigkeit des Kreditnehmers, um das Ausfallrisiko zu bewerten und hierauf aufbauend Kapitalunterlegung und Liquidität sicherzustellen. Dies setzt notwendig die Beschaffung individueller bzw. personenbezogener Informationen voraus. Die Verpflichtung, die mit Kreditgewährungen verbundenen Risiken zu überwachen, folgt rechtshistorisch bereits aus den hergebrachten kaufmännischen Grundsätzen ordnungsgemäßer Geschäftsführung (Boos/Fischer/Schulte-Mattler/Bock, Kreditwesengesetz, 5. Aufl. 2016, KWG § 18 Rn. 1). **88**

Inzwischen wurden die Risikothemen deutlich erweitert; sie umfassen heute neben den Adressausfall-, Marktpreis- und Liquiditätsrisiken auch die allgemeine Kategorie der **operationellen Risiken,** dessen Definition und Umgrenzung in weiten Teilen den Instituten überlassen wird und das – teilweise aber auch als gesonderte Kategorie erfasst – auch beispielsweise Compliance- und Reputationsrisiken erfassen kann (zu alledem MaRisk BTR 4, Boss/Fischer/Schulte-Mattler/Braun, KWG, § 25a Rn. 351 ff.). Dies wird auch auf Risiken ausgedehnt, rechtswidrige Geschäfte Dritter zu unterstützen (EBA BS 2019 rev. 4 v. 28.4.2020, Rn. 8). Diese Offenheit des Risikobegriffs ermöglicht im Grunde genommen über das allgemeine Einfallstor „Risikomanagement" auch Zweckänderungen bei Verarbeitungsvorgängen, bspw. wenn Kontobewegungen von Kunden nicht nur auf das Adress-/Ausfall-/Kreditrisiko, sondern auch auf ein Compliance-Risiko von Rechtsverstößen des Kunden ausgedehnt würden. **89**

Durch die Finanzkrise 2008 ist das Aufsichtsrecht heute weitgehend europäisiert. Im November 2016 wurde sodann die erste große Revision (sog. „Bankenpaket") der nach der angesprochenen Bankenkrise verabschiedeten Regelungen auf den Weg gebracht, welche nun schließlich am 27.06.2019 in Kraft getreten ist (Wojcik ZBB 2019, 272 (273)). Diese umfasste ua die VO (EU) 2019/876 des Europäischen Parlaments und des Rates vom 20.5.2019 (sog. CRR II) zur Änderung der VO (EU) Nr. 575/2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen (sog. CRR) sowie die RL (EU) 2019/878 des Europäischen Parlaments und des Rates vom 20.5.2019 (sog. CRD V) zur Änderung der RL 2013/36/EU über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen (sog. CRD IV). Die genannten Neuregelungen und weitere Rechtsakte modifizieren und verbessern vor allem den SSM („Single Supervisory Mechanism" – Einheitlicher Aufsichtsmechanismus; VO (EU) Nr. 1024/2013), welcher die Übertragung von Aufsichtsaufgaben auf die EZB regelt, und dienen somit der weiteren europäischen Harmonisierung der Aktivitäten von Kreditinstituten und Wertpapierunternehmen (Gurlit WM 2020, 57 (60); ausf. Wojcik ZBB 2019, 272 (273–276)). Sie sind größtenteils bis zum 28.12.2020 in nationales Recht umzusetzen bzw. sind ab diesem Zeitpunkt anwendbar. **89.1**

Moderne Methoden der Risikosteuerung und -erfassung haben dabei sehr intensive datenschutzrechtliche Implikationen, weil sie stark auf IT-Vorgänge aufsetzen. Kreditinstitute sind heute positivrechtlich, insbesondere nach den §§ 25a, 25h KWG verpflichtet, interne Sicherungsmechanismen zum Auffinden und der Überwachung von Risikofaktoren einzurichten bzw. besonderen Organisationspflichten zu genügen. § 25c KWG legt dies den Geschäftsleitern persönlich auf. §§ 25a, 25c KWG verfolgen mit allgemein organisatorischen Pflichten von Kreditinstituten in Hinblick auf die ordnungsgemäße Geschäftsorganisation breite aufsichtsrechtliche Zielsetzungen (dazu Boos/Fischer/Schulte-Mattler/Braun, KWG, 5. Aufl., § 25a Rn. 30 f.). **90**

Auf diese zunächst im – regulatorisch allerdings vorgegebenen – Eigeninteresse bestehenden Systeme der Datenerhebung und -verarbeitung baut § 25h KWG mit einem weitgehend im Fremdinteresse liegenden Schutzzweck auf (→ Rn. 140 ff.). Hier geht es nicht mehr um den Schutz des Instituts selbst, sondern um die Verhinderung von Geldwäsche, Terrorismusfinanzierung oder sonstigen strafbaren Handlungen. **91**

I. Interne Organisation und Risikomanagement nach §§ 25a und 25c KWG/ MaRisk und BAIT; Datenschutz als Gegenstand bankaufsichtlicher Pflichten

Die von § 25a KWG geforderten internen Organisationspflichten konkretisieren die handelsrechtlichen Grundsätze ordnungsgemäßer Geschäftsführung und namentlich Geschäftsorganisation für den Bereich der Kreditwirtschaft und erheben sie zur aufsichtsrechtlich relevanten Pflicht (Boos/Fischer/Schulte-Mattler, Kreditwesengesetz, 5. Aufl. 2016, § 25a Rn. 15 ff.). Die Vorschrift regelt aufsichtsrechtlich die organisatorischen Maßnahmen, welche die Geschäftsführung eines **92**

Kreditinstitutes ergreifen muss. Die gesetzliche Regelung wird intensiv durch weitere Vorschriften wie die **Mindestanforderungen an das Risikomanagement (MaRisk)** und die **bankaufsichtlichen Anforderungen an die IT (BAIT)** der BaFin konkretisierend ergänzt.

93 Inhaltlich setzt inzwischen § 25a KWG größtenteils **europäische Vorgaben** um (dazu Boos/Fischer/Schulte-Mattler/Braun, Kreditwesengesetz, 5. Aufl. 2016, KWG § 25a Rn. 3 ff.). Zur ordnungsgemäßen Geschäftsorganisation gehört bei Finanzdienstleistern zwingend ein Hinweisgebersystem (Whistleblower-System), § 25a Abs. 1 S. 6 Nr. 3 KWG (dazu allg. Artikel 29-Datenschutzgruppe (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_de.pdf. und DüK http://www.datenschutz.hessen.de/download.php?download_ID=246), zur Auslagerung Greve ZD 2014, 336).

94 Auch die in der Neufassung der **MaRisk** von Oktober 2017 enthaltenen Regelungen sind ungeachtet der schon hohen gesetzlichen Regelungsdichte **norminterpretierenden Verwaltungsvorschriften,** die die BaFin zur genaueren Ausgestaltung des Risikomanagements bei Kreditinstituten in Form eines Rundschreibens erlassen hat und die ihre vormaligen Rundschreiben in diesem Bereich in gewissem Umfang ablösen (vgl. MaRisk idF v. 27.10.2017, Vorbem. Rn. 1; dazu auch Gurlit WM 2020, 105 (109)). Der allgemeine Teil der MaRisk (Modul AT) enthält Vorschriften zur grundsätzlichen Ausgestaltung des Risikomanagements; der besondere Teil (Modul BT) legt spezifische Anforderungen für bestimmte Organisationsbereiche fest.

95 Aufgrund der wachsenden Bedeutung von IT-Services folgte kurz darauf die **BAIT,** welche 2018 erneut ergänzt wurde und seither einen flexiblen und praxisnahen Rahmen für die technisch-organisatorische Ausstattung der Institute – insbesondere für das Management der IT-Ressourcen und für das IT-Risikomanagement – bietet. Die Regelungen der MaRisk bleiben daneben unberührt und werden durch die BAIT lediglich weiter konkretisiert (vgl. Rundschreiben 10/2017 (BA) idF vom 14.9.2018 Rn. 1). Beide Rundschreiben konkretisieren demnach im Ergebnis sowohl § 25a KWG als auch § 25b KWG im Hinblick auf das (IT-)Risikomanagement und die Auslagerung von Prozessen.

96 Datenschutzrechtlich relevant ist sowohl das Modul AT als auch das Modul BT der MaRisk. So müssen Institute nach BTO 1.2.1 MaRisk vor der Vergabe von Krediten etwa die Kreditwürdigkeit des Kreditnehmers überprüfen. Dies setzt die Erhebung, Verwendung und Verarbeitung personenbezogener Daten notwendig voraus.

97 Das wiederum aktiviert den datenschutzrechtlichen Ermächtigungsvorbehalt des Art. 6 Abs. 1 DS-GVO, wonach die Verwendung personenbezogener Daten nur zulässig ist, wenn einer der enumerativ aufgezählten Rechtfertigungsgründe erfüllt ist. In Betracht kommt im Falle der MaRisk und der BAIT vor allem Art. 6 Abs. 1 lit. c DS-GVO, die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung und Art. 6 Abs. 1 lit. f DS-GVO.

98 Zwar sind als Rechtsgrundlagen lt. Erwägungsgrund 41 zur DS-GVO nicht nur von einem Parlament angenommene Gesetzgebungsakte ausreichend, sondern auch Rechtsverordnungen wie bspw. Satzungen. Dennoch kommen Verwaltungsvorschriften aufgrund ihrer fehlenden unmittelbaren Rechtswirkung als Rechtsgrundlage nicht in Betracht (BeckOK Datenschutzrecht/Albers/Veit Art. 6 Rn. 58). Sowohl die MaRisk als auch die BAIT selbst stellen demnach als Verwaltungsvorschriften der BaFin keine rechtliche Verpflichtung iSv Art. 6 Abs. 1 lit. c DS-GVO dar und bieten somit keine eigenständige datenschutzrechtliche Ermächtigungsgrundlage. Trotzdem erscheint die Datenverarbeitung vorliegend rechtlich unproblematisch: Die Vorschriften der MaRisk und der BAIT sind **norminterpretierende Konkretisierungen der in § 25a KWG** gesetzlich festgelegten Grundsätze ordnungsgemäßer Geschäftsführung (vgl. MaRisk idF v. 27.10.2017, Vorbem. Rn. 1 und BAIT idF v. 14.09.2018 Rn. 1).

99 Umgekehrt sind die datenschutzrechtlichen Pflichten auch als **einzuhaltende Rechtsvorschriften,** die Gegenstand der Organisationspflichten, namentlich des Risikomanagements sein müssen, im Aufsichtsrecht integriert. Die **Einhaltung des Datenschutzrechts** ist somit, soweit Thema der Geschäftsorganisation, auch **bankaufsichtlich** relevant. Aufsichtlich ist eine Durchsetzung nach § 45b KWG möglich; im Zusammenhang mit Auslagerungen auch nach § 25b KWG. Für die Einhaltung von Einzelanforderungen des Datenschutzrechts bleibt es dennoch bei einer ausschließlichen Zuständigkeit der datenschutzrechtlichen Aufsichtsbehörden; im Hinblick auf das Managementsystem und Organisationspflichten besteht aber – auch – eine Zuständigkeit der Finanzdienstleistungsaufsicht durch die BaFin.

II. § 25b Abs. 1 KWG: Auslagerung von Geschäftsprozessen

100 Die häufig, beispielsweise als **Auftragsverarbeitung,** auch datenschutzrechtlich relevanten Auslagerungsprozesse (DSB Bay TB 2011/2012, 41 ff.) haben aufsichtsrechtlich eine eigenständige,

zusätzliche Regelung erfahren. § 25b KWG enthält Anforderungen an die Auslagerung von Aktivitäten und Prozessen eines **Kredit- bzw. Finanzdienstleistungsinstituts** auf ein anderes Unternehmen. Sie sind als Bestandteil der allgemeinen Anforderungen an eine ordnungsgemäße Geschäftsorganisation aus § 25a Abs. 1 KWG ableitbar (Boos/Fischer/Schulte-Mattler/Braun, Kreditwesengesetz, 5. Aufl. 2016, KWG § 25b Rn. 52). Für **Zahlungsinstitute** gilt die parallele Regelung in § 26 Abs. 2 ZAG (→ Rn. 137 f.). Ähnliche Vorschriften enthält das Kapitalmarktrecht für Kapitalmarktintermediäre.

Eine erste umfassende Klärung wesentlicher bankaufsichtlicher Fragen hierzu enthielt das **101**
Rundschreiben des Bundesaufsichtsamtes für das Kreditwesen 11/2001 Auslagerung von Bereichen auf ein anderes Unternehmen gem. § 25a Abs. 2 KWG (vgl. BAKred, Rundschreiben 11/2001 v. 6.12.2001 – I 3–272A – 2/98). In den folgenden Rundschreiben wurden die Anforderungen deutlich gestrafft und die Verantwortlichkeit der Institute für die Ordnungsmäßigkeit der Auslagerung stärker betont (vgl. zuletzt BaFin, Rundschreiben 10/2017 (MaRisk 2017), AT 9). Mit der überarbeiteten MaRisk von 2017 und der neuen BAIT, ebenfalls aus 2017, lässt sich eine zunehmende Regulierung bzgl. der IT der Institute feststellen (Lensdorf CR 2017, 753 (755)). Dem korrespondiert eine entsprechende Aufsichtstätigkeit der BaFin.

Eine **Auslagerung** iSd § 25b Abs. 1 KWG liegt vor, wenn ein anderes Unternehmen mit der **102**
Wahrnehmung solcher Aktivitäten und Prozesse im Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen beauftragt wird, die ansonsten vom Institut selbst erbracht würden (MaRisk 2017 AT 9 Rn. 1). Da häufig auch personenbezogene Daten betroffen sind, bedarf es für die informationellen Vorgänge auch einer datenschutzrechtlichen Rechtfertigung. Typisch war unter dem BDSG aF die Auftrags(daten)verarbeitung; unter der DS-GVO ist auch an die **gemeinsame Kontroll**e und die **selbständige Übermittlung** zu denken.

Unter Berücksichtigung der Zielsetzung der Gesetzesvorschrift (Sicherstellung der aufsichts- **103**
rechtlichen Kontroll- und Prüfungsrechte) gilt als anderes Unternehmen jede andere Stelle, Einheit oder Person, die in Bezug auf die ausgelagerte Funktion oder Tätigkeit nicht dem auslagernden Institut zuzurechnen und organisatorisch von ihm abgegrenzt ist, ohne dass es auf die Kaufmannseigenschaft, Rechtsfähigkeit oder Rechtsform ankommt (Boos/Fischer/Schulte-Mattler/Wolfgarten, Kreditwesengesetz, 5. Aufl. 2016, KWG § 25b Rn. 21 mit Verweis auf die Definition im Rundschreiben 11/2001). Ein anderes Unternehmen iSd § 25b Abs. 1 KWG soll jedenfalls dann vorliegen, wenn die andere Stelle eine eigene Rechtspersönlichkeit besitzt (Boos/Fischer/Schulte-Mattler/Wolfgarten, Kreditwesengesetz, 5. Aufl. 2016, KWG § 25b Rn. 21).

Nur eine **wesentliche Auslagerung** von Aktivitäten und Prozessen unterliegt den besonderen **104**
Anforderungen des § 25b KWG. **Nicht erfasst** werden der **einmalige oder gelegentliche Fremdbezug von Gütern und Dienstleistungen** sowie der Bezug von Leistungen, die **typischerweise nicht vom Institut** selbst erbracht werden können (MaRisk 2017 AT 9 Rn. 1). Schwierige Abgrenzungsfragen stellen sich mitunter bei IT-Beschaffungsakten (Lensdorf CR 2017, 753 (755 f.)), der isolierte Bezug von Software fällt allerdings im Regelfall unter den „sonstigen Fremdbezug" (MaRisk 2017 AT 9 Rn. 1). Nicht-wesentliche Auslagerungen unterfallen grundsätzlich den allgemeinen Anforderungen an eine ordnungsgemäße Geschäftsführung gem. § 25a Abs. 1 KWG, welche durch die BAIT jedoch erheblich konkretisiert wurden und sich regulatorisch gesehen den Anforderungen für wesentliche Auslagerungen nach MaRisk AT 9 stark annähern (Lensdorf CR 2017, 753 (761)). Während die ursprüngliche Regelung die Wesentlichkeit einer Auslagerung noch abstrakt bestimmte (BAKred, Rundschreiben 11/2001 v. 6.12.2001 – I 3–272A – 2/98), müssen die Institute nach den nunmehr geltenden Bestimmungen auf Grundlage einer **eigenen Risikoanalyse selbst festlegen,** welche Auslagerungen von Aktivitäten und Prozessen unter Risikogesichtspunkten wesentlich sind (MaRisk 2017 AT 9 Rn. 2). Die Durchführung einer solchen Risikoanalyse ist sowohl regelmäßig als auch anlassbezogen erforderlich, wobei die Intensität der Analyse von Art, Umfang, Komplexität und Risikogehalt der ausgelagerten Aktivitäten und Prozesse abhängt (MaRisk 2017 AT 9 Rn. 2). Die in dem inzwischen aufgehobenen Rundschreiben 11/2001 aufgeführten Beispiele unwesentlicher Bereiche können zur Norminterpretation weiter herangezogen werden (so etwa Boos/Fischer/Schulte-Mattler/Wolfgarten, Kreditwesengesetz, 5. Aufl. 2016, KWG § 25b Rn. 21 bzgl. des Begriffs des anderen Unternehmens). Im Rahmen gruppeninterner Auslagerungen können wirksame Vorkehrungen wie etwa ein einheitliches und umfassendes Risikomanagement auf Gruppenebene oder Durchgriffsrechte, bei der Erstellung und Anpassung der Risikoanalyse Risiko mindernd berücksichtigt werden (MaRisk 2017 AT 9 Rn. 2).

Als **auslagerungsfähig** gilt eine Auslagerung, sofern sie **aufsichtsrechtlich zulässig** ist. Auslage- **105**
rungsfähig sind dabei grundsätzlich alle Aktivitäten und Prozesse, solange durch die Auslagerung

nicht die Ordnungsmäßigkeit der Geschäftsorganisation nach § 25b Abs. 1 KWG beeinträchtigt wird (MaRisk 2017 AT 9 Rn. 4). Letztlich entscheidend ist damit die Frage, ob ein angemessenes und wirksames Risikomanagement trotz Auslagerung erhalten bleibt (Boos/Fischer/Schulte-Mattler/Wolfgarten, Kreditwesengesetz, 5. Aufl. 2016, KWG § 25b Rn. 33). Die Auslagerung darf daher nicht zu einer Delegation der Verantwortung der Geschäftsleitung an das Auslagerungsunternehmen führen; die Leitungsaufgaben der Geschäftsleitung, insbesondere die Unternehmensplanung, -koordination und -kontrolle sowie die Besetzung der Führungskräfte, sind dementsprechend nicht auslagerbar (MaRisk 2017 AT 9 Rn. 4). Ausnahmen dieses Auslagerungsverbots werden in MaRisk 2017 AT 9 Rn. 5 statuiert. Für den Fall einer (unerwarteten) Beendigung der Auslagerungsvereinbarung muss das Institut bereits zu Beginn der Auslagerung Vorkehrungen zu treffen, um die Kontinuität und Qualität der ausgelagerten Aktivitäten und Prozesse auch nach dem Beendigungszeitpunkt zu gewährleisten (MaRisk 2017 AT 9 Rn. 6). Der Umfang dieser präventiven Maßnahmen unterliegt dem Proportionalitätsgrundsatz (Boos/Fischer/Schulte-Mattler/Wolfgarten, Kreditwesengesetz, 5. Aufl. 2016, KWG § 25b Rn. 57).

106 Seit 2017 ist das Institut verpflichtet, jeweils abhängig von Art, Umfang und Komplexität der Auslagerungsaktivitäten, ein zentrales **Auslagerungsmanagement** einzurichten, welches jedenfalls jährlich einen Bericht über die wesentlichen Auslagerungen zu erstellen hat. Hierbei müssen Risikoabwägungen getroffen und dementsprechend ggf. die Ergreifung von risikomindernden Maßnahmen empfohlen werden (MaRisk 2017 AT 9 Rn. 12 f.).

107 Nach **§ 25b Abs. 3 S. 3 KWG** bedarf die **Auslagerung eines schriftlichen Auslagerungsvertrages.** Dieser muss die zur Wahrung der in Abs. 1 genannten Anforderungen erforderlichen Rechte des Instituts, sowie die korrespondierenden Pflichten des Auslagerungsunternehmens enthalten. Soweit – wie meist – auch personenbezogene Daten betroffen sind, enthält der **Auslagerungsvertra**g dann auch die datenschutzrechtlich erforderlichen Inhalte, bspw. die **Auftragsverarbeitung** oder gemeinsame Kontrolle.

108 Die MaRisk 2017 AT 9 Rn. 7 konkretisieren diese Anforderung durch eine **Auflistung der notwendigen Vertragsinhalte,** welche manche Parallelen zu Art. 28 Abs. 3 DS-GVO aufweisen. Auch die Voraussetzungen und, wenn möglich, Zustimmungsvorbehalte für Weiterverlagerungen sind im Auslagerungsvertrag zu regeln; insbesondere ist für den Fall einer Weiterverlagerung eine Informationspflicht mit in die schriftliche Vereinbarung aufzunehmen (MaRisk 2017 AT 9 Rn. 8). Werden durch eine wesentliche Auslagerung Prüfungsrechte und Kontrollmöglichkeiten der BaFin beeinträchtigt, so kann diese auf Grundlage der in § 25b Abs. 4 S. 1 KWG enthaltenen und nur durch die Privatautonomie begrenzte (Boos/Fischer/Schulte-Mattler/Wolfgarten, Kreditwesengesetz, 5. Aufl. 2016, KWG § 25b Rn. 96) **Anordnungsbefugnis** reagieren. Zur Sicherstellung der Prüfungs- und Kontrollrechte kann ein Institut dabei etwa auch zu einer Vertragsänderung angehalten werden. Als letztes Mittel kann auch die Übertragung auf einen geeigneten Dienstleister bzw. die Wiedereingliederung des betroffenen Bereichs angeordnet werden (Boos/Fischer/Schulte-Mattler/Wolfgarten, Kreditwesengesetz, 5. Aufl. 2016, KWG § 25b Rn. 95).

109 Auf europäischer Ebene gelten für die Auslagerung von (IT-)Geschäftsprozessen seit September 2019 die EBA-Leitlinien über die Auslagerung von Geschäftsfunktionen als Reaktion auf das ebenso populäre wie risikoreiche Outsourcing von IT-Funktionen unter Inanspruchnahme von Cloud-Anbietern (EBA Guidelines on outsourcing arrangements, 14 f.; Gurlit WM 2020, 57 (61)). Die BaFin hat die Leitlinien zum 1.7.2019 in ihre Verwaltungspraxis übernommen.

III. Offenlegungspflichten nach § 18 S. 1 KWG

110 Die in § 18 S. 1 KWG festgelegte Verpflichtung von Kreditinstituten, sich die **wirtschaftlichen Verhältnisse** des Kreditnehmers vor der Kreditgewährung von diesem **offen legen** zu lassen, hat ihren Ursprung in der Weltwirtschaftskrise der späten Zwanziger und Dreißiger Jahre des letzten Jahrhunderts. Seinerzeit wurde offenkundig, dass Umfang und Intensität der Bonitätsprüfung ein bestimmender Wettbewerbsfaktor bei der Vergabe von Krediten war: Nicht nur erschloss sich bei einer geringeren Prüfungstiefe und -intensität der Kreditwürdigkeit ein größerer Kreis von Kunden, die bei einer strengen Prüfung möglicherweise keinen Kredit erhalten hätten.

111 Dieser Logik folgt im Grundsatz auch der heutige § 18 KWG (s. Konesny, Gesetze über das Kreditwesen, 28. Aufl. 2014, KWG § 18). Auch der § 18 KWG fußt auf den kaufmännischen Grundsätzen ordnungsgemäßer Geschäftsführung und soll eine risikobewusste Kreditvergabe sicherstellen (Boos/Fischer/Schulte-Mattler/Bock, Kreditwesengesetz, 5. Aufl. 2016, KWG § 18 Rn. 1).

112 Die aus § 18 S. 1 KWG folgende Pflicht zur Erhebung individueller wirtschaftlicher Daten ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung, soweit natürliche Personen betroffen sind. Damit dürfte auch die gesetzliche Regelung selbst Eingriffscharakter haben.