B 57464

BKR Zeitschrift für Bank- und Kapitalmarktrecht

bkr.beck.de

C.H.BECK

BKR Bank- und Kapitalmarktrecht

5/2018 18. Jahrgang
Seite 177 bis 220, 22. Mai 2018

K150201805

BKR

Zeitschrift für Bank- und Kapitalmarktrecht

5/2018 Seite 177–220, 22. Mai 2018

Redaktion: Poppelsdorfer Allee 64, 53115 Bonn · bkr.beck.de

Florian Frisse, LL. M., Ramón Glaßl, LL. M. Anne Baranowski, LL. M., Lisa Duwald[1]

Unternehmenssicherheit bei Banken – IT-Sicherheit, Know-how Schutz, Datensicherheit und Datenschutz

A. Einleitung

„*Cyberangriffe sind nicht nur Stoff für Science-Fiction-Filme. Sie sind Alltag – sehr ernst zu nehmender Alltag.*" Mit diesen treffenden Worten machte Felix Hufeld, Präsident der Bundeanstalt für Finanzdienstleistungsaufsicht („BaFin") in seiner Rede[2] im Rahmen der BaFin-Informationsveranstaltung „IT-Aufsicht bei Banken" im März 2017 auf die Brisanz des Themas IT-Sicherheit aufmerksam. Digitale Bedrohungen, sei es durch Krisen oder durch externe Angriffe auf Banken, an denen es in der jüngsten Vergangenheit gleichermaßen nicht mangelte, stellen Banken und Finanzdienstleister sowie Gesetzgeber und Aufsicht vor neue Herausforderungen. Dies insbesondere, da die Bedeutung der Informations- und Kommunikationstechnik für Kreditinstitute in den letzten Jahren weiter zugenommen hat.

Hinzukommen Änderungen bzgl. des Schutzes von Geschäftsgeheimnissen auf EU-Ebene, die der nationale Gesetzgeber bis zum 5.7.2018 umzusetzen hat. Wesentliche Änderung ist, dass ein Geschäftsgeheimnis nunmehr nur noch dann geschützt ist, wenn es Gegenstand von konkreten und angemessenen Schutzmaßnahmen ist. Die neue EU-Richtlinie nimmt also auch den Geheimnisträger, die Bank, in die Pflicht.

Banken stehen auch vor der Herausforderung, ihre Verarbeitung von personenbezogenen (Kunden-) Daten den Anforderungen der europäischen Datenschutz-Grundverordnung entsprechend zu gestalten. Die Datenschutz-Grundverordnung wird ab dem 25.5.2018 Anwendung finden und stellt das Datenschutzrecht auf eine neue Grundlage. Die datenschutzrechtlichen Grundsätze bleiben im Kern zwar erhalten, jedoch bringt die Verordnung eine Reihe von Veränderungen mit sich. Wie bisher gehört zur Datenschutz-Compliance auch die Sicherheit der Datenverarbeitung, durch die neue Verordnung werden jedoch die zu treffenden Maßnahmen konkretisiert.

Dieser Beitrag gibt eine Übersicht über diese (regulatorischen und rechtlichen) Themen IT-Sicherheit, Know-how Schutz, Datensicherheit und Datenschutz, die Banken (auch) im Jahr 2018 beschäftigen werden.

B. IT-Sicherheit

I. Lage der IT-Sicherheit

„*Der größte Unique Selling Point der Kreditwirtschaft besteht im Vertrauen der Kunden.*"[3] – mit diesem Satz bringt der Bundesverband deutscher Banken e. V. treffend zum Ausdruck, was bei der Vermarktung von Produkten im Kreditwesen von wesentlicher Bedeutung ist: Das Vertrauen der Kunden. Doch dieses Vertrauen der Kunden in die Kreditwirtschaft will stets gepflegt und immer wieder neu aufgebaut werden.

Das Bundesamt für Sicherheit in der Informationstechnik („BSI") sieht in seinem jährlichen Bericht zwar keine steigenden Tendenzen digitaler Bedrohungen mehr (anders als noch in den Jahren zuvor), allerdings stagnieren die Werte auf hohem Niveau[4]. So zählen zu den größten digitalen Bedrohungen neben Spam und Phishing insbesondere Denial of Service Angriffe, Drive-By Exploits, Schadsoftware und Social Engineering sowie gezielte Hackingangriffe. Die

1) *Florian Frisse* ist Rechtsanwalt und Partner in der Anwaltssozietät Schalast in Frankfurt a. M., *Ramón Glaßl*, *Anne Baranowski* und *Lisa Duwald* sind Rechtsanwälte/Rechtsanwältinnen in der Anwaltssozietät Schalast in Frankfurt a. M.

2) Rede von *Felix Hufeld* bei der BaFin-Informationsveranstaltung „IT-Aufsicht bei Banken" am 16.3.2017 in Bonn, veröffentlicht am 16.3.2017, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Reden/re_170316_IT_Aufsicht_p.html, zuletzt abgerufen am 12.2.2018.

3) Branchenspezifischer Sicherheitsstandard – Mindeststandard der privaten Banken zum IT-Sicherheitsgesetz, herausgegeben vom Bundesverband deutscher Banken, Seite 5.

4) Die Lage der IT-Sicherheit in Deutschland 2017, herausgegeben durch das Bundesamt für Sicherheit in der Informationstechnik, Seite 75.

größte Sicherheitslücke stellen hierbei i. d. R. die eigenen Mitarbeiter dar. Sei es durch eine private Internetnutzung am Arbeitsplatz oder eine Bring Your Own Device Policy des Arbeitgebers – die Einfallstore für Eindringlinge sind hier am größten.

Ungeachtet gezielter oder ungezielter externer Angriffe bestehen jedoch auch intern Sicherheitslücken, die den Geschäftsbetrieb einer Bank nachhaltig beeinflussen können. Bis heute werden weltweit bei ca. 95 Prozent aller Geldautomaten als Betriebssystem immer noch Windows XP eingesetzt[5], obwohl die Bundesregierung die Kreditwirtschaft bereits im Jahre 2014 zum Umstieg auf neuere Betriebssysteme aufgefordert hatte. Neben praktischen Fragen wie Zugangsbeschränkungen, einem abgeschlossenen Serverraum sowie einem gesperrten USB Port am Arbeitsrechner, stellen auch (alte) Auslagerungsverträge, unabhängig davon ob diese wesentlich oder unwesentlich sind, ebenso eine potentielle Sicherheitslücke dar, wie die individuelle Datenverarbeitung, die sich auf die Geschäfte von Banken nachteilig auswirken kann: Während Mitarbeiter A mit einem von ihm entworfenen Excel-Sheet zum Ergebnis kommt, dass eine bestimmte Investition lohnenswert ist, kann Mitarbeiter B mit einem von diesem entworfenen Excel-Sheet zum Ergebnis kommen, dass dieselbe Investition sich nicht lohnt.

II. Rechtsgrundlagen: KWG, MaRisk, BAIT, PSD2, IT Sicherheitsgesetz

Hand in Hand mit den genannten Sicherheitsrisiken ergaben Prüfungen der Bundesbank, dass Kreditinstitute tatsächlich Defizite in der IT-Strategie und IT-Governance, in der Informationssicherheit, im Berechtigungsmanagement und der Anwendungsentwicklung aufweisen[6]. Vor diesem Hintergrund und zwecks besserer Abbildung notwendiger und geforderter Standards hat die BaFin der IT-Sicherheit ein eigenes Rundschreiben gewidmet, die Bankaufsichtlichen Anforderungen an die IT („BAIT")[7], welche ab sofort zu berücksichtigen sind. Die Anforderungen der BAIT tragen dem Umstand Rechnung, dass Kreditinstitute bzw. Finanzdienstleistungsinstitute zunehmend Prozesse, die nicht zum Kerngeschäft gehören, an Dienstleister beziehungsweise FinTechs auslagern und somit der umfassende Blick auf die Informationssicherheit verloren gehen könnte.

Ausgehend von § 25a Abs. 1, Abs. 3 und § 25b Kreditwesengesetz („KWG") geben die Mindestanforderungen an das Risikomanagement („MaRisk")[8], zukünftig die BAIT sowie das IT-Sicherheitsgesetz den regulatorischen Standard vor. Die MaRisk in ihrer Neufassung[9] wurden zuletzt von der BaFin am 27.10.2017 veröffentlicht, enthaltene Neuerungen sind bis zum 31.10.2018 umzusetzen, während Klarstellungen ab sofort zu beachten sind.

Die MaRisk und die BAIT legen auf Grundlage der Bestimmungen des KWG einen flexiblen und praxisnahen Rahmen fest, wobei die BAIT Vorgaben des KWG präzisieren und relevante Passagen der MaRisk konkretisieren. Hierbei folgen die BAIT dem Aufbau der MaRisk und verweisen auf die entsprechenden Teilziffern. Allerdings befreien die BAIT die Institute nicht von den Vorgaben der MaRisk. Die dort getroffenen Vorgaben und die Verpflichtung des Instituts, gängige Standards (z. B. der Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik und der internationale Sicherheitsstandard ISO/IEC 27OOX) einzuhalten, bleiben unberührt.

Die prinzipienorientierten Anforderungen der MaRisk und der BAIT unterliegen dem Proportionalitätsprinzip, d. h. je nach Größe, Komplexität, einer besonderen Risikoexponierung oder Internationalität der Geschäftsaktivitäten können über die expliziten Vorgaben hinaus weitere Vorkehrungen i. S. eines angemessenen und wirksamen Risikomanagements erforderlich sein – die Vorgaben sind in jedem Fall nicht abschließend zu verstehen.

Primäres Anliegen der BAIT ist es, die Erwartungshaltung und gängige Praxis der Aufsicht transparenter zu machen und zudem das IT-Risikobewusstsein im Institut selbst und gegenüber den Auslagerungsunternehmen zu stärken.

Auf europäischer Ebene gibt das Single Supervisory Mechanism (SSM) Handbuch der Europäischen Zentralbank[10] („EZB") den Leitfaden für die Prüfung bedeutender Institute vor. Vor dem Hintergrund des anhaltenden Wachstums der FinTech-Szene dürfte die Position der EZB zur Aufsicht dieser Startups von besonderem Interesse sein: In ihrem im September 2017 veröffentlichten Handbuch zur Bewertung von FinTech-Instituten im Lizensierungsverfahren[11] äußerte die EZB, dass für FinTech-Unternehmen die gleichen Anforderungen wie für alle Institute gelten sollen. Einer regulatorischen „Sandbox", in der Startups sich unter weniger strengen Vorgaben ausprobieren können, erteilte die EZB damit eine klare Absage. Europäische aufsichtsrechtliche Vorgaben zu den Themen IT, Informationssicherheit und Dienstleistungsbezug werden derzeit entworfen. So hat die Europäische Bankaufsichtsbehörde („EBA") speziell zur IT-Aufsicht im Mai 2017 Richtlinien zur Bewertung von Informations- und Kommunikationstechnologien[12] herausgegeben, die Konsultationsphase zu den Empfehlungen der EBA zum Outsourcing an Cloud Service Provider[13] ist abgeschlossen, die Veröffentlichung der finalen Fassung steht bevor.

Daneben stellt die zweite Zahlungsdienste-Richtlinie („PSD2") Anforderungen an starke Kundenauthentifizierung und sichere Kommunikation auf. Das deutsche Umsetzungsgesetz hierzu trat am 13.1.2018 in Kraft. Hierzu erarbeitet die EBA mit Blick auf die Themen IT-Sicherheit und IT-Technologie Regulatory Standards[14] und Guidelines[15].

---

5) https://www.heise.de/newsticker/meldung/95-Prozent-aller-Geldautomaten-laufen-mit-Windows-XP-2088583.html, zuletzt abgerufen am 12.2.2018.

6) So *Felix Hufeld* in seiner Rede bei der BaFin-Informationsveranstaltung „IT-Aufsicht bei Banken" am 16.3.2017 in Bonn, veröffentlicht am 16.3.2017, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Reden/re_170316_IT_Aufsicht_p.html, zuletzt abgerufen am 12.2.2018.

7) Rundschreiben 10/2017 (BA) vom 3.11.2017, veröffentlicht von der BaFin am 3.11.2017, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=6, zuletzt abgerufen am 12.2.2018.

8) Rundschreiben 09/2017 (BA) vom 27.10.2017, veröffentlicht von der BaFin am 27.10.2017, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs1709_marisk_pdf_ba.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 12.2.2018.

9) Die Neufassung des Rundschreibens 09/2017 (BA) vom 27.10.2017 als Delta-View-Version, veröffentlicht von der BaFin am 27.10.2017.

10) Guide to Banking Supervision, veröffentlicht von der EZB im November 2014, https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssmguidebankingsupervision201411.en.pdf, zuletzt abgerufen am 12.2.2018.

11) Guide to Assessments of Fintech Credit Institution Licence Applications,veröffentlicht von der EZB im September 2017.

12) Final Report: Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) (EBA/GL/2017/05), veröffentlicht von der EBA am 11.5.2017.

13) Consultation Paper: Draft Recommendations on Outsourcing to Cloud Service Providers under Article 16 of Regulation (EU) No 1093/2010 EBA/CP/2017/06), veröffentlicht von der EBA am 15.5.2017.

14) Final Report: Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2) (EBA/RTS/2017/02), veröffentlicht von der EBA am 23.2.2017.

15) Consultation Paper: Draft Guidelines on the Security Measures for Operational and Security Risks of Payment Services under PSD2 (EBA/CP/2017/04), veröffentlicht von der EBA am 5.5.2017, und Final Report: Guidelines on Major Incident Reporting under Directive (EU) 2015/2366 (PSD2) (EBA/GL/2017/10), veröffentlicht von der EBA am 27.7.2017.

Eine weitere Rechtsquelle für den Schutz von Informationstechnologie stellt das IT-Sicherheitsgesetz dar. Das IT-Sicherheitsgesetz ist kein eigenständiges Gesetz, sondern änderte Vorschriften in zahlreichen anderen Gesetzen, u. a. dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik („BSIG"). Nach § 8a Abs. 1 Satz 1 BSIG müssen Betreiber kritischer Infrastrukturen angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen. Hierbei soll der Stand der Technik einzuhalten sein, § 8a Abs. 1 Satz 2 BSIG. Wer Betreiber einer kritischen Infrastruktur ist, wird wiederum durch eine separate Rechtsverordnung bestimmt, wobei Infrastrukturen aus den Sektoren Energie, Finanz- und Versicherungswesen, Ernährung, Wasser, Gesundheit, Transport und Verkehr sowie Informationstechnik und Telekommunikation als potentiell kritisch angesehen werden.

III. Vorgaben

Aufbauend auf § 25a Abs. 1, Abs. 3 und § 25b KWG legen die MaRisk und die BAIT fest, dass die Geschäftsleitung eine mit der Geschäftsstrategie konsistente IT-Strategie mit in den BAIT festgelegten Mindestinhalten festlegen muss. Diese muss regelmäßig überwacht und angepasst werden. Daneben ist die Geschäftsleitung verantwortlich für die Umsetzung der Regelungen zur IT-Governance, d. h. die Struktur zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der dazugehörigen IT-Prozesse auf Basis der IT-Strategie. Hand in Hand mit den Regelungen der MaRisk ist insbesondere das Informationsrisikomanagement, das Informationssicherheitsmanagement, der IT-Betrieb sowie die Anwendungsentwicklung quantitativ und qualitativ angemessen mit Personal auszustatten und Interessenkonflikte und unvereinbare Tätigkeiten innerhalb der IT-Aufbau- und IT-Ablauforganisation zu vermeiden. Im Bereich des Informationsrisikomanagements ist der Schutzbedarf zu ermitteln und eine Risikoanalyse auf Grundlage eines Vergleichs von den ermittelten Referenzmaßnahmen mit den tatsächlich wirksam umgesetzten Maßnahmen durchzuführen. Verbundene Risiken sind nach neugefasster MaRisk ausdrücklich beim Bezug von Software angemessen zu bewerten. Auf Basis einer im Rahmen des Sicherheitsmanagements zu schaffenden Informationssicherheitsrichtlinie sind näher konkretisierende und den Stand der Technik wiedergebende Informationssicherheitskonzepte und -prozesse zu bestimmen. Zentrales Element der Regelungen ist die Stelle des Informationssicherheitsbeauftragten, welche organisatorisch und prozessual unabhängig auszugestalten ist und nur unter sehr engen Voraussetzungen ausgelagert werden kann. Daneben werden Vorgaben insbesondere hinsichtlich des Benutzerberechtigungsmanagements, der IT-Projekte und des IT-Betriebs, was die Verwaltung und Aktualisierung der verwendeten IT-Systeme und den Umgang mit Störungen einschließt, sowie der Auslagerung von IT-Dienstleistungen getroffen. Insgesamt wurden durch die Vorgaben der neugefassten MaRisk die Anforderungen an die Auslagerung verschärft, insbesondere durch die verpflichtende Einführung einer zentralen Auslagerungsfunktion sowie von Eskalations- und Exit-Konzepten. Für systemrelevante Kreditinstitute wurde durch die novellierte MaRisk zudem ein neues (und umfassendes) System für Datenmanagement, Datenqualität und Aggregation von Risikodaten eingeführt.

Auch nach dem BSIG müssen Banken grds. bestimmte Sicherheitsvorkehrungen treffen. Wie bereits oben unter Ziffer B.III. dargelegt, müssen Betreiber kritischer Infrastrukturen angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse einrichten. Während bei technischen Maßnahmen ausdrücklich der Stand der Technik als Maßstab herangezogen wird, § 8a Abs. 1 Satz 2 BSIG, wird man bei organisatorischen Maßnahmen darauf abstellen müssen, ob diese „*State of the Art*" sind oder nicht.

Am 30.6.2017 wurde die Erste Verordnung zur Änderung der BSI-Kritisverordnung veröffentlicht. Mit dieser Änderungsverordnung wurden nicht nur die noch ausstehenden Sektoren Kritischer Infrastrukturen i. S. d. IT-Sicherheitsgesetzes konkretisiert, sondern auch einige der ursprünglichen Vorgaben der Verordnung partiell überarbeitet. Im Sektor *Finanz- und Versicherungswesen* unterfallen Betreiber kritischer Infrastrukturen („KRITIS") gem. den Vorgaben des BSIG die Bargeldversorgung, der kartengestützte Zahlungsverkehr, der konventionelle Zahlungsverkehr, die Verrechnung und die Abwicklung von Wertpapier- und Derivatgeschäften sowie Versicherungsdienstleistungen. Die Bargeldversorgung umfasst im Einzelnen die folgenden Bereiche: Autorisierung einer Abhebung, Einbringen in den Zahlungsverkehr, Belastung des Kundenkontos und Bargeldlogistik. Kartengestützter Zahlungsverkehr beinhaltet die Bereiche Autorisierung, Einbringen in den Zahlungsverkehr sowie Belastung des Kundenkontos und die Gutschrift auf dem Konto des Zahlungsempfängers. Der konventionelle Zahlungsverkehr wird in den Bereichen Annahme einer Überweisung oder einer Lastschrift, Einbringen in den Zahlungsverkehr sowie Belastung und Gutschrift auf dem Kundenkonto erbracht. Die Verrechnung und die Abwicklung von Wertpapier- und Derivatgeschäften umfasst vor allem auch die Verbuchung von Wertpapieren sowie von entsprechenden Geldern. Kritische Versicherungsdienstleistung ist die Inanspruchnahme von Versicherungsleistungen.

Neben den Sicherheitsvorkehrungen müssen KRITIS eine Kontaktstelle zum BSI einrichten, § 8b Abs. 3 Satz 1 BSIG. Sofern erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen KRITIS führen können oder geführt haben, auftreten, sind diese Störungen an das BSI zu melden, § 8b Abs. 4 BSIG.

IV. (Rechtliche) Sicherungsmaßnahmen

Wie die angemessenen Sicherheitsvorkehrungen auszusehen haben, wird weder im BSIG noch in der MaRisk oder den BAIT ausdrücklich geregelt. Klar ist jedoch, dass neben technischen Maßnahmen auch organisatorische und rechtliche Maßnahmen erforderlich sein werden. Darüber hinaus müssen sie auch stets auf dem aktuellen Stand gehalten werden.

Doch bevor man mit der Identifizierung und Umsetzung der Maßnahmen beginnt, empfiehlt es sich, in einer Art Bestandsaufnahme das Unternehmen bzw. die Bank vollständig zu durchleuchten und auf aktuelle Abläufe und Sicherheitslücken zu prüfen.

1. Organisationshandbuch

Die besten technischen Maßnahmen sind nutzlos, wenn die größte Sicherheitslücke – der Endnutzer – nicht entsprechend vorsichtig handelt. Insofern werden sich nicht nur Arbeitsanweisungen empfehlen, die bspw. den Umgang des Mitarbeiters mit potentiellen Sicherheitslücken, die Verwendung von eigenen Excel-Sheets zur Berechnung von Investitionsentscheidungen oder den Umgang mit vertraulichen Informationen[16] regeln, sondern auch der Abschluss

16) Siehe hierzu auch Ziff. C.

von Non Disclosure Agreements, die Etablierung bestimmter Informationspflichten und Back-Up Regelungen sowie die Installation eines Business Continuity Managements. All diese Maßnahmen werden in einem Organisationshandbuch aufzunehmen sein, das als Basis der organisatorischen Sicherheitsvorkehrungen gelten wird. Das Organisationshandbuch ist stets auf dem aktuellsten Stand zu halten und sich etwaig ergebenden Änderungen anzupassen.

2. Individuelle Datenverarbeitung

Unter der individuellen Datenverarbeitung (IDV) werden durch einzelne Fachbereiche bzw. Einzelanwender selbst entwickelte Anwendungen verstanden. Darunter kann auch schon die mit Hilfe von Visual Basic für Applikationen (VBA) automatisierten Exceltabellen fallen. Typischerweise werden diese Anwendungen zur Lösung von ad-hoc Datenbedürfnissen verwendet, aber auch oft für regelmäßige Informationsbedürfnisse. Für den Anwender liegt der Vorteil der individuellen Datenverarbeitung klar auf der Hand: Schnelle und flexible Anpassung an die individuellen Wünsche des jeweiligen Anwenders sowie die fehlende Einschaltung von anderen Organisationseinheiten bzw. der IT-Abteilung.

An der individuellen Datenverarbeitung ist die mangelnde Kontrolle über die Anwendungen problematisch: Werden im Rahmen der individuellen Datenverarbeitung die richtigen Daten genutzt? Sind die Quelldaten aktuell? Sind vertrauliche Daten angemessen geschützt? Bestehen Zugriffsbeschränkungen? Sind die Ergebnisse für die interne und externe Revision nachvollziehbar? Deshalb ist auch die individuelle Datenverarbeitung in die Schutzbedarfklassifizierung von klassischen Anwendungen der Bank aufzunehmen. Es muss also auch bei der individuellen Datenverarbeitung die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sichergestellt werden.

C. Know-how Schutz

Vor Inkrafttreten der Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtwidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (RiL 2016/943) („Know-how Richtlinie")[17] waren Geschäftsgeheimnisse im europäischen Binnenmarkt nicht gleichermaßen geschützt. Zwar gibt die Definition in Art. 39 Abs. 2 des Übereinkommens über handelsbezogene Aspekte der Rechte des geistigen Eigentums („TRIPS") auf internationaler Ebene einen Mindeststandard für den Schutz von Geschäftsgeheimnissen vor, der von den Mitgliedstaaten und der Europäischen Union selbst zu beachten ist. Gleichwohl hat sich europaweit bislang kein einheitliches Verständnis zum Geheimnisschutz gebildet. Der Geheimnisschutz erfolgt teilweise im Straf-, Kartell- oder Wettbewerbsrecht, zumeist jedoch nicht über das Zivilrecht. Schützenswerte Informationen drohen bei der Übertragung in einen Mitgliedstaat mit niedrigerem Schutzniveau entwertet zu werden. Ein mangelnder Schutz gefährdet die auf Geschäftsgeheimnissen basierenden Wettbewerbsvorteile – schon die einmalige Verletzung bzw. das Offenkundigwerden von Geschäftsgeheimnissen kann zu deren Entwertung führen, sodass damit auch der Wissensvorsprung im Wettbewerb sowie die Wettbewerbsfähigkeit verloren gehen.

Aus diesen Gründen hat sich die Europäische Kommission im Rahmen der Strategie „Europa 2020" zum Ziel gesetzt, den Schutz von Geschäftsgeheimnissen zu harmonisieren. Die Know-how Richtlinie soll insbesondere Anreize zu grenzüberschreitenden Know-how Austausch fördern und zugleich Wettbewerbsvorteile der Mitgliedstaaten gegenüber außereuropäischer Konkurrenz sichern. Die Know-how Richtlinie ist bis zum 5.7.2018 in nationales Recht umzusetzen.

I. Was ist Know-how/Geschäftsgeheimnisse

Was unter Know-how zu verstehen ist, ergibt sich aus der Definition des Begriffs Geschäftsgeheimnis in Art. 2 Nr. 1 der Know-how Richtlinie. Hiernach sind als Geschäftsgeheimnis solche Informationen anzusehen, die geheim sind, deshalb einen kommerziellen Wert besitzen und Gegenstand angemessener Geheimhaltungsmaßnahmen sind. Der so bestimmte Schutzgegenstand entspricht im Wesentlichen der von der deutschen Rechtsprechung entwickelten Definition des Geschäftsgeheimnisses, ist jedoch nicht mit ihr identisch. Der Erwägungsgrund 14 der Know-how Richtlinie stellt zudem klar, dass von der Definition auch Know-how, technologische Informationen und Geschäftsinformationen umfasst sein sollen.

Ein Geschäftsgeheimnis muss demnach geheim sein, also weder in seiner Gesamtheit noch in der genauen Zuordnung und Zusammensetzung seiner Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Information umgehen, allgemein bekannt oder ohne weiteres zugänglich sein. Art. 2a. Informationen, die von interessierten Fachkreisen ohne größere Schwierigkeiten in Erfahrung gebracht werden können, sind hingegen nicht geschützt[18].

Ferner muss die Information einen kommerziellen Wert haben, was den in der deutschen Rechtsprechung entwickelten Schutzmerkmalen des Geheimhaltungsinteresses sowie der Betriebsbezogenheit entspricht[19].

Schließlich, und das ist eine wesentliche Änderung, muss die Information Gegenstand von den Umständen entsprechenden Geheimhaltungsmaßnahmen sein, Art. 1c[20].

Insbesondere für Banken ist der Schutz von Geschäftsgeheimnissen von erheblicher Bedeutung. Nicht nur gilt es, sich aufgrund einer präzisen Geschäftsstrategie von anderen Wettbewerbern abzugrenzen. Auch die Investmentstrategie, interne Planungsunterlagen und Kundeninformationen gilt es vor einem unberechtigten Abfluss zu schützen.

II. Was ändert sich?

Bereits die Definition des Begriffs Geschäftsgeheimnis zeigt, dass künftig konkrete faktische und rechtliche Geheimhaltungsmaßnahmen ergriffen werden müssen, um einen Geheimnisschutz zu erlangen. Daraus folgt konkreter Handlungsbedarf für die Unternehmen, insbesondere an der Schnittstelle zwischen Informationsmanagement und Compliance[21].

Die Know-how Richtlinie sieht zudem erstmals vor, dass eine Entschlüsselung oder Dekonstruktion durch einen Konkurrenten (auch *Reverse Engineering* genannt) von auf dem Markt frei erhältlichen Produkten, nunmehr – entgegen der bisherigen Rechtslage[22] – zulässig ist, sofern der Konkurrent rechtmäßigen Besitz an dem

17) Für eine ausführliche Auseinandersetzung mit dem Know-how Schutz vor und nach Erlass der Know-how Richtlinie: *Baranowski/Glaßl*, BB 2016, 2563.

18) *Baranowski/Glaßl*, BB 2016, 2563, 2564; *Heinzke*, CCZ, 2016, 179, 181.

19) *Baranowski/Glaßl*, BB 2016, 2563, 2565; *Heinzke*, CCZ, 2016, 179, 182.

20) Siehe hierzu auch Ziff. C.II.

21) Siehe hierzu sogleich, Ziff. C.III.

22) RGZ 149, 329, 334; *Harte-Bavendamm*, in: Gloy/Loschelder/Erdmann, Wettbewerbsrecht, 4. Aufl., § 77 RdNr. 14; *Ohly*, in: Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb, 7. Aufl., § 17 RdNr. 26 a; einschränkend wohl *OLG Düsseldorf*, OLGR 1999, 55, wonach Fortschritte im Reverse Engineering zu Lasten des Geheimnisträgers gehen sollen, siehe auch *Köhler*, in: Köhler/Bornkamm, UWG, 34. Aufl., § 17 RdNr. 8; *Baranowski/Glaßl*, BB 2016, 2563, 2565.

Produkt hat, Art. 3 Abs. 1 lit. b[23]. Insofern wird nunmehr auch innerhalb der Europäischen Union die Innovationsförderung als bedeutsamer als der Know-how Schutz angesehen[24]. Ungeachtet dessen haben Unternehmen und Geheimnisträger jedoch die Möglichkeit, *Reverse Engineering* in gewissem Maße einzuschränken. Gemäß Art. 3 Abs. 1 lit. b der Richtlinie darf der Erwerber keiner rechtsgültigen Pflicht zur Beschränkung des Erwerbs des Geschäftsgeheimnisses unterliegen. Insofern ist Unternehmen die Möglichkeit an die Hand gegeben, bspw. in R&D-Verträgen ein entsprechendes vertragliches Verbot aufzunehmen[25]. Hier zeigt sich ein durch die gesamte Richtlinie ziehender roter Faden: Wird das Unternehmen nicht aktiv tätig um seine Informationen zu schützen, wird ihm kein gesetzlicher Schutz gewährt.

Die Know-how Richtlinie sieht in Art. 5 zudem ausdrücklich Ausnahmen vom Grundsatz der Rechtswidrigkeit des Geheimnisverrats (auch *Whistleblowing* genannt) vor. Insbesondere zur Aufdeckung eines beruflichen oder sonstigen Fehlverhaltens oder einer illegalen Tätigkeit soll Geheimnisverrat erlaubt sein, sofern der Whistleblower in der Absicht handelte, das allgemeine öffentliche Interesse zu schützen. Hier wird grds. zu unterscheiden sein zwischen internem *Whistleblowing*, also dem unternehmensinternen Verrat eines Geheimnisses zum Zwecke der Aufdeckung von Missständen, Vorgängen oder Straftaten, sowie externem *Whistleblowing*, also letztlich der Strafanzeige[26]. Bislang galt der Grundsatz, dass internes *Whistleblowing* insbesondere dann gerechtfertigt bzw. unbefugt sein soll, wenn das Unternehmen Kontroll- und Selbststeuerungssysteme installiert hat[27]. Bei externem *Whistleblowing* hingegen wird bislang häufig differenzierter vorgegangen und darauf abgestellt, ob der Geheimnisverrat angemessen war oder ob nicht zuvor ein internes *Whistleblowing* hätte stattfinden müssen[28].

Die Know-how Richtlinie sieht nunmehr auch einen umfangreicheren Maßnahmenkatalog zur gerichtlichen Durchsetzung des Geheimnisschutzes vor und nähert den Know-how Schutz damit stark dem Schutz von gewerblichen Schutzrechten an. Art. 10 der Richtlinie sieht bspw. vor, dass die zuständigen Gerichte auf Antrag des Inhabers des Geschäftsgeheimnisses bestimmte vorläufige oder vorbeugende Maßnahmen gegen den angeblichen Rechtsverletzer erlassen können. Hierzu gehören insbesondere die vorläufige Einstellung der Nutzung oder Offenlegung der Geheimnisse, ein Verbot der Nutzung, der Herstellung, des Anbietens oder des Vermarktens rechtsverletzender Produkte sowie deren Beschlagnahme oder Herausgabe. Neben den vorläufigen und vorbeugenden Maßnahmen kann das Gericht nach Art. 10 Abs. 2 der Richtlinie jedoch auch anordnen, dass die Fortsetzung der Nutzung eines Geschäftsgeheimnis an die Stellung einer oder mehrerer Sicherheiten geknüpft ist, die eine Entschädigung des Inhabers sicherstellen. Die Offenlegung eines Geschäftsgeheimnisses darf hingegen nicht erlaubt werden.

Die Know-how Richtlinie sieht zudem eine Reihe von gerichtlichen Maßnahmen vor, die zum Schutz vor Geheimnisverrat erlassen werden können. So hat das Gericht die Möglichkeit, Unterlassungsanordnungen hinsichtlich des Verrats sowie der Nutzung von Geschäftsgeheimnissen oder dem Vertrieb oder Herstellung rechtsverletzender Produkte zu erlassen. Auch die Vernichtung bzw. den Rückruf der Gesamtheit oder eines Teils der Dokumente, Gegenstände, Materialien, Stoffe oder elektronischen Dateien, die das Geschäftsgeheimnis enthalten oder verkörpern, kann das Gericht anordnen, Art. 12 Abs. 1 der Richtlinie.

III. (Rechtliche) Sicherungsmaßnahmen

Die wesentlichste Änderung durch die Know-how Richtlinie, nämlich die Tatsache, dass Geheimnisinhaber nunmehr aktiv zum Schutz ihrer Geheimnisse tätig werden müssen, Art. 2c der Know-how Richtlinie, führt dazu, dass Unternehmen und Banken bestimmte Schutzmaßnahmen implementieren sollten. Diese Maßnahmen müssen zudem „angemessen" und „den Umständen entsprechend" sein. Je nach Art und Bedeutung der geheimen Information können sich Grad und Intensität der erforderlichen Sicherungsmaßnahmen im Einzelfall also unterscheiden[29].

Insofern steht auch hier wieder zunächst eine Bestandsaufnahme an, welche die schützenswerten Informationen identifiziert und entsprechend ihrer Wichtigkeit kategorisiert. Sodann können diese mit einem abgestuften Schutzsystem gesichert werden. Je wichtiger die schützenswerte Information ist, desto umfassender müssen auch die erforderlichen Sicherheitsmaßnahmen ausfallen. Neben technischen Vorkehrungen (Installation einer Firewall; Beschränkung des USB Zugriffs) sind es insbesondere juristische Mittel, die ergriffen werden müssen, u. a. die sogleich vorgestellten.

1. Organisationshandbuch

Auch beim Know-how Schutz empfiehlt sich zunächst, in einem Organisationshandbuch die getroffenen Maßnahmen und Anweisungen schriftlich festzuhalten und die Mitarbeiter hierauf zu verpflichten (siehe hierzu bereits oben, Ziff. B IV.1). Denn, gelingt es dem Geheimnisinhaber nicht, die ergriffenen Schutzmaßnahmen darzulegen und nachzuweisen oder sind die Schutzmaßnahmen nicht ausreichend, geht dies zu seinen Lasten.

2. Arbeitsrechtliche Maßnahmen

Aus arbeitsrechtlicher Sicht sollten bspw. bestehende und künftige Arbeitsverträge überarbeitet (Vereinbarung von Wettbewerbsverboten und Einräumung von Nutzungs- und Verwertungsrechten) und insbesondere mit Geheimnisträgern eine Geheimhaltungsvereinbarung getroffen werden. Darüber hinaus kann es sich empfehlen, einzelnen Mitarbeitern nur so viel Zugriff auf unternehmensinternes Know-how zu gewähren, wie für die jeweilige Arbeit erforderlich ist (*need to know*-Ansatz). Auch die Installation einer *Travel Policy* kann sich empfehlen, wenn die Mitarbeiter häufig in Länder reisen, in denen der Zoll auch eine Untersuchung der Inhalte auf Telefon und Computer vornehmen kann (bspw. in den USA).

3. Lizenzverträge; Research & Development

Bestehende und künftige Lizenzverträge, sofern bspw. wegen FinTech-Produkten vorhanden, sollten ebenfalls überarbeitet und an

23) Art. 3 Abs. 1 lit. b sieht ausdrücklich vor, dass eine Erlangung von Informationen durch „*Beobachtung, Untersuchung, Rückbau oder Testen eines Produkts oder Gegenstands, das bzw. der öffentlich verfügbar gemacht wurde oder sich im rechtmäßigen Besitz des Erwerbers der Information befindet, der keiner rechtsgültigen Pflicht zur Beschränkung des Erwerbs des Geschäftsgeheimnisses unterliegt*", rechtmäßig ist.

24) Eine ausführliche Analyse des Reverse Engineering mit einer gelungenen Auseinandersetzung mit diesem Phänomen ist zu finden bei *Harte-Bavendamm*, Festschrift Köhler, zum 70. Geburtstag, 1. Aufl., 2014, 245 ff.

25) Siehe auch Erwägungsgrund 16 der Richtlinie; *Heinzke*, Richtlinie zum Schutz von Geschäftsgeheimnissen, CCZ 2016, 179, 180; so wohl auch schon *OLG Düsseldorf*, OLGR 1999, 55.

26) *Brammsen*, in: MünchKomm zum Lauterkeitsrecht, 2. Aufl., § 17 RdNr. 57, 60 f.

27) *Brammsen*, in: MünchKomm zum Lauterkeitsrecht, 2. Aufl., § 17 RdNr. 57 m. w. Nachw.

28) Ausführlich hierzu *von Pelchrzim*, CCZ 2009 25 ff.; *Brammsen*, in: MünchKomm zum Lauterkeitsrecht, 2. Aufl., § 17 RdNr. 57, 60 f.

29) *Kalbfus/Harte-Bavendamm*, in: GRUR, Protokoll der Sitzung des Fachausschusses für Wettbewerbs- und Markenrecht zum Richtlinienvorschlag über den Schutz von Geschäftsgeheimnissen, 2014, S. 453-457, S. 453.

die neue rechtliche Situation angepasst werden, insbesondere da nunmehr *Reverse Engineering* u. U. erlaubt sein kann. Gleiches gilt für Kooperationen im Bereich von Forschung & Entwicklung (*Research & Development*), um den Abfluss von gewonnenem Know-how wirksam zu verhindern.

D. Datensicherheit und Datenschutz

Die Datenschutz-Grundverordnung („DSGVO") vereinheitlicht das Datenschutzrecht europaweit und bringt im Vergleich zum bisherigen deutschen Datenschutzrecht Neuerungen mit sich, die viele Unternehmen vor erhebliche Herausforderungen stellen. Besonders schwer wiegen die drastisch verschärften Sanktionen von bis zu 20 Mio. Euro oder vier Prozent des weltweiten jährlichen Jahresumsatzes. Hinzu kommt auch, dass betroffene Personen im Fall eines Datenschutzverstoßes künftig auch Ersatz von immateriellen Schäden verlangen können.

I. Allgemeine Neuerungen durch die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung gilt, wenn es um die Verarbeitung personenbezogener Daten geht. Das sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wie bspw. Name, Anschrift, E-Mail-Adresse, Online-Kennungen, IP-Adresse, Cookie-Kennungen, Kfz-Kennzeichen, Informationen zum Gerät oder zu Software-Anwendungen einer Person.

Bei der Verarbeitung von personenbezogenen Daten sind folgende, durch die Datenschutz-Grundverordnung ergänzte Grundprinzipien (Art. 5 DSGVO) zu beachten: der Grundsatz der Zweckbindung, von Treu und Glauben, der Rechenschaftspflicht, der Rechtmäßigkeit der Verarbeitung, der Transparenz, der Datenminimierung, der Integrität und Vertraulichkeit, der sachlichen Richtigkeit der Daten, der Begrenzung der Speicherdauer, Privacy by Design und Privacy by Default. Die Datenverarbeitung muss also insbesondere rechtmäßig, transparent und fair, nur für explizit festgelegte und legitime Zwecke und begrenzt auf das für die Zweckerreichung notwendige Maß erfolgen. Zudem müssen die Verantwortlichen (hier die Banken) die Rechtmäßigkeit ihrer Verarbeitung nachweisen. Eine Einwilligung ist bspw. nicht verbindlich, wenn sie einen Verstoß gegen die Datenschutz-Grundverordnung darstellt; den Verantwortlichen trifft dann eine Nachweispflicht für das Vorliegen der Einwilligung.

Durch die Datenschutz-Grundverordnung werden auch die Informations- und Auskunftspflichten um weitere Angaben erweitert. Dabei wird danach differenziert, ob die Daten bei der betroffenen Person erhoben werden, Art. 13 DSGVO, oder nicht, Art. 14 DSGVO. Künftig müssen insbesondere folgende Grundinformationen bereitgehalten werden: Name und Kontaktdaten des Verantwortlichen, Kontaktdaten des Datenschutzbeauftragten, Zwecke und Rechtsgrundlage der Verarbeitung, Empfänger oder Kategorien von Empfängern, ggf. Informationen zum beabsichtigten Datentransfer in Drittstaaten sowie Hinweise auf das Widerspruchsrecht.

II. Datensicherheit

Als zentrales Prinzip des Datenschutzes wurde mit Art. 32 der DSGVO auch die Datensicherheit normiert und somit besondere Gewährleistungspflichten festgelegt. Art. 32 DSGVO soll den Betroffenen insbesondere vor sicherheitsrelevanter Vernichtung, Verlust und unbefugter Offenlegung bereits erhobener Daten schützen. Der Verantwortliche für die Datenverarbeitung sowie der Auftragsverarbeiter werden umfassend verpflichtet, geeignete Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung zu ergreifen. So sind u. a. geeignete technische und organisatorische Maßnahmen unter Berücksichtigung von folgenden acht Kriterien zu implementieren: Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Die Angemessenheit des Schutzniveaus richtet sich – wie auch schon beim Know-how Schutz, siehe oben – nach den Risiken aus. Dabei sind u. a. auch die unterschiedliche Eintrittswahrscheinlichkeit sowie die Schwere des Risikos für die persönlichen Rechte und Freiheiten natürlicher Personen zu beachten. Bestimmte Maßnahmen wie Pseudonymisierung, Verschlüsselung, Verfügbarkeit der Systeme usw. werden beispielhaft benannt.

In der Praxis hat also eine Schutzbedarfsfeststellung zu erfolgen, indem der jeweilige Schutzbedarf der unterschiedlichen personenbezogenen Daten ermittelt wird. Dabei werden i. d. R. zunächst typische Schadenszenarien ermittelt und anschließend der Schutzbedarf für die einzelnen personenbezogenen Daten abgeleitet.

Die Erfüllung der Anforderungen an die geeigneten technischen und organisatorischen Maßnahmen kann durch Einhaltung genehmigter Verhaltensregeln (Art. 40 Abs. 2h DSGVO) oder eines genehmigten Zertifizierungsverfahrens (Art. 42 DSGVO) nachgewiesen werden. Dies ist insbesondere vor dem Hintergrund der allgemeinen Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) für die Datensicherheit, die sich aus Art. 5 Abs. 1f DSGVO ergibt, vorteilhaft.

III. Ausgewählte Neuerungen durch die DSGVO

Für die Datenverarbeitung der Banken werden insbesondere folgende Neuerungen durch die DSGVO relevant sein.

1. Einwilligungen

Bestehende Einwilligungserklärungen sollen auch nach Inkrafttreten der Datenschutz-Grundverordnung wirksam bleiben. Für solche Alt-Einwilligungen ist jedoch ein gewisser Mindestgehalt erforderlich, wie z. B. die Voraussetzung der Freiwilligkeit sowie der Transparenz (Erwägungsgründe 42 und 43 DSGVO).

Die Anforderungen an neu einzuholende Einwilligungen wurden durch die Datenschutz-Grundverordnung erhöht. In vielen Fällen erklärt die DSGVO eine Einwilligung, die eigentlich vorliegt, für unbeachtlich. Eine Einwilligung muss insbesondere folgenden Kriterien entsprechen: Die Einwilligung muss in informierter Weise bezogen auf einen bestimmten Fall und einen bestimmten Zweck erfolgen, sie muss freiwillig gegeben werden, in informierter Weise, unmissverständlich in Form einer Erklärung oder einer eindeutig bestätigenden Handlung geschehen und nachweisbar sein.

2. Zusammenarbeit mit Auskunfteien

Anfragen von verantwortlichen Stellen bei Auskunfteien zur Prüfung der Bonität im vorvertraglichen Bereich, aber auch Bonitätsabfragen etwa zur Prüfung der Erfolgsaussichten von Vollstreckungsmaßnahmen können grds. i. S. v. Art. 6 Abs. 1 lit. b DSGVO als erforderlich zur Durchführung vorvertraglicher oder vertraglicher Maßnahmen angesehen werden. Für die Erteilung einer Auskunft durch Auskunfteien bietet Art. 6 Abs. 1 lit. f DSGVO eine ausreichende Rechtsgrundlage. Dem sollen grds. nach Auffassung des Hessischen Datenschutzbeauftragten auch nicht die Interessen oder

Grundrechte und Grundfreiheiten der betroffenen Personen entgegenstehen[30]. Wie bisher kann ein bestehendes oder drohendes kreditorisches Risiko die Rechtmäßigkeit einer Bonitätsabfrage indizieren.

Auf einen vorherigen Nachweis der Zulässigkeit einer Bonitätsabfrage gegenüber der Auskunftei kann verzichtet werden. Zwar enthält die Datenschutz-Grundverordnung nicht mehr die grds. Privilegierung der Bonitätsabfrage nach § 29 Abs. 2 BDSG. Allerdings wird die Forderung eines Einzelnachweises und dessen Speicherung bzw. Aufbewahrung im Massengeschäft als überzogen angesehen, da sie berechtigte und zulässige Datenübermittlungen aus rein formalen Gründen vereiteln würde. Vielmehr soll es nach Auffassung des Hessischen Datenschutzbeauftragten weiterhin ausreichen, wenn das berechtigte Interesse glaubhaft gemacht wird[31]. Mangels ausdrücklicher gesetzlicher Privilegierung kann jedoch nicht mehr von einer generellen Zulässigkeit der bloßen Glaubhaftmachung ausgegangen werden.

3. Scoring nach der DSGVO

Scoring ist eine Art des Profiling, was wiederum in Art. 4 Nr. 4 DSGVO definiert ist. „Profiling" ist demnach jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten. Für automatisierte Entscheidungen ist Art. 22 Abs. 1 DSGVO zu beachten. Demnach ist es verboten, eine betroffene Person einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung zu unterwerfen, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Nach Auffassung des Hessischen Landesschutzbeauftragten entsprechen die derzeit üblichen Scoring-Verfahren den Anforderungen des Art. 6 Abs. 1 lit. b und f DSGVO, sofern und soweit nur risikorelevante Merkmale eingesetzt werden[32]. Eine Auswertung von personenbezogenen Daten aus Social Media Netzwerken soll jedoch nicht rechtmäßig sein. Denn alleine aus der etwaigen freien Zugänglichkeit dieser Daten ergibt sich noch keine Rechtmäßigkeit ihrer Verwendung im Profiling.

4. Auftragsverarbeitung nach der DSGVO

Viele Banken nutzen in erheblichem Umfang Auftragsverarbeiter, z. B. für IT-Leistungen und das Hosting. Auch für die Auftragsverarbeitung gelten geänderte Rahmenbedingungen. Während nach den Vorgaben des Bundesdatenschutzgesetzes allein der Auftraggeber für die Datenverarbeitung verantwortlich ist, kann auf Grundlage der Datenschutz-Grundverordnung künftig auch der Auftragsverarbeiter in gewissen Grenzen zur Verantwortung gezogen werden, z. B. bei der Festlegung der angemessenen technischen und organisatorischen Datensicherheitsmaßnahmen (gem. Art. 32 DSGVO) und der Regelung für rechtmäßige Drittlandtransfers (gem. Art. 44 bis 49 DSGVO).

Des Weiteren ist voraussichtlich für den Abschluss einer Auftragsverarbeitung neben der Schriftform nun zukünftig ausdrücklich auch die elektronische Form zulässig, was in der Praxis zu wesentlichen Erleichterungen bei Vertragsabschlüssen insbesondere im Online-Bereich führen dürfte.

5. Forderungskauf nach der DSGVO

Die Bereitstellung und Weitergabe darlehensnehmerbezogener Daten bei einem Forderungskauf bedarf wegen des auch nach der Datenschutz-Grundverordnung geltenden Verbots mit Erlaubnisvorbehalt der datenschutzrechtlichen Zustimmung. Nach der Datenschutz-Grundverordnung ist eine Datenverarbeitung zulässig, wenn eine Einwilligung (Art. 6 Abs.1 lit. a DSGVO) oder ein weiterer gesetzlicher Rechtfertigungsgrund (Art. 6 Abs. 1 lit. b-f DSGVO) vorliegt. Anders als im Bundesdatenschutzgesetz wird künftig nicht mehr zwischen Erheben, Nutzen und Verarbeiten unterschieden. Vielmehr werden diese Begriffe als „Verarbeitung" zusammengefasst.

Für die Zugänglichmachung der Daten der Kreditnehmer an den Forderungserwerber kommt Art. 6 Abs. 1 lit. b DSGVO als Rechtsgrundlage in Betracht. Demnach ist die Verarbeitung und somit auch die Datenweitergabe gestattet, wenn sie für die Erfüllung des Vertrages erforderlich ist. Der Begriff der „Erfüllung" umfasst regelmäßig die Durchführung des Vertrages sowie auch dessen Abwicklung in Bezug auf Gewährleistung und sekundäre Leistungspflichten[33]. Neben der Erfüllung sind i. d. R. auch Vertragsanbahnungen erfasst. Das Kreditinstitut bedarf der Daten, um die Erfüllung der Zahlungsverpflichtungen durch den Darlehensnehmer zu überwachen und zu verbuchen und um bei etwaigen Zahlungsausfällen tätig zu werden. Aus diesen Gründen ist die Erforderlichkeit der Verarbeitung der Daten i. d. R. gegeben[34].

Die Datenübermittlung zwischen dem Schuldner und der Bank ist als Verarbeitung gem. Art. 6 Abs. 1 lit. b DSGVO zulässig, wenn sie zur Abwicklung des Vertrags zwischen dem Schuldner und der Bank zulässig ist. Da der Forderungskäufer an die Stelle des bisherigen Gläubigers tritt und daher alle diesem zulässigerweise vorliegenden Vertragsinformationen zum Darlehensnehmer benötigt, ist die Datenübermittlung dementsprechend erforderlich und damit zulässig[35].

Bei der Datenweitergabe an den Zessionar sind zudem die allgemeinen Verarbeitungsgrundsätze nach Art. 5 DSGVO einzuhalten. Der Zweck der Verarbeitung, nämlich Erfüllung bzw. Durchführung des Darlehensvertrags, bleibt beim Empfänger derselbe. Verkauf und Abtretung der Kreditforderung werden bei einer offenen Zession gegenüber dem Kreditnehmer offengelegt[36].

Demzufolge ist festzuhalten, dass die Übermittlung der Vertragsdaten vom Ursprungsgläubiger an den Zessionar bei einem Forderungsverkauf nach Art. 6 Abs. 1 lit. b DSGVO grds. datenschutzrechtlich zulässig ist.

IV. Vorbereitungsmaßnahmen für die Datenschutz-Grundverordnung

Bis zum Inkrafttreten der Datenschutz-Grundverordnung am 25.5.2018 dürften sich folgende Maßnahmen zur Vorbereitung empfehlen. In einem ersten Schritt sollten die Prozesse identifiziert werden, in denen personenbezogene Daten verarbeitet werden (die Bestandsaufnahme, siehe oben). Im nächsten Schritt ist ein Verzeichnis der Verarbeitungstätigkeiten anzulegen. Dann ist zu prüfen, ob das neue Recht für alle Prozesse eine entsprechende Rechtsgrundlage bereitstellt oder ob eine entsprechende Einwilligung vorliegt. Des Weiteren kann es erforderlich sein, eine Daten-

30) 45. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Stand 24.4. 2017, Ziff. 4.2.1.1.
31) 45. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Stand 24.4. 2017, Ziff. 4.2.1.1.
32) 45. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Stand 24.4. 2017, Ziff. 4.2.1.3.
33) *Plath*, in: Plath, BDSG/DSGVO, 2. Aufl., 2016, Art. 6 DSGVO, RdNr. 9.
34) *Frenzel*, in: Paal/Pauly, DSGVO, 1. Aufl., 2017, Art. 6 RdNr. 14.
35) ZD 2017, 114/117.
36) ZD 2017, 114/117.

schutzfolgenabschätzung mit verpflichtender Konsultation der zuständigen Aufsichtsbehörde (Art. 35, 36 DSGVO) vorzunehmen. Zudem sind bereits bestehende Verträge zur Auftragsverarbeitung anzupassen. Die Melde- und Konsultationspflichten gegenüber den Aufsichtsbehörden nach Art. 33, 36 und 37 DSGVO sind in den internen Abläufen der Banken abzubilden (neu: 72-Stunden-Frist). Außerdem ist auch die Erfüllung der Dokumentationspflichten zu organisieren, z. B. Verarbeitungsverzeichnis (Art. 30 DSGVO), Dokumentation von Datenschutzvorfällen (Art. 33 Abs. 5 DSGVO) oder Dokumentation von Weisungen im Rahmen von Auftragsverarbeitungsverhältnissen (Art. 28 Abs. 3 lit. a DSGVO). Im Übrigen sind auch die Betroffenen- und Informationspflichten umzusetzen, z. B. das Recht auf Löschung, auf Berichtigung, auf Einschränkung der Verarbeitung, Übertragbarkeit, Recht auf Vergessenwerden und Widerspruch.

E. Ausblick

Der Regulierungsdruck auf Banken steigt – nicht nur durch die BaFin sondern auch durch den Europäischen Gesetzgeber. Neben den laufenden Kontrollen zur Einhaltung regulatorischer Zulässigkeitsanforderungen müssen Banken nunmehr auch ihre Sicherheit im Blick haben und Cyberangriffen erfolgreich vorbeugen, ihr Know-how identifizieren und entsprechend schützen sowie die Prozesse zur Datenverarbeitung überarbeiten. Es gibt also für die Banken viel zu tun im Jahr 2018 – und es sieht nicht danach aus, dass der Regulierungsdruck absinken wird.