D 7465

Zeitschrift für das gesamte
KREDITWESEN

71. Jahrgang · 15. Juni 2018

12-2018

Pflichtblatt der Frankfurter Wertpapierbörse
Fritz Knapp Verlag · ISSN 0341-4019

Digitaler Sonderdruck

Swaantje Anneke Haß / Nils Purwin / Vladimir Bozok

Anstehende Regularien mit Auswirkungen auf den Zahlungsverkehr

Foto: freevector

Swaantje Anneke Haß / Nils Purwin / Vladimir Bozok

Anstehende **Regularien** mit Auswirkungen auf den Zahlungsverkehr

Nachdem die zweite Zahlungsdiensterichtlinie (PSD2) in deutsches Recht umgesetzt wurde, ist es sinnvoll einen Blick auf weitere Regulierungsvorhaben zu werfen, die den Zahlungsverkehr betreffen. Neben der EU-Datenschutzgrundverordnung (EU-DSGVO) und der Geldwäscherichtlinie gibt es zahlreiche weitere Regelwerke, die 2018 und darüber hinaus auf Zahlungsdienstleister zukommen und sie mittelbar oder unmittelbar berühren (Abbildung).

Datenschutz für alle in der EU ansässigen Unternehmen

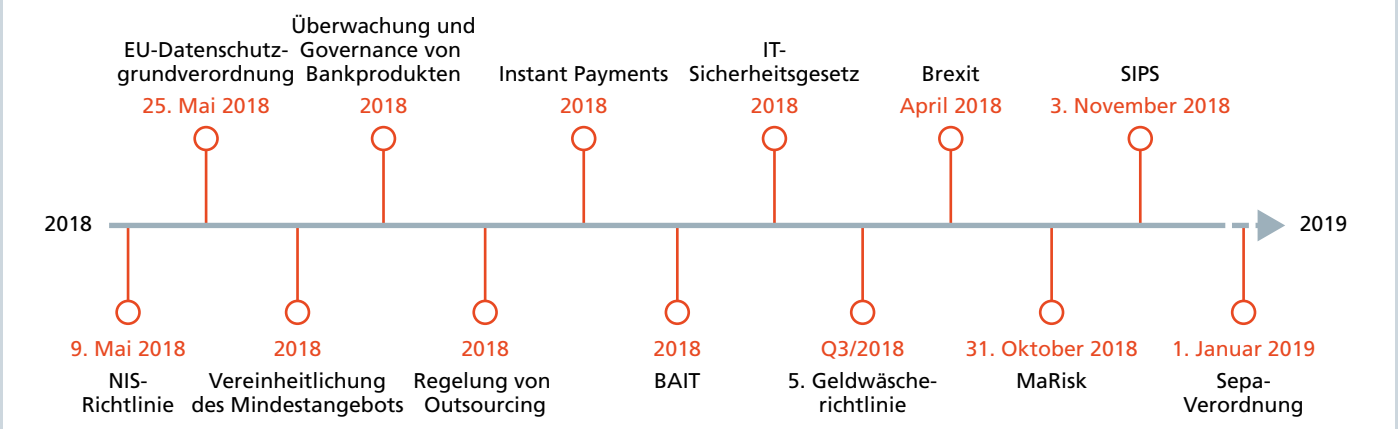
1. EU-Datenschutz-Grundverordnung (EU-DSGVO) und E-Privacy-Reform: Mit der EU-DSGVO ist am 25. Mai 2018 eine in der Öffentlichkeit oft diskutierte Verordnung in Kraft getreten. Zeitgleich aktualisiert der deutsche Gesetzgeber das Bundesdatenschutzgesetz (BDSG), da er die Öffnungsklauseln der EU-DSGVO nutzt und im gleichen Zug das BDSG modernisiert. Von der Verordnung sind grundsätzlich alle Unternehmen betroffen, die in der EU ansässig sind, personenbezogene Daten verarbeiten oder auch Unternehmen aus Drittstaaten, die sich in der EU niedergelassen haben. Der Schwerpunkt liegt dabei auf Daten, die sich auf identifizierte oder identifizierbare Personen beziehen wie zum Beispiel Name, Adresse, E-Mail-Adresse, Geburtsdatum oder auch Kontodaten (sogenannte personenbezogenen Daten).

Da die EU-DSGVO für alle in der EU ansässigen Unternehmen Anwendung findet, gilt sie auch für Kreditinstitute und Zahlungsdienstleister. Folglich müssen auch gerade die mit der PSD2 eingeführten Payment Initiation Service Provider (PISP) und Account Information Service Provider (AISP) den Anforderungen der EU-DSGVO nachkommen. So muss die Auswertung von Zahlungsverkehrsdaten vom Anbieter offengelegt und ihr muss vom Nutzer ausdrücklich zugestimmt werden. Insbesondere ist das bei der Durchführung des Risikoscorings für die Kreditvergabe und der Kreditwürdigkeitsprüfung relevant. Zudem müssen dem Nutzer alle an dem Prozess beteiligten Dienstleister sowie die Zwecke der Datenverarbeitung benannt werden (Transparenzgrundsatz nach Art. 14 DSGVO).

Recht auf das Löschen der Nutzerdaten

Eine wesentliche Neuerung der EU-DSGVO ist das Recht auf das Vergessenwerden (Löschung der Nutzerdaten, Art. 17 DSGVO). So können die Nutzer ihr Recht auf das Löschen der Nutzerdaten geltend machen, wenn für die Verwendung der Daten keine Berechtigung mehr vorliegt. Deshalb wird im Art. 17 der DSGVO erstmals eine eigenständige Regelung eingeführt, die es den Personen möglich machen soll, die Daten aus den folgenden Gründen löschen zu las-

Übersicht der ZV-Regulierungen 2018/2019



Quelle: PPI AG

sen: der Zweck der Datenverarbeitung ist weggefallen (Art. 17 a), der Betroffene hat seine Einwilligung widerrufen (Art. 17 b) und die Datenverarbeitung war unrechtmäßig (Art. 17 d). Dies gilt sowohl für Suchmaschinen als auch für jeden anderen Anbieter, der personenbezogene Daten verarbeitet.

Die neu eingeführte Datenportabilität (Art. 20 DSGVO) gibt den Nutzern das Recht auf eine einfache und schnelle Datenübertragbarkeit von einem Anbieter zum anderen. So können die Nutzer ihren alten Anbieter auffordern, die personenbezogenen Daten in einem geeigneten Format an den neuen Anbieter zu übertragen (zum Beispiel beim Wechsel der Bank).

Daneben kommen noch Neuerungen wie Rechenschaftspflicht (Art. 5), Haftungsregeln und höhere Sanktionen (Art. 77 bis 84), Meldepflichten von Datenpannen (Art. 33) oder Technikgestaltung (Privacy by Design, Art. 25 Abs. 1) und datenschutzfreundliche Voreinstellungen (Privacy by Default, Art. 25 Abs. 2) auf die Geldhäuser zu, die sie zu implementieren haben.

Gleiche Entgelte für inländische und grenzüberschreitende Zahlungen

Gleichzeitig plant die EU eine ePrivacy-Reform. Die abschließenden Verhandlungen sollen im Trilog-Verfahren im Herbst 2018 stattfinden. Die Reform soll den Nutzern mehr Selbstbestimmung über private Kommunikationsdaten im Browser und in Apps ermöglichen. So wären beispielsweise Cookie-Tracking, Datenerhebung durch Dritte oder Reichweitenmessung unter Umständen gar nicht oder nur eingeschränkt möglich. Bereits Ende vergangenen Jahres kam es zu heftigen Diskussionen zwischen Journalisten, Datenschutzbeauftragten, Politikern und Ökonomen über die möglichen Auswirkungen der ePrivacy-Reform.

2. Sepa-Verordnung (Single Euro Payments Area): Auf der Grundlage der EU-Preisverordnung Nr. 924/2009 vom 16. September 2009, die gleiche Entgelte für inländische und grenzüberschreitende Zahlungen in Euro verlangte, haben das Europäische Parlament und der Rat mit der Sepa-Verordnung (2012/260) den Eurozahlungsverkehr zum 1. Februar 2014 weiter harmonisiert. Es wurden einheitliche Regeln für Überweisungen und Lastschriften eingeführt. Zudem wurde die Kontonummernsystematik mit der Einführung der IBAN standardisiert und die technischen Formate mittels des ISO-Standards vereinheitlicht.

Mehr Transparenz bei der Währungsumrechnung

Nun hat die Europäische Kommission die Sepa-Verordnung aktualisiert und ihren Entwurf am 28. März 2018 dem Europäischen Parlament und dem Rat vorgelegt. Dieser enthält einen Vorschlag für die Einführung eines gleichen Entgeltniveaus für interstaatliche und grenzüberschreitende Zahlungen in allen EU-Währungen. Demzufolge erhebt der ZDL (Zahlungsdienstleister) von einem ZDN (Zahlungsdienstnutzer) für grenzüberschreitende Zahlungen in der EU Entgelte in gleicher Höhe, wie er sie von einem ZDN für entsprechende Inlandszahlungen in der Landeswährung erheben würde (Artikel 3, Abs.1 SEPA-VO).

Gleichzeitig soll dem Auftraggeber und dem Zahlungsempfänger mehr Transparenz bei der Währungsumrechnung gewährleistet werden. Dies geschieht durch eine verpflichtende Offenlegung der gesamten Kosten von Währungsumrechnungsdiensten. Diese sind dem ZDN sowohl an einem Geldautomaten als auch am Point-of-Sale anzuzeigen (Artikel 3, Absatz 2 SEPA-VO). Die Verordnung soll zum 1. Januar 2019 in Kraft treten. Es ist jedoch abzuwarten, wie schnell eine Einigung in den Trilogverhandlungen erzielt werden kann.

3. Instant Payments: Seit Ende 2017 ist es europaweit möglich, Zahlungen in Euro binnen Sekunden vom Auftraggeber zum Empfänger zu transferieren. Der European Payments Council (EPC) hat dazu ein eigenes Rulebook (Scheme) für SCT Inst (Überweisungen in Echtzeit) veröffentlicht. Der Service des sogenannten Instant Payments (SCT Inst) dauert nur bis zu 15 Sekunden, ist 365 Tage im Jahr verfügbar und wird bis zu einem maximalen Betrag von 15 000 Euro angeboten. Bald soll der Dienst flächendeckend in den 34 zur Single Euro Payments Area (Sepa) gehörenden Ländern nutzbar sein.


Foto: PPI AG

Swaantje Anneke Haß

Managing Consultant Zahlungsverkehr, PPI AG, Frankfurt am Main


Foto: PPI AG

Nils Purwin

Managing Consultant Zahlungsverkehr, PPI AG, Frankfurt am Main


Foto: PPI AG

Vladimir Bozok

Associate Consultant, PPI AG, Frankfurt am Main

Nachdem Anfang dieses Jahres die zweite Zahlungsdiensterichtlinie (PSD2) und kürzlich die EU-Datenschutzgrundverordnung (EU-DSGVO) umgesetzt werden mussten, beschäftigen sich die Autoren mit weiteren Regulierungsmaßnahmen, die 2018 und darüber hinaus auf die Zahlungsdienstleister zukommen. Sie nennen beispielsweise die Aktualisierung der Sepa-Verordnung, die das gleiche Entgelt für inländische und grenzüberschreitende Zahlungen in Euro verlangt. Bei den neuen Mindestanforderungen an das Risikomanagement (MaRisk) wiederum sehen die Autoren die Änderungen bei der Steuerung der Liquiditätsrisiken als aufwendigsten Punkt an. Doch auch die ungeklärten Fragen des Brexits, die Zulassung von Fintechs und die 5. Geldwäscherichtlinie, mit bereits angekündigten Anpassungen derselben, werden nach Auffassung der Autoren für einigen Aufwand bei den Zahlungsdienstleistern führen. (Red.)

Für die Einführung werden viele Banken noch Vorlaufzeit benötigen, um ihre IT an diese Standards anzupassen. Der Großteil des deutschen Marktes wird sich deswegen erst im Laufe des Jahres 2018 dem Dienst anschließen. Zunächst soll der Dienst als Extraleistung angeboten und dementsprechend bepreist werden. Doch über kurz oder lang soll Instant Payments die üblichen Sepa-Überweisungen ablösen und zum Standardangebot der Banken gehören. Aktuell ist die Teilnahme an Instant Payments freiwillig.

4. Brexit: Der Austritt Großbritanniens (GB) aus der Europäischen Union (EU) ist eine beschlossene Sache, die zum 29. März 2019 rechtswirksam sein wird. Die konkrete Ausgestaltung des Austrittsprozesses soll in den Verhandlungen zwischen der EU und GB bis Herbst 2018 erarbeitet und zur Konsultation gestellt werden.

Ungelöste Rechtsfragen

In den letzten Wochen haben sich die Parteien auf eine Übergangslösung bis 2020 geeinigt, in der der Brexit in mehreren, kleinen Phasen erfolgen soll. In dieser Übergangszeit wird GB die Vorteile des EU-Binnenmarkts eingeschränkt nutzen dürfen, gleichzeitig aber auch die EU-Regeln einhalten müssen. Nach der Übergangsfrist würde GB endgültig nicht mehr zur EU gehören. Damit wären Zahlungen von und nach GB nicht mehr als innereuropäische Zahlungen zu behandeln und würden folglich nicht mehr dem europäischen Zahlungsverkehrsrecht unterliegen. Demnach müssten zum Beispiel die Entgelte für Zahlungen in britischem Pfund (GBP) und die Ausführungsfristen der Zahlungen denen in andere Drittstaaten angepasst werden.

Beim heutigen Stand müssten zudem viele der zugelassenen Finanzdienstleister ihren Sitz von Großbritannien nach Europa verlagern, damit sie ihre Dienste auch weiterhin europaweit anbieten können. Aufgrund der unterschiedlichen Zulassungspflichten zwischen GB und anderen EU-Ländern, dürfte sich dieser Vorgang nicht als unproblematisch erweisen. Denn GB gehört zu den EU-Mitgliedsstaaten, in denen es vergleichsweise einfach ist, die Auflagen für eine Lizenz zu erfüllen. Deshalb versucht die EU-Kommission eine Lösung für die anstehenden Verlagerungen der Firmensitze zu erarbeiten, um den Unternehmen einen unkomplizierten Einstieg in den EU-Binnenmarkt zu ermöglichen.

So sollen beispielsweise größere Wertpapiergesellschaften, die als Drittstaatsunternehmen aufgeführt werden und bankähnliche Tätigkeiten nachgehen, dem Aufsichtsmechanismus der Europäischen Zentralbank (EZB) unterliegen. Dadurch wären CRR-Kreditinstitute und große Wertpapiergesellschaften einer einheitlichen Aufsicht unterstellt und müssten dieselben Standards erfüllen.

5. Mindestanforderungen an das Risikomanagement (MaRisk): Am 27. Oktober 2017 hat die BaFin die neuen MaRisk (5. Novelle) veröffentlicht und schreibt eine Umsetzungsfrist bis zum 31. Oktober 2018 vor. In der Novellierung werden einige Anpassungen und Neuerungen auf die Banken zukommen. Insgesamt sind Änderungen in den Bereichen BTO 1 Kreditgeschäft, BTR 3.1 Steuerung der Liquiditätsrisiken, BT 3.1 Risikoberichterstattung und AT 9 Auslagerungen vorgesehen.

Änderungen bei der Steuerung der Liquiditätsrisiken

Einen signifikanten Umsetzungsaufwand werden die Änderungen bei der Steuerung der Liquiditätsrisiken verursachen. Hier müssen die Geldhäuser einen Prozess für die angemessene, zeitnahe Messung, Steuerung und Überwachung der untertägigen Liquidität implementieren. Daraus soll dann eine aussagekräftige Übersicht mit den entsprechenden Fristigkeiten der Liquiditätslage abgeleitet werden.

Im Bereich der Risikoberichterstattung und der Auslagerung wurden vor allem viele, kleinere Anpassungen vorgenommen. Die Berichterstattung soll zeitnah und vollständig mit einem gewissen Standard an Qualität der Informationen erfolgen. Ausgelagert werden soll nur an Dienstleister, mit denen im Vorfeld ein Auslagerungsvertrag über etwa zivilrechtliche Gestaltung, Risikoanalyse, Schlechtleistung vereinbart wurde. Betroffen sind unter anderem die Kreditinstitute, die beispielsweise ihre Zahlungsverkehrsabwicklung ausgelagert haben.

6. Zulassung von Fintechs: Einen großen Stellenwert haben mittlerweile Fintechs im Finanzsektor eingenommen und sind ernstzunehmende Konkurrenten für das traditionelle Bankgeschäft. Über Kredit- und Einlagengeschäft bis hin zum Zahlungsverkehr sind sie in allen Finanzbereichen vertreten. Seit Juli 2016 haben bereits sechs Fintech-Kreditinstitute von der Europäischen Zentralbank (EZB) eine Zulassung erhalten. Da dieser Trend an Dynamik gewinnt, hat die EZB im September 2017 ein Konsultationspapier zur Leitlinie für die Zulassung von Fintech-Kreditinstituten veröffentlicht. Dieser Entwurf soll nun 2018 in der finalen Version erscheinen und wird auf Fintechs anwendbar sein, die einen Antrag auf die Erlaubnis für das Anbieten von Fintech-Produkten stellen. Damit soll zum einen eine Harmonisierung bei der Verwaltung der Zulassungsanträge erreicht werden und zum anderen Hilfestellung für Antragsteller geleistet werden.

Der Fokus der Leitlinie liegt vor allem auf IT-Sicherheit, Gewährleistung des Datenschutzes und Schutz vor Cyberangriffen. Damit macht die EZB den Antragstellern deutlich, welche Aspekte eine besondere Bedeutung für eine Zulassung darstellen. Daneben verlangt die Leitlinie fachlich ausreichende Managementqualitäten sowie technisches Fachwissen seitens Investoren, damit ein hoher Einfluss von Investoren mit wenig/kaum Fachwissen auf die Unternehmensführung verhindert wird. Vornehmlich soll das in der Gründungsphase der Fall sein, da hier die Start-ups auf Investitionen angewiesen und möglicherweise bereit sind, ihre Stimmgewicht gegen frisches Kapital zu reduzieren. Unter gewissen Umständen muss zudem ein Chief Technology Officer auf der Ebene der Geschäftsleitung bestimmt werden. Ebenfalls wird ein Exit-Plan als Bestandteil des Geschäftsplans der Fintechs von der EZB erwartet, der

eine systematische Abwicklung im Insolvenzfall aufzeigen soll.

7. Fünfte/Sechste Geldwäscherichtlinie: Am 15. Dezember 2017 wurde durch eine Einigung in den Trilogverhandlungen eine neue Geldwäscherichtlinie hervorgebracht, die sich nun in Konsultation befindet. Der Gesetzestext wird im Sommer 2018 erwartet.

Breit gefasster Anwendungsbereich

Der Anwendungsbereich der, mittlerweile 5. Geldwäscherichtlinie, ist ohnehin sehr breit gefasst und schließt Kreditinstitute, Zahlungsinstitute, E-Geldinstitute, Wertpapiergesellschaften, Versicherungen, Investmentfonds, Abschlussprüfer oder Immobilienmakler ein. Nun wird dieser um Umtauschplattformen virtueller Währungen sowie elektronische Geldbörsen (etwa Wallets für Bitcoins) erweitert.

Darüber hinaus soll der Schwellenbetrag für nicht wiederaufladbare Prepaid-Produkte (von 250 auf 150 Euro) reduziert werden und eine anonyme Ausgabe von E-Geld nur unterhalb dieser Grenze möglich sein. Diese Maßnahme soll zu mehr Transparenz im Bereich der E-Geldprodukte führen. In diesem Zusammenhang soll es gleichzeitig strengere Anforderungen an die Kundenüberprüfung geben.

Für eine schnelle und effektive Aufdeckung von Verstößen sollen die Geldhäuser und nationale Aufsichtsbehörden in Zukunft enger zusammenarbeiten. Dazu werden zentrale Meldestellen (Financial Intelligence Units) die Erlaubnis erhalten, auf Zahlungskonten des Kontoinhabers über zentralisierte Registerstellen zuzugreifen, um unverzüglich eingreifen zu können.

Aus Sicht der EU-Kommission scheint die 5. Geldwäscherichtlinie noch immer keine ausreichende Grundlage für die Verhinderung von Geldwäsche und Terrorismusfinanzierung zu bieten. So schlägt sie bereits heute weitere Anpassungen vor. Deshalb wird in Fachkreisen bereits von der „sechsten" Geldwäscherichtlinie gesprochen. Die geplanten Änderungen stellen kein „Update" mehr dar, sondern beinhalten wesentliche materielle Veränderungen. So soll beispielsweise eine Liste mit möglichen Vortaten für Geldwäsche verfasst werden. Darunter fallen Steuerdelikte, Cyberkriminalität oder auch Umweltkriminalität.

Spezielle Überwachungssysteme vorgeschrieben

Betroffene Unternehmen, speziell natürlich Zahlungsdienstleister und Kreditinstitute, müssen ihre Mitarbeiter über die Änderungen schulen, damit eine lückenlose Verhinderung von Geldwäsche gewährleistet werden kann. Zusätzlich müssen Unternehmen spezielle Überwachungssysteme einführen, um Zahlungsvorgänge zu ermitteln, die mit möglichen Vortaten zusammenhängen könnten.

8. Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme (Systemically Important Payment Systems = SIPS): Am 3. November 2017 veröffentlichte die Europäische Zentralbank (EZB) die Verordnung (EU) 2017/2094. Basierend auf den Ergebnissen aus der Überprüfung der Verordnung (EU) 795/2014 zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme, sieht der EZB-Rat die Notwendigkeit einer Verbesserung und Präzisierung des Inhalts der ursprünglichen Verordnung. Er gibt den Adressaten ein Jahr Umsetzungszeit (bis November 2018).

Systemrelevante Zahlungsverkehrssysteme sind Großbetrags- und Massenzahlungssysteme, die aufgrund der Transaktionsvolumina, eines großen Marktanteils, der Relevanz für grenzüberschreitende Zahlungen und der Bereitstellung von Dienstleistungen für andere Infrastrukturen eine enorme Bedeutung für die Finanzstabilität darstellen. Zu diesen Systemen gehören Target-2, Euro-1, Step-2-T und Core, wobei die Liste kontinuierlich aktualisiert wird.

Neben einigen formalen Anpassungen enthält die Verordnung Änderungen auf drei Ebenen. Die Unterteilung erfolgt in Kreditrisiko, Liquiditätsrisiko und allgemeine Geschäftsrisiken. So hat ein SIPS-Betreiber einen robusten Rahmen zur Messung, Überwachung und Steuerung der Kreditrisiken einzurichten, die sich aus den Zahlungs- und Verrechnungsprozessen des SIPS ergeben.

Zusätzlich müssen die SIPS-Betreiber über angemessene Instrumente zur effektiven Steuerung ihrer Liquidität verfügen, die einen ungehinderten Liquiditätsfluss überwachen und kontinuierlich verbessern. Woraufhin ein entsprechender Rahmen zum Management einzurichten ist und diesem angemessene Instrumente zur Verfügung zu stellen sind, die eine effektive Überwachung und reibungslose Funktionalität der Zahlungsströme ermöglichen.

Die frühe Erkennung von allgemeinen Geschäftsrisiken soll durch solide Verwaltungs- und Kontrollsysteme überwacht und gesteuert werden. Zu diesen Risiken gehören Verluste aus mangelhafter Umsetzung der Unternehmensstrategie, negativen Cashflows oder unerwarteten und übermäßig hohen Betriebskosten. Daneben wird für die Sicherstellung einer effektiven Risikominderung eine klare Trennung zwischen operationellem Risikomanagement und dem Funktionieren der internen Revision verlangt.

Leitlinie für das Privatkundengeschäft

9. Überwachung und Governance von Bankprodukten im Privatkundengeschäft: Ab dem 3. Januar 2017 gilt die Leitlinie (EBA/GL/2015/18) zur Überwachung und Governance von Bankprodukten im Privatkundengeschäft, die eine Umsetzungsfrist von eineinhalb Jahren hat. Die BaFin verkündete am 21. Juli 2017 den ersten Entwurf zur Umsetzung der Leitlinie und hatte bis zum 31. August 2017 zur Konsultation aufgerufen.

In den Anwendungsbereich dieser Regulierung fallen Verbraucherdarlehensverträge, Einlagen, Bausparverträge, Zahlungsdienste, E-Geld-Geschäfte und Zahlungskonten. Dabei gilt sie sowohl für neue als auch bereits existierende Pro-

dukte der Kreditinstitute. Die Leitlinie verlangt von den Banken zunächst, einen Zielmarkt für diese Produkte zu definieren. Dieser soll anhand des Risikogehalts des Produkts sowie der Merkmale des benötigten Wissensstandes, Verständnisses, der potenziellen Kreditwürdigkeit und der finanziellen Leistungsfähigkeit des Verbrauchers bestimmt werden.

Regelung für eine wirksame Überwachung und Steuerung

Parallel sollen die Kreditinstitute eine Regelung für eine wirksame Überwachung und Steuerung der Entwicklung und des Vertriebs der Finanzprodukte treffen (internes Kontrollsystem). Damit soll ein gewisses Sicherheitsniveau erreicht werden, um die Risiken abzuschwächen. Dieser Prozess soll sowohl in den Vertrieb der Finanzprodukte als auch in die bestehenden Mechanismen des Compliance- und Risikocontrollings integriert werden.

10. Verordnung zur Vereinheitlichung des Mindestangebots: Gestützt auf der Richtlinie 2014/92 über die Vergleichbarkeit von Zahlungskontoentgelten, die seit dem 18. September 2016 rechtsverbindlich ist, veröffentlichte das Europäische Parlament und der Rat am 28. September 2017 eine Verordnung zur Ergänzung der sogenannten Zahlungskonten-Richtlinie. Mit dieser Maßnahme hat das Europäische Parlament auf die Empfehlung der Europäischen Kommission reagiert und die Banken verpflichtet, mehr Transparenz bei Kontenentgelten und beim Wechsel von Konten zu schaffen. Die Vergleichbarkeit von Zahlungskontoentgelten, beim Wechsel von Zahlungskonten und Zugang zu Zahlungskonten mit grundlegenden Funktionen (Basiskonto/ Jedermann-Konto) wurden harmonisiert.

Zahlungsverkehr als kritische Dienstleistung eingestuft

Vor dem Hintergrund von unterschiedlichen Interpretationen von Begriffen sah sich die Kommission nun gezwungen, nachzubessern und eine standardisierte Unionsterminologie für diese Dienste festzulegen. Die neue Verordnung enthält daher Begriffsbestimmungen in sämtlichen Amtssprachen der zur EU gehörenden Mitgliedstaaten und definiert Begriffe wie Zahlungskonto, Entgelte, Kontoführung, Ausgabe einer Debitkarte, Überweisung oder Dauerauftrag.

11. IT-Sicherheitsgesetz: Bereits im Juli 2015 hat die Bunderegierung mit dem Gesetz zur Erhöhung der Sicherheit informationsrelevanter Systeme (IT-Sicherheitsgesetz) dazu beigetragen, die IT-Systeme und digitale Infrastrukturen in Deutschland sicherer zu machen. Den Fokus hat sie dabei auf die kritischen Infrastrukturen (KRITIS) gelegt, zu denen auch der Finanzsektor gehört. Denn ein Ausfall oder eine Beeinträchtigung der Versorgungsdienstleistung würde in diesem Segment zu schwerwiegenden Folgen für Staat, Gesellschaft und Wirtschaft führen.

Als weiteres Ziel verfolgt das IT-Sicherheitsgesetz die Verbesserung der IT-Sicherheit bei Unternehmen und der Bundesverwaltung. Die Sektoren Finanz- und Versicherungswesen wurden am 30. Juni 2017 durch eine Änderung zur ersten Verordnung in die BSI-Kritisverordnung aufgenommen. Im § 7 Abs. 1 der Änderung der Verordnung sind aufgrund ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens auch der Zahlungsverkehr (Bargeldversorgung, kartengestützter Zahlungsverkehr und konventioneller Zahlungsverkehr) als kritische Dienstleistung eingestuft worden. Damit haben die Kreditinstitute dafür Sorge zu tragen, dass ihre IT-Systeme den genannten Anforderungen der Verordnung nachkommen und das dauerhafte Funktionieren dieser Systeme sicherstellen.

12. NIS-Richtlinie: Neben dem IT-Sicherheitsgesetz tritt ab dem 9. Mai 2018 die NIS-Richtlinie (Netz- und Informationssysteme) in Kraft und soll ebenfalls die IT-Infrastruktur der verschiedenen EU-Länder auf ein einheitliches Niveau bringen. Die Richtlinie wurde am 6. Juni 2016 vom Europäischen Parlament und dem Rat verabschiedet.

Damit alle Risiken und Vorfälle berücksichtigt werden können, gilt die Richtlinie nicht nur für Anbieter digitaler Dienste, sondern auch für Betreiber wesentlicher Dienste. Als „wesentliche Dienste" sind die aus dem IT-Sicherheitsgesetz genannten „Kritischen Infrastrukturen" gemeint, etwa die Sektoren Banken, Energie, Finanzmarktinfrastruktur.

Gemeinsames Sicherheitsniveaus von Netz- und Informationssystemen

Das oberste Ziel der Kommission und des Rates ist das Sicherstellen eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen für das Funktionieren des Binnenmarkts. Dieses soll durch die Festlegung nationaler Strategien, Schaffung einer Kooperationsgruppe, Schaffung eines Netzwerks von Computer-Notfallteams (CRIRTS), Meldepflichten und Benennung von zentralen Anlaufstellen erreicht werden. Wie auch beim IT-Sicherheitsgesetz müssen Banken und Finanzdienstleister angemessene Sicherheitsmaßnahmen gemäß dem aktuellen Stand der Technik treffen, um erhebliche Ausfälle mit schwerwiegenden Auswirkungen im Finanzsektor zu vermeiden. Insbesondere sind Vorkehrungen im Hinblick auf Hackerangriffe und technische Ausfälle zu treffen, um das Ausmaß von möglichen Schäden zu begrenzen.

Daneben soll die Zusammenarbeit zwischen den EU-Mitgliedsstaaten verstärkt werden. Um einen Informationsaustausch zwischen den Mitgliedsstaaten zu ermöglichen, werden digitale Dienste verpflichtet Sicherheitsvorfälle zu melden.

13. BAIT: Im November vergangenen Jahres veröffentlichte die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ein Rundschreiben zu den Bankaufsichtlichen Anforderungen an die IT (BAIT). Diese dienten zur Konkretisierung der MaRisk in Sachen ordnungsmäßiger Geschäftsorganisation im Bereich der Informationstechnologie. Da die BAIT keine neuen Anforderungen enthält, sondern lediglich die bestehenden erläutert und konkretisiert, ist keine Umsetzungsfrist vorgesehen.

Das Rundschreiben ist in acht Themengebiete aufgeteilt (IT-Strategie, IT-Governance, Informationsrisikomanagement, Informationssicherheitsmanagement, Benutzerberechtigungsmanagement, IT-Projekte/Anwendungsentwicklung, IT-Betrieb und Auslagerungen) und knüpft unmittelbar an die Anforderungen der MaRisk an. Damit verfolgt die BaFin das Ziel, bei den Instituten einen verständlichen und flexiblen Rahmenplan an die Organisation der Informationstechnik (Basisinfrastruktur für fachliche und nichtfachliche Prozesse) zu schaffen und damit eine sichere Ausgestaltung der IT-Systeme zu gewährleisten. Darüber hinaus plant die BaFin in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Teil der KRITIS-Verordnung in die BAIT aufzunehmen.

Zudem ist es denkbar, dass ein Teil der in der PSD2 vorgesehenen Leitlinien ebenfalls die BAIT erweitern werden. Hier ist insbesondere die Leitlinie zu den „Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten" relevant. Diese enthält inhaltliche Überschneidungen zur BAIT in den Punkten IT-Governance und Auslagerungen.

Regelung von Outsourcing

14. Leitlinie zur Regelung von Outsourcing: In diesem Jahr plant die EZB in Zusammenarbeit mit der EBA eine Leitlinie für die Regelung des Outsourcings von Aktivitäten bei Großbanken in der Europäischen Union zur Konsultation zu stellen. Auf der Agenda des Dokuments stehen die Erwartungen an die Outsourcing-Vereinbarungen, das Risikomanagement, Governance, Überwachung und Verfahren des Outsourcings. Dieser Entwurf soll noch im Laufe des Jahres zur Konsultation gestellt werden. So geht es zumindest aus dem aktuellen Newsletter des Single Supervisory Mechanism der Europäischen Zentralbank hervor. Auch diese Inhalte dieser Leitlinie könnten demnächst in die BAIT aufgenommen werden.

Ein großer Teil der Regulierungsvorhaben der Europäischen Union ist besonders auf die Bereiche des Datenschutzes, des Risikomanagements und der IT ausgerichtet. Die mit Spannung erwartete EU-DSGVO ist bereits am 25. Mai in Kraft getreten und hatte einen enormen Umsetzungsaufwand inne.

Noch vor der EU-DSGVO ist am 9. Mai die NIS-Richtlinie in Kraft getreten, die eine einheitliche IT-Infrastruktur in den EU-Ländern schaffen soll. Im Zusammenhang mit weiteren Anpassungen der IT durch das IT-Sicherheitsgesetz oder den BAIT ist ein Trend der EU-Vorhaben erkennbar. Es soll zunehmend die IT und IT-Infrastruktur modernisiert werden, um weltweit wettbewerbsfähig zu bleiben und ein angemessenes Sicherheitsniveau zu erreichen.

Darüber hinaus ist das Ziel des Verbraucherschutzes weiterhin deutlich erkennbar. Auch in Zukunft ist damit zu rechnen, dass sich der Trend zur Regulierung fortsetzt. Das zeigen unter anderem aktuelle politische Debatten, die über die Digitalisierung und den E-Commerce geführt werden.

Swaantje Anneke Haß
Managing Consultant, PPI AG
Swaantje.Anneke.Hass@ppi.de

Swaantje Anneke Haß ist Zahlungsverkehrsexpertin bei der PPI AG für Inlandszahlungsverkehr und Regulierung. Neben dem bankfachlichen und betriebswirtschaftlichen Know-how verfügt sie als zertifizierte Testmanagerin über methodische Expertise sowie mehrjährige praktische Erfahrung in der Projektarbeit rund um den Zahlungsverkehr in Banken in Deutschland und Europa.

Nils Purwin
Managing Consultant, PPI AG
nils.purwin@ppi.de

Nils Purwin ist Zahlungsverkehrsexperte für In- und Auslandszahlungsverkehr, Regulierung und Compliance. Mit seinem juristischen und betriebswirtschaftlichen Hintergrund und seiner Erfahrung im internationalen Bankenumfeld liegen seine Beratungsschwerpunkte in der Analyse und Umsetzung von regulatorischen Anforderungen und der Durchsetzung von Finanzsanktionen.

Vladimir Bozok
Associate Consultant, PPI AG
vladimir.bozok@ppi.de

Vladimir Bozok verfügt auf Grund seiner Berufserfahrung Kenntnisse im Bankenumfeld und ist studierter Wirtschaftswissenschaftler mit dem Schwerpunkt Finance. Bei PPI ist er im Bereich Zahlungsverkehr tätig und beschäftigt sich mit Themen rund um Compliance und Regulierung.

ppi

PPI AG – Geschäftsstelle Frankfurt am Main
Wilhelm-Leuschner-Straße 79, 60329 Frankfurt am Main,
Telefon +49 69 2222942-0