International Cybersecurity Law Review (2024) 5:213–236
https://doi.org/10.1365/s43439-024-00121-5

ORIGINAL PAPER

Geteiltes Wissen, gestärkte Resilienz: Informationsaustausch über Cyberbedrohungen gemäß Art. 45 DORA

Gerd Waschbusch · Ben Schlenker

Eingegangen: 20. März 2024 / Angenommen: 11. April 2024 / Online publiziert: 3. Mai 2024

Zusammenfassung Die zunehmende Bedrohung durch Cyberangriffe stellt insbesondere die Finanzbranche vor große Herausforderungen. Der ab dem 17. Januar 2025 geltende Digital Operational Resilience Act (DORA) verpflichtet Finanzunternehmen in der EU daher zu einem umfassenden Management von IKT-Risiken, um ihre digitale operationale Resilienz zu stärken. Der Austausch von Informationen und Erkenntnissen über Cyberbedrohungen, insbesondere sogenannter Threat Intelligence, spielt eine zentrale Rolle beim Schutz vor Cyberangriffen. Der DORA fördert deshalb den europaweiten Informationsaustausch zwischen Finanzunternehmen durch die erstmalige Schaffung eines einheitlichen gesetzlichen Rahmens. Bisher findet ein solcher Austausch hauptsächlich auf nationaler Ebene statt. Dieser Beitrag beleuchtet den regulatorischen Rahmen für den Austausch von Informationen und Erkenntnissen über Cyberbedrohungen gemäß DORA. Berücksichtigt werden dabei insbesondere Interdependenzen zu dem Recht zum Schutz von Geschäftsgeheimnissen, dem Datenschutzrecht und dem Wettbewerbsrecht. Darüber hinaus werden bestehende Kooperationsformen vorgestellt, wie die Allianz für Cybersicherheit, der Verein Cyber Security Sharing and Analytics, die European Cloud User Coalition und die TIBER-DE Community.

Schlüsselwörter Cybersicherheit · DORA · Resilienz · Informationsaustausch · Threat intelligence · Horizontal-Leitlinien

✉ Gerd Waschbusch · Ben Schlenker
Lehrstuhl für Betriebswirtschaftslehre, insb. Bankbetriebslehre, Campus, Universität des Saarlandes, Postfach 151150, 66123 Saarbrücken, Deutschland
E-Mail: gerd.waschbusch@bank.uni-saarland.de

Ben Schlenker
E-Mail: ben.schlenker@bank.uni-saarland.de

Shared intelligence, enhanced resilience: sharing cyber threat information and intelligence under DORA

Abstract The escalating threat of cyberattacks poses significant challenges, particularly for the financial sector. The Digital Operational Resilience Act (DORA), which comes into force in the EU on January 17, 2025, therefore obliges financial entities to implement a comprehensive ICT risk management framework to bolster their digital operational resilience. The exchange of information and intelligence about cyber threats, in particular so-called threat intelligence, plays a central role in protecting against cyber attacks. DORA facilitates the Europe-wide exchange of information among financial entities by establishing a unified legal framework for the first time. Until now, this exchange has primarily occurred at the national level. This article explores the regulatory framework governing the exchange of cyber threat information and intelligence under DORA. Particular attention is paid to the interdependencies with trade secret protection law, data protection law, and competition law. Furthermore, existing cooperative frameworks are presented, including the Alliance for Cyber Security, the Cyber Security Sharing and Analytics Association, the European Cloud User Coalition, and the TIBER-DE Community.

Keywords Cyber security · DORA · Resilience · Information-sharing · Threat intelligence · Horizontal Cooperation Agreements

1 Einleitung

Der am 14. Dezember 2022 verabschiedete Digital Operational Resilience Act (DORA)[1] verpflichtet Finanzunternehmen[2] in der Europäischen Union zu einem umfassenden Management von Risiken der Informations- und Kommunikationstechnologie (IKT), von IKT-bezogenen Vorfällen sowie des IKT-Drittparteienrisikos.[3] Erklärtes Ziel ist die Vollharmonisierung der Anforderungen an das IKT-Risikomanagement im gesamten europäischen Finanzsektor.[4] Ab dem Jahr 2025 müssen die betroffenen Unternehmen – wie beispielsweise CRR-Kreditinstitute[5],

[1] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27. Dezember 2022, S. 1–79).

[2] In Art. 2 Abs. 1 Buchst. a bis t DORA werden die in den Anwendungsbereich des DORA fallenden Finanzunternehmen (engl. „financial entities“) enumerativ aufgelistet.

[3] Vgl. [23; 33; 70, S. 161]; *Wuermeling,* ZfgK 2022 [71, S. 1072, 1073].

[4] Vgl. ErwG 12 DORA.

[5] CRR-Kreditinstitute betreiben das Einlagengeschäft und zugleich das Kreditgeschäft. Vgl. Art. 3 Nr. 31 DORA i. V. m. Art. 4 Abs. 1 Nr. 1 CRR sowie § 1 Abs. 3d KWG.

[6] Betroffen sind Versicherungsunternehmen im Sinne von Art. 13 Nr. 1 Solvency II-Richtlinie. Vgl. Art. 2 Abs. 1 Buchst. n i. V. m. Art. 3 Nr. 47 DORA.

[7] Betroffen sind Schwarmfinanzierungsdienstleister im Sinne von Art. 2 Abs. 1 Buchstabe e SF-VO. Vgl. Art. 2 Abs. 1 Buchst. s i. V. m. Art. 3 Nr. 58 DORA.

Versicherungsunternehmen[6] oder Schwarmfinanzierungsdienstleister[7] – daher einen umfassenden IKT-Risikomanagementrahmen einrichten und umsetzen. Neben zahlreichen weiteren Pflichten[8] soll die digitale Resilienz im Finanzsektor auch durch einen Informationsaustausch zwischen den in den Anwendungsbereich der Verordnung fallenden Finanzunternehmen gesteigert werden. Dieser Beitrag liefert einen Überblick über die Relevanz eines solchen Informationsaustauschs sowie die organisatorischen und rechtlichen Anforderungen an diesen gemäß Art. 45 DORA.

2 Grundlegender Regelungsgehalt des Art. 45 DORA

2.1 Inhalte des Informationsaustauschs: Cyber Threat Intelligence

Gemäß Art. 45 Abs. 1 DORA können Finanzunternehmen Informationen und Erkenntnisse über Cyberbedrohungen auf freiwilliger Basis untereinander austauschen. Der Begriff „Cyberbedrohung" i. S. d. Verordnung bezeichnet einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netzwerk- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.[9]

Die häufigsten (externen) Cyberbedrohungen in der Europäischen Union sind Ransomware-Angriffe und Denial-of-Service-Angriffe (DoS-Attacken).[10] Bei einem Angriff mittels Ransomware übernimmt „ein Angreifer die Kontrolle über ein Asset[11] und fordert Lösegeld als Gegenleistung für die Wiederherstellung der Verfügbarkeit[12] und Vertraulichkeit[13] des Assets."[14] Bei einer DoS-Attacke werden mit einer Flut an Anfragen IKT-Systeme überlastet, sodass die Verfügbarkeit der Systeme bzw. Daten eingeschränkt oder nicht mehr gegeben ist.[15]

Mögliche Inhalte für einen Informationsaustausch über Cyberbedrohungen zwischen Finanzunternehmen sind:

[8] Vgl. ausführlich *Clausmeier,* ICLR 2023 [19, S. 79]; [70].

[9] Vgl. Art. 3 Nr. 12 DORA i. V. m. Art. 2 Nr. 8 CSA.

[10] Vgl. [30, S. 9].

[11] Ein Informationsasset ist gemäß Art. 3 Nr. 6 DORA eine Sammlung materieller oder immaterieller Informationen, die schützenswert ist. Ein IKT-Asset ist gemäß Art. 3 Nr. 7 DORA eine Software oder Hardware in den von einem Finanzunternehmen genutzten Netzwerk- und Informationssystemen.

[12] „Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendenden stets wie vorgesehen genutzt werden können." [17, Glossar, S. 8].

[13] „Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein." [17, Glossar, S. 8].

[14] [29, S. 8]. Vgl. ferner *Sohr/Kemmerich*, in: Kipker, Cybersecurity [60, Kapitel 3., Rn. 177].

[15] Vgl. [17, SYS.1.1, S. 3]; *Sohr/Kemmerich*, in: Kipker, Cybersecurity [60, Kapitel 3., Rn. 181].

- Kompromittierungsindikatoren (engl. Indicators of compromise, IoC),[16]
- (neue) Angriffsarten,
- Taktiken, Techniken und Verfahren (engl. Tactics, Techniques and Procedures, TTPs) der Angreifer,[17]
- Mechanismen eines Angriffs,[18]
- Häufigkeit, Dauer und Herkunft von Cyberangriffen,
- die für einen Angriff Verantwortlichen und ihre Beweggründe,[19]
- Sicherheitswarnungen und Hinweise auf Sicherheitslücken[20] sowie
- effektive Gegenmaßnahmen bzw. Best Practices.[21]

Ein Großteil dieser Inhalte kann unter dem Begriff „Cyber Threat Intelligence" (CTI) zusammengefasst werden. Darunter versteht man eine Sammlung evidenzbasierter Informationen über Cyberbedrohungen, welche zuvor von Experten geordnet, bewertet und analysiert wurden.[22] Bei einer Cyber-Bedrohungsdatenanalyse „machen sich Cyber-Sicherheitsteams historische Daten über Motive, Ziele und das Angriffsverhalten von Cyber-Bedrohungsakteuren zunutze, um proaktive, Erkenntnis gestützte Sicherheitsentscheidungen zu treffen, Anpassungen in Konfigurationen vorzunehmen und angewendete Cyber-Abwehrstrategien nachzujustieren."[23]

2.2 Grundsätzliche Bedingungen des Informationsaustauschs

Der europäische Gesetzgeber hat in Art. 45 Abs. 1 DORA drei wesentliche Bedingungen formuliert, welche die Finanzunternehmen beim Austausch von Informationen und Erkenntnissen (engl. cyber threat information and intelligence) einhalten müssen.

Gemäß der ersten Bedingung muss der Austausch darauf abzielen, die digitale operationale Resilienz der Finanzunternehmen zu stärken. Dazu soll er beispielsweise das Bewusstsein für Cyberbedrohungen steigern. Der Austausch von Informationen über Cyberbedrohungen soll dabei helfen, deren Verbreitung einzuschränken bzw. zu verhindern. Darüber hinaus könnten mögliche austauschbare Erkenntnis-

[16] Vgl. Art. 45 Abs. 1 DORA. Hierzu zählt beispielsweise ein verdächtiger DNS-Domänenname, eine Datei-Hash für eine bösartige ausführbare Datei oder die Betreffzeile einer bösartigen E-Mail-Nachricht. Vgl. [42, S. 2].

[17] Vgl. Art. 45 Abs. 1 DORA. TTPs beschreiben das Verhalten und Vorgehen eines Angreifers, indem sie beispielsweise die typische Reihenfolge von Operationen eines bestimmten Angreifers bei seinen Attacken darstellen. Vgl. [42, S. 2].

[18] Vgl. [65].

[19] Vgl. Art. 3 Nr. 15 DORA.

[20] Vgl. Art. 45 Abs. 1 DORA; [42, S. 2].

[21] Vgl. zu dieser Aufzählung insbesondere [42, S. 2–3].

[22] Vgl. [42, S. 2; 65]. Art. 3 Nr. 15 DORA definiert Threat Intelligence i. S. d. DORA als, „Informationen, die aggregiert, umgewandelt, analysiert, ausgewertet oder erweitert wurden, um den notwendigen Kontext für die Entscheidungsfindung zu schaffen und ein relevantes und ausreichendes Verständnis für die Abmilderung der Auswirkungen eines IKT-bezogenen Vorfalls oder einer Cyberbedrohung zu ermöglichen, einschließlich der technischen Einzelheiten eines Cyberangriffs, der für den Angriff verantwortlichen Personen und ihres Modus Operandi und ihrer Beweggründe."

[23] *Bausewein*, in: Bernzen/Fritzsche/Heinze/Thomsen, Herbstakademie 2023 [10, S. 317].

se dazu beitragen, die Verteidigungsfähigkeit, die Techniken zur Erkennung von Bedrohungen, die Abmilderungsstrategien oder die Reaktions- und Wiederherstellungsverfahren der Finanzunternehmen zu verbessern.[24]

Der Austausch von Informationen und Erkenntnissen muss gemäß der zweiten Bedingung innerhalb vertrauenswürdiger Gemeinschaften von Finanzunternehmen erfolgen.[25] Der Begriff der „vertrauenswürdigen Gemeinschaft" ist nicht im DORA definiert. Ihre Ausgestaltung ergibt sich durch die nachfolgend erläuterten Anforderungen.

Die dritte und letzte Bedingung betrifft die Ausgestaltung der Vereinbarungen zum Austausch innerhalb von vertrauenswürdigen Gemeinschaften. Diese Vereinbarungen sind so zu gestalten, dass der potenziell sensible Charakter der Informationen beim Austausch geschützt wird. Zudem sollen sie Verhaltensregeln unterliegen, durch die Geschäftsgeheimnisse weiterhin gewahrt, personenbezogene Daten geschützt und das Wettbewerbsrecht eingehalten wird.[26]

Die Voraussetzungen zum Beitritt und der Teilnahme an einer vertrauenswürdigen Gemeinschaft müssen zuvor festgelegt werden. Ebenso sind eine eventuelle Einbindung von Behörden oder IKT-Drittdienstleistern zu regeln. Neben diesen formellen Aspekten sind ebenso operative Aspekte zu regeln, wie beispielsweise die Nutzung spezieller IT-Plattformen zum Informationsaustausch.[27]

Finanzunternehmen müssen den für sie zuständigen Aufsichtsbehörden mitteilen, wenn sie tatsächlich einer vertrauenswürdigen Gemeinschaft zum Austausch von Informationen und Erkenntnissen beitreten bzw. aus ihr austreten. Maßgeblich ist der Tag des Inkrafttretens des Eintritts bzw. Austritts.[28]

3 Relevanz des Informationsaustauschs über Cyberbedrohungen

Unter den zuvor erläuterten Bedingungen ist ein Informationsaustausch zwischen Finanzunternehmen ausdrücklich erlaubt. Gemäß ErwG 34 DORA sollen Finanzunternehmen sogar ermutigt werden, einen solchen Austausch verstärkt durchzuführen. Durch den Informationsaustausch soll das Problembewusstsein (Awareness) für Cyberbedrohungen geschärft werden.[29] Hierdurch wird wiederum die Cyber-Resilienz der Finanzunternehmen verbessert. Das heißt, die Fähigkeiten zur Abwehr bzw. Verhinderung des Eintretens von Cyberbedrohungen sowie die Fähigkeiten zur

[24] Vgl. zu diesem Absatz Art. 45 Abs. 1 Buchst. a DORA.

[25] Vgl. Art. 45 Abs. 1 Buchst. b DORA.

[26] Vgl. zu diesem Absatz Art. 45 Abs. 1 Buchst. c DORA.

[27] Vgl. zu diesem Absatz Art. 45 Abs. 2 DORA.

[28] Vgl. zu diesem Absatz Art. 45 Abs. 3 DORA.

[29] Vgl. ErwG 32 DORA; *Brabetz,* bank und markt 2023 [14, S. 312, 314].

(schnellen) Reaktion und Wiederherstellung[30] bei IKT-bezogenen Vorfällen[31] werden gestärkt.[32] Durch einen schnellen und unkomplizierten Austausch bei einem laufenden Cyberangriff können andere Unternehmen frühzeitig gewarnt werden und diese können zielgerichtete Gegenmaßnahmen ergreifen.[33]

Generell kann der Austausch von Informationen zu unterschiedlichen Effizienzgewinnen führen, beispielsweise durch das Beheben von Informationsasymmetrien[34] oder den Abgleich von internen Prozessen, um Verbesserungsmöglichkeiten abzuleiten.[35] Unternehmen, die am Informationsaustausch teilnehmen, können neue Informationen und Erkenntnisse gewinnen, die ihnen ohne einen solchen Austausch möglicherweise nicht zur Verfügung stehen.[36] Das Aufdecken einer Bedrohung durch ein Unternehmen kann so zur Prävention in einem anderen Unternehmen beitragen.[37] Beispielsweise könnte durch den Abgleich mit Schadsoftware, die bereits von anderen Unternehmen erkannt wurde, bisher unentdeckte Schadsoftware im unternehmenseigenen IKT-System früher identifiziert und bekämpft werden.[38] „Nur durch Kooperation und das Teilen von Informationen können die Unternehmen den professionell und zum Teil auch arbeitsteilig organisierten Angreifern zuvorkommen und sich wirksam schützen."[39]

Der europäische Gesetzgeber merkt in ErwG 32–33 DORA an, dass ein Informationsaustausch auf europäischer Ebene aufgrund mehrerer Faktoren bisher selten stattgefunden hat. Als mögliche Gründe dafür führt er unter anderem Unsicherheiten der Unternehmen hinsichtlich der Vereinbarkeit eines Informationsaustauschs mit Datenschutz-, Kartell- und Haftungsvorschriften an.[40] Auf nationaler Ebene existieren allerdings bereits einige freiwillige bzw. verpflichtende Initiativen für den Informationsaustausch im Bereich der Cybersicherheit.[41] So gab es im Jahr 2018 bei 75% der 28 Mitglieder[42] des Basel Committee on Banking Supervision (BCBS)

[30] Geregelt in Art. 11 DORA.

[31] Gemäß Art. 3 Nr. 1 DORA ist ein IKT-bezogener Vorfall „ein von dem Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, das bzw. die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt und nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzunternehmen erbrachten Dienstleistungen hat."

[32] Vgl. zu den letzten beiden Sätzen ErwG 32 DORA. Vgl. ferner *Clausmeier,* ICLR 2023 [19, S. 79, 86].

[33] Vgl. *Krautscheid/Nash,* BaFin Perspektiven 2020 [44, S. 35, 38].

[34] „Die Wirtschaftstheorie der Informationsasymmetrien beschäftigt sich mit der Untersuchung von Entscheidungen in Situationen, in denen eine Partei über mehr Informationen verfügt als die andere." Fn. 7 zu Rn. 373 Horizontal-LL.

[35] Vgl. Rn. 373 Horizontal-LL.

[36] Vgl. [42, S. 3].

[37] Auf englisch: Threat information sharing „enables one organization's detection to become another organization's prevention." *Sager* zitiert in [42, S. 3].

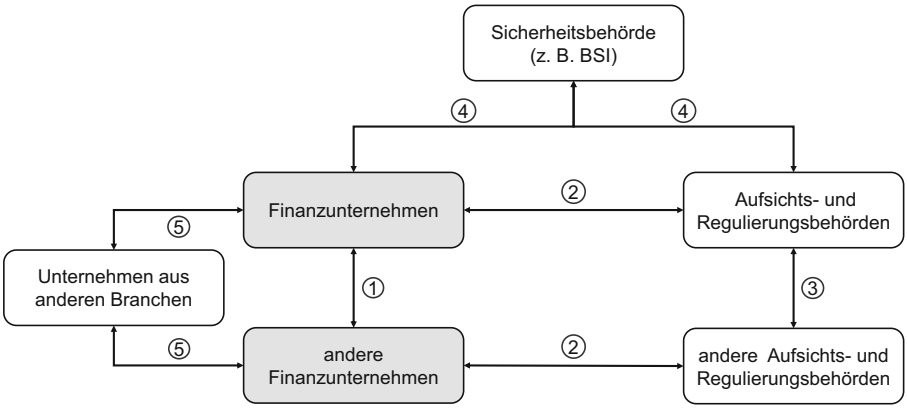
[38] Vgl. *Krautscheid/Nash,* BaFin Perspektiven 2020 [44, S. 35, 38].

[39] *Balz/Sinn,* ZfgK 2023 [9, S. 222, 224].

[40] Vgl. zu den letzten beiden Sätzen ErwG 32 DORA. Vgl. ebenso *Krautscheid/Nash,* BaFin Perspektiven 2020 [44, S. 35, 39].

[41] Vgl. ferner ErwG. 33 DORA.

[42] Acht Mitglieder des BCBS sind EU-Mitgliedstaaten und die EU selbst ist auch Mitglied des BCBS.



①	Austausch zwischen Finanzunternehmen
②	Austausch zwischen Finanzunternehmen sowie Aufsichts- und Regulierungsbehörden
③	Austausch zwischen Aufsichts- und Regulierungsbehörden
④	Austausch mit Sicherheitsbehörden
⑤	Sektorübergreifender Austausch

Abb. 1 Arten des Informationsaustauschs. (Eigene Darstellung in Anlehnung an [11, S. 22])

zumindest eine Art von Austausch über Cyber Threat Intelligence zwischen Banken untereinander.[43] In Brasilien, Japan und Saudi-Arabien war dieser Austausch zum damaligen Zeitpunkt sogar verpflichtend.[44]

Abb. 1 zeigt verschiedene Möglichkeiten der Gestaltung eines Informationsaustauschs. Dieser Beitrag konzentriert sich auf den Austausch zwischen Finanzunternehmen (in der Abb. 1 markiert mit ①).

4 Bestehende Beispiele für einen sektorübergreifenden Informationsaustausch

In Deutschland gibt es unter anderem bereits die Zusammenschlüsse „Allianz für Cyber-Sicherheit“ und „Cyber Security Sharing and Analytics e. V.“, in denen ein – allerdings sektorübergreifender – Austausch über Informationssicherheitsthemen und Cyberbedrohungen stattfindet.[45] Die Allianz für Cyber-Sicherheit wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (bitkom) im Jahr 2012 gegründet. Sie dient als Austauschplattform für Unternehmen, Verbände, Behörden und Organisationen über aktuelle Cyberbedrohungen und

[43] Vgl. [11, S. 23].

[44] Vgl. [11, S. 24].

[45] Vgl. ebenso *Brisch/Rexin,* CR 2019 [15, S. 606, Rn. 35].

Cybersicherheitsmaßnahmen.[46] Zurzeit hat die Allianz über 7200 Teilnehmer, darunter sind auch zahlreiche deutsche Finanzunternehmen.[47] Innerhalb der Allianz verschickt das BSI beispielsweise aktuelle Cybersicherheitswarnungen sowie regelmäßige Lageberichte zur aktuellen Bedrohungslage.[48]

In dem im Jahr 2014 gegründeten Verein „Cyber Security Sharing and Analytics" (CSSA) haben sich überwiegend weltweit tätige Wirtschaftsunternehmen zusammengeschlossen, „die über Inhouse CyberSecurity-Ressourcen verfügen und sowohl die Bereitschaft als auch die Fähigkeit besitzen, relevante Informationen über Cyber-Angriffe und -Bedrohungen unter Gleichgesinnten zu teilen."[49] Der Verein hat zurzeit 16 Mitgliedsunternehmen, darunter sind der Versicherungskonzern Allianz SE, die Deutsche Bank AG und die Finanz Informatik GmbH & Co. KG.[50]

Hauptziel des Vereins ist es, einen branchenübergreifenden vertraulichen Austausch zu Informationssicherheitsvorfällen, -Bedrohungen und -Schwachstellen zwischen den mit dem Thema Informationssicherheit betrauten Mitarbeitern und externen Experten zu ermöglichen. Dadurch sollen Cyberbedrohungen proaktiv, schneller und wirksamer bekämpft werden können. Des Weiteren erfolgt ein technischer Austausch von Threat Intelligence über eine Sharing-Plattform und in Data Analytics-Projekten. Darüber hinaus wird regelmäßig ein Lagebericht für die Chief Information Security Officer (CISOs) der beteiligten Unternehmen und für weitere interessierte Mitarbeiter erstellt.[51]

CSSA setzt zur Realisierung eines sicheren Austauschs die Software MISP Threat Sharing (MISP) ein. Auf dieser Open-Source-Threat-Intelligence-Plattform können Gefährdungsindikatoren, Threat Intelligence sowie Informationen über Finanzbetrug, Schwachstellen oder Terrorismusbekämpfung gespeichert und ausgetauscht werden. Außerdem kann die Software automatisiert nach Verbindungen und Mustern zwischen den gespeicherten Merkmalen und Indikatoren von Schadsoftware, Angriffskampagnen oder Analysen suchen. Mit Hilfe der Plattform soll die Effizienz „von reaktiven Gegenmaßnahmen gegen gezielte Angriffe"[52] gesteigert werden. Weiterhin soll sie präventive Maßnahmen fördern und das Aufdecken von Cyberbedrohungen erleichtern. Die Open-Source-Software wurde unter anderem von der Europäischen Union finanziert. Sie wird beispielsweise auch von der NATO eingesetzt.[53]

[46] Vgl. zu den letzten beiden Sätzen [5, S. 6–10]; *Wunderlich*, in: Bartsch/Frey [72, S. 66–67].

[47] Vgl. [4].

[48] Vgl. *Wunderlich*, in: Bartsch/Frey [72, S. 70].

[49] [20].

[50] Vgl. [21]. Die Finanz Informatik GmbH & Co. KG ist der IT-Dienstleister der Sparkassen-Finanzgruppe.

[51] Vgl. zu diesem Absatz [20; 21, S. 1].

[52] *Brisch/Rexin,* CR 2019 [15, S. 606, Rn. 40].

[53] Vgl. zu diesem Absatz *Brisch/Rexin,* CR 2019 [15, S. 606, Rn. 39–41]; [18; 20; 51].

5 Regulatorische Herausforderungen beim Informationsaustausch

5.1 Recht zum Schutz von Geschäftsgeheimnissen

Gemäß Art. 45 Abs. 2 DORA sollen die Vereinbarungen zum Informationsaustausch Verhaltensregeln unterliegen, um die Einhaltung der Regulatorik zu den drei Rechtsgebieten Geschäftsgeheimnisschutz, Datenschutz und Wettbewerbsrecht zu gewährleisten. Welche Vorgaben die jeweiligen Rechtsakte machen und wie sie eingehalten werden können, wird im Folgendem untersucht.

Beim Austausch von Informationen und Erkenntnissen über Cyberbedrohungen sollen Finanzunternehmen die europarechtlichen Vorgaben im Hinblick auf den Schutz von Geschäftsgeheimnissen einhalten.[54] Die nicht unmittelbar geltende Richtlinie zum Schutz von Geschäftsgeheimnissen[55] wurde im deutschen Recht durch das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) umgesetzt.

Ein Geschäftsgeheimnis i. S. d. § 2 Nr. 1 GeschGehG ist eine nicht allgemein bekannte (das heißt eine geheime) Information mit einem wirtschaftlichen Wert, für die deren Inhaber angemessene Geheimhaltungsmaßnahmen ergreift und ein berechtigtes Interesse an dessen Geheimhaltung besitzt.[56] Sowohl (geheime) Daten in Datensätzen bzw. -banken als auch Rohdaten haben i. d. R. einen gewissen Informationsgehalt und können daher geschützte Geschäftsgeheimnisse darstellen.[57] Auch die Schutzwürdigkeit von Zugangsdaten, Algorithmen oder Prozessabläufen ist grundsätzlich zu bejahen.[58] Außerdem kann die Kenntnis über eine (eigene) Informationssicherheitslücke ein geschütztes Geschäftsgeheimnis darstellen.[59] Ein solches Wissen über eine Gefahr bzw. ein Risiko stellt eine „negative" Information dar, die grundsätzlich ebenfalls durch das GeschGehG geschützt wird.[60]

Die Ausgestaltung des gemäß Art. 6 DORA einzurichtenden IKT-Risikomanagementrahmens stellt ebenso ein Geschäftsgeheimnis dar.[61] Finanzunternehmen sollen im Rahmen des IKT-Risikomanagements Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und -Tools entwickeln, um die Informationssicherheit und

[54] Vgl. Art. 45 Abs. 1 Buchst. c DORA.

[55] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (ABl. L 157 vom 15. Juni 2016, S. 1–18).

[56] Vgl. ausführlich § 2 Nr. 1 GeschGehG; *Alexander*, in: Köhler/Bornkamm/Feddersen [3, GeschGehG § 2, Rn. 8–88a]; *Lang/Bollinger,* WM 2022 [47, S. 2218, 2219]; *Renner,* in: BeckOK IT-Recht [55, GeschGehG § 2, Rn. 1–43.1]; *Ziechnaus,* ZfgK 2019 [73, S. 1053, 1053–1054].

[57] Vgl. *Renner,* in: BeckOK IT-Recht [55, GeschGehG § 2, Rn. 8].

[58] Vgl. *Krüger/Wiencke/Koch,* GRUR 2020 [46, S. 578, 583]; *Renner,* in: BeckOK IT-Recht [55, GeschGehG § 2, Rn. 8].

[59] Vgl. *Renner,* in: BeckOK IT-Recht [55, GeschGehG § 2, Rn. 9].

[60] Vgl. *Alexander*, in: Köhler/Bornkamm/Feddersen [3, GeschGehG § 2, Rn. 28]; *Glinke*, in: Keller/Schönknecht/Glinke [32, Rn. 52]; [40, Rn. 2.29]; *Hoppe/Momtschilow/Lodemann/Tholuck*, in: Hoppe/Oldekop [41, Rn. 97]; *Renner,* in: BeckOK IT-Recht [55, GeschGehG § 2, Rn. 9]; *Sousa e Silva,* JIPLP 2014 [61, S. 923, 931–932].

[61] Vgl. zur Schutzwürdigkeit von „IT-Sicherheitsmaßnahmen und -konzepten" *Renner,* in: BeckOK IT-Recht [55, GeschGehG § 2, Rn. 8].

die digitale Resilienz ihrer Informations- und IKT-Assets sowie ihrer Infrastruktur zu gewährleisten.[62] Bei dem gemäß Art. 45 DORA angedachten Austausch über solche (Informationssicherheits-)Konzepte sind daher Maßnahmen zu ergreifen, um diese Geschäftsgeheimnisse zu wahren.

Ein sinnvoller und i. d. R. unabdingbarer Ansatz zur Wahrung der Geschäftsgeheimnis-Compliance, die ein kompliziertes Querschnittsthema darstellt, ist die Etablierung eines konsistenten unternehmensweiten Geheimnisschutzkonzepts bzw. Geschäftsgeheimnis-Management(-Systems). Es besteht aus einer Kombination aus technisch-organisatorischen und personellen Maßnahmen sowie juristischen Vorgaben zum Informations- bzw. Geheimnisschutz.[63] Bereits grundlegende Informationssicherheitsmaßnahmen, wie sie gemäß DORA oder den Bankaufsichtlichen Anforderungen an die IT (BAIT[64]) zu ergreifen sind, schützen auch Geschäftsgeheimnisse. Beispielhaft für solche Maßnahmen sind die Zugangsbeschränkung und -kontrolle von Infrastruktur, Systemen und Daten sowie die Verschlüsselung von Daten und Verbindungen.[65] Ergreifen Unternehmen keine oder nur unzureichende Schutzmaßnahmen, verlieren sie den gesetzlich vorgesehenen Schutz für ihre Geschäftsgeheimnisse.[66] Die Satzung des CSSA verpflichtet deshalb Vereinsmitglieder dazu, gewissenhaft mit als vertraulich gekennzeichneten Informationen umzugehen, das heißt diese Geschäftsgeheimnisse nicht gegen andere Mitglieder einzusetzen und nicht an Dritte weiterzugeben.[67]

5.2 Datenschutzrecht

Neben Geschäftsgeheimnissen sind beim Informations- und Erkenntnisaustausch auch personenbezogene Daten[68] zu schützen. Beim Austausch von Cyber Threat Intelligence können unter anderem Daten über Angreifer oder Opfer – das heißt z. B. E-Mail-Adressen, MAC-Adressen oder IP-Adressen – unter die Kategorie personenbezogene Daten i. S. d. Art. 4 Nr. 1 DS-GVO fallen.[69] So könnte bei der Analyse eines konkreten Phishing-Angriffs neben dem Inhalt der E-Mail auch die E-Mail-

[62] Vgl. Art. 6 Abs. 2 DORA.

[63] Vgl. zu den letzten beiden Sätzen *Ann,* GRUR 2014 [6, S. 12, 14]; *Harte-Bavendamm*, in: Harte-Bavendamm/Ohly/Kalbfus [34, GeschGehG § 2, Rn. 55]; *Hiéramente/Golzio,* CCZ 2018 [38, S. 262, 266–267]; *Höfer,* GmbHR 2018 [39, S. 1195, 1196–1197]; *Lang/Bollinger,* WM 2022 [47, S. 2218, 2222]; *Ohly,* GRUR 2019 [53, S. 441, 444]; *Voigt/Herrmann/Grabenschröer,* BB 2019 [66, S. 142, 144–145]; *Ziechnaus,* ZfgK 2019 [73, S. 1053, 1054].

[64] Siehe Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021 (https://www.bafin.de/ref/19595164).

[65] Vgl. zu den letzten beiden Sätzen *McGuire,* IPRB 2018 [49, S. 202, 205]; *Voigt/Herrmann/Grabenschröer,* BB 2019 [66, S. 142, 145].

[66] Vgl. *Ziechnaus,* ZfgK 2019 [73, S. 1053, 1054].

[67] Vgl. [21, S. 3].

[68] Gemäß Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

[69] Vgl. *Albakri/Boiten/Lemos*, in: ARES 2018 [1, S. 3]; *Albakri/Boiten/Lemos,* APF 2019 [2, S. 28]. Vgl. ausführlich zur umstrittenen Frage, ob und wie bei Online-Kennungen eine Identifizierbarkeit einer Person vorliegen kann, *Arning/Rothkegel*, in: Taeger/Gabel [7, DS-GVO Art. 4, Rn. 27] (m. w. N.).

Adresse des Empfängers (z. B. eines Kunden oder Mitarbeiters) absichtlich oder unabsichtlich zwischen den Experten ausgetauscht werden.

Der Austausch über Cyberbedrohungen soll im Einklang mit den Vorgaben der Datenschutzgrundverordnung (DS-GVO) erfolgen.[70] Grundsätzlich dürfen personenbezogene Daten nur verarbeitet werden, wenn dies „auf rechtmäßige Weise" (im engeren Sinne) geschieht, das heißt mindestens einer der in Art. 6 Abs. 1 UAbs. 1 DS-GVO aufgeführten Erlaubnisgründe für die in Frage stehende Verarbeitung zutrifft.[71] Bei einem Informationsaustausch erfolgt eine Verarbeitung i. S. d. Art. 4 Nr. 2 DS-GVO unter anderem in Form einer Speicherung, Verbreitung oder Verwendung.

Als Rechtsgrundlage der Verarbeitung kommen weder die Erfüllung einer konkreten rechtlichen Verpflichtung (Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO), der Schutz lebenswichtiger Interessen in Notlagen (Art. 6 Abs. 1 UAbs. 1 Buchst. d DS-GVO) noch die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO), in Betracht. Auch ist der Informationsaustausch i. d. R. nicht unmittelbar zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich (Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO). Sofern keine Einwilligung (Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO) in die Verarbeitung vorliegt, ist eine Verarbeitung im Rahmen eines Informationsaustauschs deshalb regelmäßig nur rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des verantwortlichen Unternehmens oder eines Dritten erforderlich ist (Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO).[72]

Für diesen Fall muss, sofern ein berechtigtes Interesse des Verantwortlichen an der Verarbeitung besteht, eine Interessenabwägung mit dem entgegenstehenden Interesse des Betroffenen erfolgen, insoweit auch dieses besteht.[73] Es kommen grundsätzlich jedwede rechtlichen, wirtschaftlichen oder ideellen Interessen in Betracht.[74] Die Interessenabwägung fällt zu Gunsten des Betroffenen aus, wenn seine Interessen oder Grundrechte und Grundfreiheiten, die den Schutz personenbezogener Daten erfordern, überwiegen.[75] Bei der Feststellung der einer Verarbeitung möglicherweise entgegenstehenden Interessen ist auf die objektivierbaren Interessen der von der Verarbeitung typischerweise betroffenen Personen abzustellen.[76] Das berechtigte Interesse der Finanzunternehmen besteht hier unter anderem darin, die

[70] Vgl. Art. 45 Abs. 1 Buchst. c DORA.

[71] Vgl. Art. 5 Abs. 1 Buchst. a i. V. m. Art. 6 Abs. 1 UAbs. 1 DS-GVO. Vgl. ausführlich *Herbst*, in: Kühling/Buchner [36, DS-GVO Art. 5, Rn. 8–12].

[72] Vgl. *Voskamp/Klein*, in: Kipker, Cybersecurity [67, Kapitel 7., S. 295]; *Albakri/Boiten/Lemos*, in: ARES 2018 [1, S. 3]. ErwG 34 DORA führt die Rechtsgrundlagen gemäß Buchst. c und e DS-GVO ebenso als mögliche Erlaubnistatbestände an. Da aber weder eine konkrete Verpflichtung zum Informationsaustausch mit Art. 45 DORA besteht noch eine Aufgabenübertragung auf die Finanzunternehmen ersichtlich vorliegt, kommen diese Rechtsgrundlagen für die Verarbeitung im Rahmen eines Informationsaustausches nicht in Betracht.

[73] Vgl. *Borges/Steinrötter,* in: BeckOK IT-Recht [13, DS-GVO Art. 6, Rn. 44–46].

[74] Vgl. *Schulz*, in: Gola/Heckmann [59, DS-GVO Art. 6, Rn. 61].

[75] Vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO.

[76] Vgl. *Taeger*, in: Taeger/Gabel [64, DS-GVO Art. 6, Rn. 140]; *Borges/Steinrötter,* in: BeckOK IT-Recht [13, DS-GVO Art. 6, Rn. 50–52].

Informationssicherheit zu gewährleisten bzw. zu erhöhen.[77] Dies liegt grundsätzlich auch im Interesse des betroffenen Kunden. Dem entgegen stehen jedoch „jene Grundrechte und Grundfreiheiten, die den Schutz der personenbezogenen Daten gebieten“[78] – das heißt insbesondere Art. 7 und Art. 8 GRCh – sowie die Interessen des Betroffenen, dass seine (Finanz-)Daten nicht mit Unternehmen geteilt werden, mit denen er in keinerlei vertraglichem Verhältnis steht. Hinzu kommt, dass eine Verarbeitung konkreter Kundendaten i. d. R. nicht erforderlich zum Informationsaustausch bzw. zum Ergreifen von Informationssicherheitsmaßnahmen ist. Insofern dürfen personenbezogene Daten von Kunden nicht im Rahmen des Informationsaustauschs über Cyberbedrohungen ausgetauscht werden, dies gilt insbesondere für deren Kontakt- und Finanzdaten.

Fraglich ist, ob personenbezogene Daten von Angreifern ausgetauscht werden dürften.[79] Da dem Wortlaut des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO nach bei der Interessenabwägung nur auf Interessen des Betroffenen und nicht explizit auf „berechtigte“[80] Interessen des Betroffenen abgestellt wird, geht eine Ansicht davon aus, dass auch „illegitime“ Interessen[81] des Betroffenen zu berücksichtigen sind.[82] „Selbst Personen, die rechtswidrige Handlungen begehen, sollten keinen unverhältnismäßigen Eingriffen in ihre Rechte und Interessen ausgesetzt werden.“[83] Die Grundrechte des Angreifers und das „illegitime“ Interesse, einen Cyberangriff erfolgreich durchzuführen, ohne gestört bzw. danach (strafrechtlich) verfolgt zu werden, sind in einer Interessenabwägung allerdings wohl den berechtigten Interessen des Opfers unterlegen, weitere Angriffe durch einen Informationsaustausch über den Angreifer zu verhindern. Abzulehnen ist allerdings eine Verarbeitung mit Prangerwirkung.[84]

Auch wenn der überwiegende Teil der Informationen beim Austausch über Cyberbedrohungen keinen Personenbezug haben dürfte, sollte dies aus datenschutzrecht-

[77] Für die Verarbeitung von personenbezogenen Daten zur Abwehr von Cyberbedrohungen durch Behörden, Computer Emergency Response Teams und anderen ist das Bestehen dieses berechtigten Interesses des Verantwortlichen in ErwG 49 DS-GVO ausdrücklich festgehalten, sofern die Verarbeitung zur Gewährleistung der Netzwerk- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist. Vgl. ausführlich *Spindler/Dalby*, in: Spindler/Schuster [62, DS-GVO Art. 6, Rn. 15].

[78] *Spindler/Dalby*, in: Spindler/Schuster [62, DS-GVO Art. 6, Rn. 17].

[79] Das Vorliegen personenbezogener Daten des Angreifers dürfte eher selten vorkommen, da die Angreifer natürlich versuchen, ihre Identität zu verschleiern, bspw. durch eine gefälschte IP-Adresse beim IP-Spoofing.

[80] Im englischen Wortlaut wird für den Begriff „berechtigt“ der Begriff „legitimate“ (deutsch: berechtigt/legitim/rechtmäßig) verwendet. Vgl. *Robrahn/Bremert,* ZD 2018 [56, S. 291].

[81] Gemeint sind „in der Sache verwerfliche oder zu missbilligende Interessen“. *Schulz*, in: Gola/Heckmann [59, DS-GVO Art. 6, Rn. 62].

[82] So [8, S. 38]; *Heberlein*, in: Ehmann/Selmayr [35, DS-GVO Art. 6, Rn. 28]; *Herdes*, in: Taeger [37, S. 212]; *Schulz*, in: Gola/Heckmann [59, DS-GVO Art. 6, Rn. 62]; *Spindler/Dalby*, in: Spindler/Schuster [62, DS-GVO Art. 6, Rn. 17]; *Taeger*, in: Taeger/Gabel [64, DS-GVO Art. 6, Rn. 147]. A. A.: *Borges/Steinrötter,* in: BeckOK IT-Recht [13, DS-GVO Art. 6, Rn. 45]; *Robrahn/Bremert,* ZD 2018 [56, S. 291, 293].

[83] [8, S. 38].

[84] Vgl. [8, S. 38]; *Schulz*, in: Gola/Heckmann [59, DS-GVO Art. 6, Rn. 62]; *Spindler/Dalby*, in: Spindler/Schuster [62, DS-GVO Art. 6, Rn. 17].

licher Sicht immer vor dem Austausch einzelfallbezogen überprüft werden. Bei der Verarbeitung im Rahmen eines Informationsaustauschs müssen außerdem die weiteren Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 DS-GVO eingehalten werden.[85] Insbesondere sind geeignete „Technische und Organisatorische Maßnahmen" (TOM) zu ergreifen, um die Sicherheit der Verarbeitung zu gewährleisten.[86] Unter technischen Maßnahmen versteht man alle Maßnahmen, die mittels Sachmitteln die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität gewährleisten sollen, während unter organisatorischen Maßnahmen alle aufgestellten Verhaltensregeln zu verstehen sind.[87]

5.3 Wettbewerbsrecht

5.3.1 Grundlagen der wettbewerbsrechtlichen Behandlung eines Informationsaustauschs

Eines der Hauptziele der Europäischen Union ist die Errichtung eines gemeinsamen Binnenmarktes.[88] Der Binnenmarkt umfasst zur Verwirklichung des Leitbilds einer offenen Marktwirtschaft mit freiem Wettbewerb unter anderem ein System, das den Wettbewerb vor Verfälschungen schützt.[89] Art. 101 Abs. 1 AEUV[90] verbietet daher Unternehmen, untereinander Vereinbarungen zu treffen, die zu einer Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs innerhalb des europäischen Binnenmarkts führen könnten.[91]

Art. 45 Abs. 1 Buchst. c DORA verweist aus wettbewerbsrechtlicher Sicht darauf, dass beim Informationsaustausch über Cyberbedrohungen Leitlinien für die Wettbewerbspolitik einzuhalten sind. Konkret handelt es sich um die „Leitlinien zur Anwendbarkeit des Artikels 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit"[92] (kurz: Horizontal-Leitlinien oder Horizontal-LL).[93] Eine überarbeitete Version der Horizontal-LL ist am 21. Juli 2023 in Kraft getreten. Diese Leitlinien sollen durch eine Konkretisierung des Art. 101 AEUV sowohl den Schutz des freien Wettbewerbs

[85] Vgl. *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann [57, DSGVO Art. 5, Rn. 15].

[86] Vgl. Art. 32 Abs. 1 DS-GVO.

[87] Vgl. [54, S. 243].

[88] Vgl. Art. 3 Abs. 3 Satz 1 EUV; [48, S. 9]; *Nettesheim*, in: Oppermann/Classen/Nettesheim, EuropaR [52, § 18, Rn. 8].

[89] Vgl. Art. 3 Abs. 3 EUV und Art. 51 EUV i. V. m. Protokoll Nr. 27; Art. 101 ff. i. V. m. Art. 119 AEUV; EuGH-Urt. v. 17. November 2011 – ECLI:EU:C:2011:740, Rn. 60; *Khan*, in: Geiger/Khan/Kotzur/Kirchmair [43, Art. 101 AEUV, Rn. 1]; *Säcker,* in: MüKo WettbR [58, Kap. A, Rn. 3].

[90] Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung) (ABl. C 326 vom 26. November 2012, S. 47–390).

[91] Vgl. Art. 101 Abs. 1 AEUV; Rn. 9 Horizontal-LL.

[92] Mitteilung der Kommission – Leitlinien zur Anwendbarkeit des Artikels 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit (ABl. C 259 vom 21. Juli 2023, S. 1–125).

[93] Vgl. ErwG 34 DORA; COM(2020) 595 final, Fn. 49.

gewährleisten als auch Rechtssicherheit für betroffene Unternehmen schaffen.[94] Sie unterstützen bei der Klärung der Fragen, welche horizontalen Vereinbarungen unter das Verbot gemäß Art. 101 AEUV fallen und welche Vereinbarungen (unter gewissen Bedingungen) erlaubt sind. Es gilt zu verhindern, dass ein Informationsaustausch zu einer wettbewerbsbeschränkenden Kollusion oder wettbewerbswidrigen Marktabschottung führt.[95]

5.3.2 Prüfung der wettbewerbsrechtlichen Behandlung eines Informationsaustauschs

Eine koordinierte Zusammenarbeit – beispielsweise in Form eines Informationsaustauschs – ist gemäß Art. 101 Abs. 1 AEUV verboten, wenn sie geeignet ist, den Handel zwischen Mitgliedstaaten zu beeinträchtigen und eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs innerhalb des europäischen Binnenmarkts bewirken könnte oder gar bezweckt. Die Prüfung, ob eine Zusammenarbeit verboten ist, erfolgt in mehreren Schritten. Die Horizontal-LL helfen bei der Prüfung horizontaler Kooperationen. Nachfolgend werden die Prüfungsschritte für eine Überprüfung einer horizontalen Zusammenarbeit in Form eines (reinen) Informationsaustauschs erläutert.[96] Sollte eine Vereinbarung gemäß Art. 101 Abs. 1 AEUV als verboten eingestuft werden, kann das Verbot dennoch gemäß Art. 101 Abs. 3 AUEV nach einer Abwägungsprüfung für nicht anwendbar erklärt werden.[97]

Art. 101 AEUV und die Horizontal-LL sind grundsätzlich auf alle Formen und Ausgestaltungsmöglichkeiten eines Informationsaustauschs anwendbar,[98] sofern dieser im Rahmen einer koordinierten horizontalen Zusammenarbeit erfolgt.[99] Eine Zusammenarbeit liegt bei einer Vereinbarung zwischen Unternehmen, einem Beschluss einer Unternehmensvereinigung oder einer aufeinander abgestimmten Verhaltensweise zwischen Unternehmen vor.[100] In einer Vereinbarung kommen zwei oder mehr Unternehmen übereinstimmend darin überein, zusammenarbeiten zu wollen.[101] Eine Vereinbarung zur Zusammenarbeit auf horizontaler – in Abgrenzung zur vertikalen – Ebene liegt vor, wenn sie zwischen aktuellen oder potenziellen Wettbewerbern eines bestimmten Marktes, wie z. B. dem Finanzmarkt, geschlossen wird.[102] Der Informationsaustausch gemäß Art. 45 DORA darf nur innerhalb vertrauenswürdiger Gemeinschaften erfolgen, über deren Beitritt die jeweiligen Unternehmen die

[94] Vgl. Rn. 1 Horizontal-LL.

[95] Vgl. ausführlich Rn. 377–383 Horizontal-LL.

[96] Bei tiefergehenden Arten von Vereinbarungen über eine horizontale Zusammenarbeit (z. B. bei Einkaufsvereinbarungen) findet ebenso ein Informationsaustausch statt. Die Prüfung, ob das Verbot gemäß Art. 101 Abs. 1 AEUV greift, erfolgt dann aber grundsätzlich zunächst anhand der Erläuterungen zu den weiteren Arten von Vereinbarungen. Vgl. Rn. 369 Horizontal-LL.

[97] Vgl. Rn. 18 Horizontal-LL.

[98] Vgl. Rn. 366–368 Horizontal-LL.

[99] Vgl. Rn. 14 und Rn. 375 Horizontal-LL.

[100] Vgl. Rn. 14 Horizontal-LL.

[101] Vgl. Rn. 14 Horizontal-LL; EuGH-Urt. v. 13. Juli 2006 – ECLI:EU:C:2006:460, Rn. 37.

[102] Vgl. *Wagner-von Papp,* in: MüKo WettbR [68, Art. 101 AEUV, Rn. 296].

zuständigen Behörden zu informieren haben.[103] Mit der Beitrittserklärung der Finanzunternehmen liegt eine Willensbekundung zur Zusammenarbeit und somit auch eine koordinierte Zusammenarbeit in Form einer Vereinigung vor.

Die Horizontal-LL sind explizit auch auf einen Informationsaustausch im Rahmen von Regulierungsinitiativen anwendbar.[104] Durch Art. 45 DORA werden Unternehmen gesetzlich dazu angehalten, Informationen mit anderen Unternehmen – auf freiwilliger Basis – auszutauschen. Mithin liegt damit eine Regulierungsinitiative vor, bei der die Horizontal-LL anzuwenden sind.

Sofern eine koordinierte Zusammenarbeit zwischen (potenziell) im Wettbewerb stehenden Unternehmen vorliegt, ist im nächsten Schritt zu prüfen, ob eine spürbare Wettbewerbsbeschränkung bezweckt oder bewirkt werden könnte. Der Begriff der „bezweckten" Wettbewerbsbeschränkung ist eng auszulegen,[105] liegt eine solche jedoch vor, so sind ihre Auswirkungen auf den Markt nicht mehr zu prüfen.[106] Eine Wettbewerbsbeschränkung wird bezweckt, wenn die Vereinbarung den Wettbewerb nach ihrem Inhalt, den mit ihr verfolgten Zielen und den wirtschaftlichen und rechtlichen Rahmenbedingungen für sich genommen so hinreichend beeinträchtigt, dass davon ausgegangen werden kann, dass die Prüfung ihrer Wirkung nicht notwendig ist.[107] Die Absicht der Parteien oder konkrete Preisabsprachen zwischen Unternehmen sind keine unbedingt notwendigen Indizien für das Vorliegen einer bezweckten Wettbewerbsbeschränkung.[108] Das Vorliegen wurde von der Rechtsprechung nach einer Einzelfallprüfung beispielsweise auch bejaht, wenn Prognosen über die aktuelle und künftige Nachfrage zwischen Wettbewerbern ausgetauscht wurden.[109] Bei Vorliegen einer bezweckten Wettbewerbsbeschränkung ist eine Prüfung der (Mindest-)Spürbarkeit nicht notwendig,[110] eine Rechtfertigung gemäß Art. 101 Abs. 3 AEUV ist i. d. R. abzulehnen und die koordinierte Zusammenarbeit somit verboten.[111]

Eine Wettbewerbsbeschränkung wird bewirkt, wenn die horizontale Vereinbarung „eine tatsächliche oder wahrscheinliche spürbare negative Auswirkung auf mindestens einen Wettbewerbsparameter des Marktes (z. B. Preis, Produktionsmenge, Produktqualität, Produktvielfalt oder Innovation) hat."[112] Zur Feststellung einer bewirkten Wettbewerbsbeschränkung ist ein einzelfallbezogener Vergleich der in Frage stehenden Wettbewerbssituation mit der hypothetischen Situation, dass die Verein-

[103] Vgl. Art. 45 Abs. 1 Buchst. b und Abs. 3 DORA.

[104] Vgl. Rn. 372 Horizontal-LL.

[105] Vgl. Rn. 23 Horizontal-LL; EuGH-Urt. v. 30. Januar 2020 – ECLI:EU:C:2020:52, Rn. 67 (m. w. N.).

[106] Vgl. Rn. 22 Horizontal-LL (m. w. N.).

[107] Vgl. Rn. 23 Horizontal-LL; EuGH-Urt. v. 30. Januar 2020 – ECLI:EU:C:2020:52, Rn. 67 (m. w. N.).

[108] Vgl. Rn. 25, 29, 414–415 Horizontal-LL.

[109] Vgl. Rn. 414 Horizontal-LL; EuG-Urt. v. 9. September 2015 – ECLI:EU:T:2015:611, Rn. 51.

[110] Vgl. EuGH-Urt. v. 13. Dezember 2012 – ECLI:EU:C:2012:795, Rn. 37.

[111] Vgl. *Wagner-von Papp,* in: MüKo WettbR [68, Art. 101 AEUV, Rn. 312].

[112] Vgl. Rn. 30 Horizontal-LL.

barung nicht existieren würde, notwendig.[113] Dabei sind in einer Gesamtabwägung verschiedene Faktoren – wie beispielsweise die Marktstruktur, die Aktualität der Informationen oder die Häufigkeit des Informationsaustausches – einzubeziehen.[114] Teilweise sind bei dieser Prüfung bereits wettbewerbsfördernde positive Auswirkungen zu berücksichtigen.[115] Allerdings sind mögliche Effizienzgewinne erst im Rahmen der Prüfung gemäß Art. 101 Abs. 3 AEUV zu untersuchen.[116]

Greift das Verbot gemäß Art. 101 Abs. 1 AEUV und ist keine Rechtfertigung gemäß Art. 101 Abs. 3 anwendbar, darf der Informationsaustausch nicht stattfinden. Damit ein Informationsaustausch über Cyberbedrohungen nicht als eine verbotene Wettbewerbsbeschränkung eingestuft wird, sollten Finanzunternehmen im Zweifel überlegen, ob der wirtschaftlich sensible Charakter der Informationen verringert werden kann, beispielsweise durch die Aggregation von Informationen.[117] Auch die Beschränkung des Austauschs auf historische Informationen wird empfohlen,[118] für den Austausch über aktuelle und zukünftige Cyberbedrohungen ist dies allerdings nur begrenzt zielführend. Es sollte eine Selbstverständlichkeit sein, dass nur das ausgetauscht wird, was zur Erreichung des Ziels der gesteigerten digitalen operationalen Resilienz des Finanzsektors notwendig und angemessen ist.[119] Der europäische Gesetzgeber hat eine Abbildung (Abb. 2) zur Verfügung gestellt, mit denen Unternehmen selbst prüfen können, ob ihr geplanter Informationsaustausch verboten sein könnte bzw. wie sie einen möglichen wettbewerbsbeschränkenden Charakter der Zusammenarbeit vermindern können.[120]

Anhand der Satzung des CSSA kann beispielhaft verdeutlicht werden, wie wettbewerbsrechtlichen Bedenken gegenüber einer Zusammenarbeit Rechnung getragen werden sollte. Gemäß § 4 Abs. 3 der Vereinssatzung ist der Austausch von Informationen über aktuelle Marktdaten wie Preise, Rabatte, Margen und Absatzmengen sowie Kostenbestandteile, Kunden- und Lieferantenbeziehungen, Kapazitäten und Auslastungen untersagt. Ebenso ist es verboten, sich über geplante Investitionen oder Vorhaben im Bereich Forschung und Entwicklung sowie über geplante Produkteinführungen und Informationen zur Organisationsstruktur, sofern letzteres kostenrelevant ist, auszutauschen. Die Aktivitäten des Vereins sollen so ausgestaltet werden, dass sich die Mitglieder nicht in ihrem Marktverhalten beeinflussen und den Wettbewerb verfälschen. Dies gilt insbesondere, wenn die an den Aktivitäten teilnehmenden Vereinsmitglieder im Wettbewerb zueinander stehen.[121]

[113] Vgl. Rn. 30 Horizontal-LL. Vgl. ferner EuGH-Urt. v. 11. September 2014 – ECLI:EU:C:2014:2201, Rn. 161 (m. w. N.) und Rn. 166; EuG-Urt. v. 12. Dezember 2018 – ECLI:EU:T:2018:918, Rn. 315; EuGH-Urt. v. 30. Januar 2020 – ECLI:EU:C:2020:52, Rn. 118.

[114] Vgl. ausführlich *Wagner-von Papp,* in: MüKo WettbR [68, Art. 101 AEUV, Rn. 359–383].

[115] Vgl. *Wagner-von Papp,* in: MüKo WettbR [68, Art. 101 AEUV, Rn. 384–385].

[116] Vgl. Rn. 425 Horizontal-LL; *Wagner-von Papp,* in: MüKo WettbR [68, Art. 101 AEUV, Rn. 385].

[117] Vgl. Rn. 406, 434 Horizontal-LL.

[118] Vgl. Rn. 434 Horizontal-LL.

[119] Vgl. Rn. 406, 434 Horizontal-LL.

[120] Vgl. Rn. 343 Horizontal-LL.

[121] Vgl. zu diesem Absatz [21, S. 2].

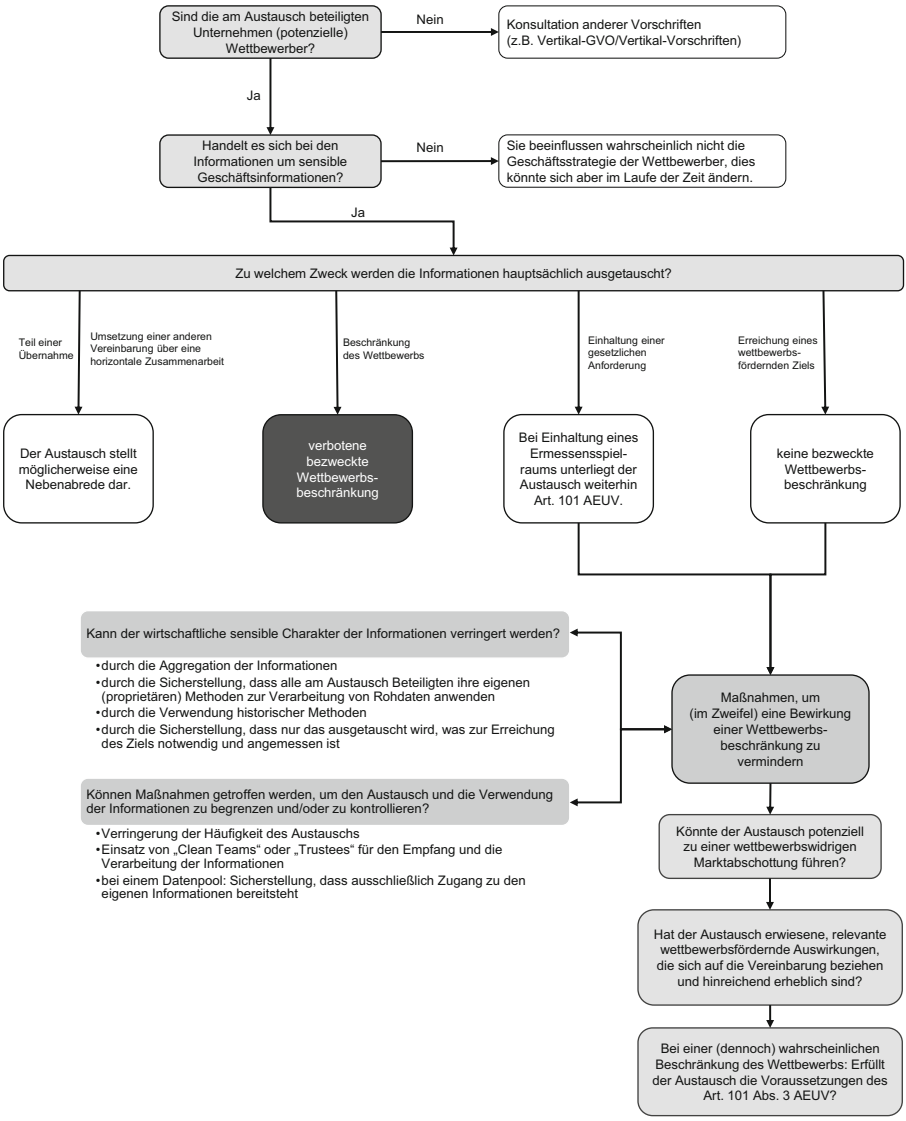


Abb. 2 Schritte der Selbstprüfung beim Informationsaustausch. (Modifiziert entnommen aus Rn. 343 Horizontal-LL)

6 Praxisbeispiel – European Cloud User Coalition (ECUC)

Die European Cloud User Coalition (ECUC) ist ein bereits bestehendes Beispiel für einen Zusammenschluss, der als Blaupause für vertrauenswürdige Gemeinschaften i. S. d. Art. 45 DORA dienen könnte. Dieser Zusammenschluss, bestehend aus derzeit 28 regulierten europäischen Finanzunternehmen, wurde im Januar 2021 gegründet.

Zu den Mitgliedern der ECUC gehören unter anderem die Commerzbank AG, die Deutsche Kreditbank AG, die Landesbank Saar und die Deutsche Börse AG.[122]

Das Ziel des Zusammenschlusses ist es, durch einen horizontalen Austausch der Mitglieder untereinander sowie einen vertikalen Austausch mit Cloud Service Providern[123] (CSPs) die Einhaltung regulatorischer Vorgaben zur Nutzung von Public Cloud-Lösungen[124] in europäischen Finanzunternehmen zu fördern. Die Finanzunternehmen möchten dazu gemeinsame technische Standards und prozessuale bzw. vertragliche Lösungen entwickeln.[125] Die Finanzunternehmen als Cloud-Nutzer sollen sich auf ein Level Playing Field[126] einigen, das heißt auf einheitliche Anforderungen für die Nutzung der Public Cloud-Technologie. Dadurch sollen Verhandlungen mit CSPs effizienter und schneller zu einem Abschluss gelangen.[127] Die Bestrebungen der Finanzunternehmen, vereinheitlichte Anforderungen durchzusetzen, sollen insbesondere globale CSPs dazu bewegen, die strengen europäischen regulatorischen Anforderungen und Datenschutzstandards zu erfüllen. Dies soll die Vielfalt an Cloud-Angeboten erhöhen, wodurch den Finanzinstituten mehr Wahlmöglichkeiten und eine größere Unabhängigkeit von einzelnen CSPs geboten werden könnte.[128]

Die ECUC gibt an, dass ein neues Mitglied vor seinem Beitritt eine Vereinbarung mit festgelegten Rechten und Pflichten unterzeichnen muss. Der Schutz des geistigen Eigentums der Mitglieder und der Datenschutz seien dabei zu gewährleisten.[129] Die ECUC verhandelt allerdings keine konkreten Verträge oder Preisausgestaltungen mit CSPs. Der Hauptzweck der Vereinigung liegt vielmehr im informativen Austausch über den Einsatz und die Ausgestaltung von Public Cloud-Lösungen in der Finanzbranche,[130] wozu auch Fragestellungen mit Bezug zur Informationssicherheit und zu Cyberbedrohungen gehören.[131] Die organisatorische Struktur der ECUC kann daher grundsätzlich als ein Beispiel für die Ausgestaltung einer vertrauenswürdigen

[122] Vgl. zu diesem Absatz [26].

[123] Ein Cloud Service Provider be- und vertreibt auf Basis der Cloud Computing-Technologie eine Cloud bzw. verschiedene Software-Lösungen innerhalb der Cloud. Cloud Computing ist „ein Modell, das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können." [50, S. 2], zitiert in der deutschen Übersetzung nach [16, S. 14].

[124] Eine Public Cloud wird üblicherweise von einem IT-Dienstleister betrieben, der seine Cloud-Lösung am Markt einer Vielzahl i. d. R. organisatorisch nicht verbundener Kunden zur Verfügung stellt. Im Gegensatz dazu bezeichnet der Begriff „Private Cloud" eine Cloud-Lösung, die nur einem vorab festgelegten Nutzerkreis zur Verfügung steht. Vgl. zu den letzten beiden Sätzen [12, S. 18]; *Krcmar*, in: Borges/Meents, Cloud Computing [45, § 1, Rn. 37 und Rn. 44].

[125] Vgl. zu den letzten beiden Sätzen [25].

[126] „Unter einem Level Playing Field ist die Gewährleistung gleicher und fairer Wettbewerbsbedingungen für alle Teilnehmer eines Marktes (beispielsweise für Kreditinstitute im Bereich bankenaufsichtsrechtlicher Regelungen) zu verstehen." *Waschbusch*, in: Gramlich/Gluchowski/Horsch/Schäfer/Waschbusch, Gabler Banklexikon [69, S. 1323].

[127] Vgl. zu den letzten beiden Sätzen [24].

[128] Vgl. zu den letzten beiden Sätzen [27].

[129] Vgl. [24].

[130] Vgl. [27].

[131] Vgl. etwa [28, S. 13–17].

Gemeinschaft i. S. d. Art. 45 Abs. 1 Buchst. b DORA angesehen werden. Dies gilt ebenso für den CSSA, dessen Satzung – wie oben bereits gezeigt – wettbewerbsrechtlichen und datenschutzrechtlichen Bedenken Rechnung trägt. Inhaltlich handelt es sich bei der ECUC um eine Interessenvertretung und der Fokus des Austauschs liegt nicht auf dem Thema Cyberbedrohungen.[132]

7 Praxisbeispiel – TIBER-DE Community

Alle unter den Anwendungsbereich des DORA fallenden Finanzunternehmen müssen über ein umfassendes Testprogramm ihrer digitalen operationalen Resilienz verfügen, um etwaige Schwächen und Mängel dieser schnell erkennen und beheben zu können.[133] So sind bspw. regelmäßig Penetrationstests und Schwachstellenscans durchzuführen.[134] Darüber hinaus müssen große und durch die Aufsichtsbehörden hierzu verpflichtete Finanzunternehmen mindestens alle drei Jahre erweiterte Tests auf Basis von TLPT durchführen.[135] Unter TLPT (engl. threat-led penetration testing) versteht man gemäß Art. 3 Nr. 17 DORA ein Rahmenwerk, dass die TTPs realer Angreifer nachahmt und einen kontrollierten, maßgeschneiderten, erkenntnisgestützten (Red-Team-)Test der kritischen Live-Produktionssysteme des Finanzunternehmens ermöglicht.

Bedrohungsgeleitete Penetrationstests können große deutsche Finanzunternehmen heute schon in Zusammenarbeit mit der Deutschen Bundesbank freiwillig durchführen. Das Programm wird als TIBER-DE (engl. Threat Intelligence-Based Ethical Red Teaming) bezeichnet.[136] TIBER-Tests basieren auf Informationen über bisherige Angriffe (threat Intelligence-Based), was noch einmal verdeutlich wie wichtig ein Austausch solcher Informationen ist.

Die Deutsche Bundesbank hat außerdem die sogenannte TIBER-DE-Community ins Leben gerufen. In dieser können sich Finanzunternehmen über ihre abgeschlossenen, gerade laufenden oder bevorstehenden TIBER-Tests austauschen und so wichtige Erfahrungen teilen. Bei regelmäßigen Treffen stellen die Unternehmen beispielsweise ihre simulierten Angriffsszenarien und ihre Testergebnisse vor. Die Deutsche Bundesbank hofft, dass sich die Mitglieder der TIBER-DE-Community dauerhaft vernetzen und sich auch bei anderen Fragen der Cybersicherheit gegenseitig unterstützen.[137]

[132] Vgl. *Sterling,* Die Bank 2022 [63, S. 70, 71].

[133] Vgl. ausführlich Art. 24 DORA.

[134] Vgl. Art. 25 Abs. 1 DORA.

[135] Vgl. ausführlich Art. 26 DORA.

[136] Vgl. zu den letzten beiden Sätzen *Balz/Sinn,* ZfgK 2023 [9, S. 222].

[137] Vgl. zu diesem Absatz ausführlich *Balz/Sinn,* ZfgK 2023 [9, S. 222, 223–224].

8 Fazit

Art. 45 DORA erlaubt einen (grenzüberschreitenden) Informationsaustausch über Cyberbedrohungen zwischen Finanzunternehmen in der Europäischen Union.[138] Er erleichtert durch einige Vorgaben dessen Einrichtung und klärt so bisher bestehende Unsicherheiten auf. Durch den Informationsaustausch soll das Bewusstsein für Cyberbedrohungen bzw. IKT-Risiken gestärkt werden. Die Erkenntnisse des Austauschs sollen dazu beitragen, die momentan sehr hohe Bedrohungslage zu entschärfen und die Abwehrkapazitäten der Finanzunternehmen zu steigern.[139]

Der Austausch von Informationen muss innerhalb vertrauenswürdiger Gemeinschaften erfolgen.[140] Zudem sind die Vorgaben weiterer europäischer Regelungsbereiche einzuhalten, darunter insbesondere das Recht zum Schutz von Geschäftsgeheimnissen, das Datenschutzrecht und das Wettbewerbsrecht.[141] Für letzteres gilt, dass auch beim Informationsaustausch im Rahmen von Regulierungsinitiativen Art. 101 AEUV anwendbar ist. Finanzunternehmen sollten den Umfang des Informationsaustauschs daher auf das beschränken, was erforderlich ist, und müssen Vorsichtsmaßnahmen ergreifen, falls sensible Geschäftsinformationen ausgetauscht werden sollen.[142]

Neben dem freiwilligen Austausch untereinander regelt der DORA weiterhin den Austausch von Finanzunternehmen mit den für sie zuständigen Behörden sowie den behördenübergreifenden Austausch.[143] Die Europäischen Aufsichtsbehörden (ESA)[144] können außerdem – unter anderem in Zusammenarbeit mit der Europäischen Zentralbank (EZB), dem Europäischen Ausschuss für Systemrisiken (ESRB) und der Agentur der Europäischen Union für Cybersicherheit (ENISA) – „Mechanismen für den Austausch wirksamer Verfahren zwischen Finanzsektoren einrichten, um die Lageerfassung zu verbessern und sektorübergreifend gemeinsame Cyberanfälligkeiten und -risiken zu ermitteln."[145] Sie können zudem (sektorübergreifende) Krisenmanagement- und Notfallübungen initiieren.[146]

Der Austausch von Informationen über Cyberbedrohungen ist von entscheidender Bedeutung, um Cyberangriffe abzuwehren und effektiv zu bekämpfen.[147] Finanzunternehmen sollten den Informationsaustausch, dem Art. 45 DORA nun einen gesetz-

[138] Vgl. *Brabetz,* bank und markt 2023 [14, S. 312, 314].

[139] Vgl. zu den letzten beiden Sätzen *Brabetz,* bank und markt 2023 [14, S. 312, 314]; *Glaser,* FLF 2023 [31, S. 270, 272].

[140] Vgl. Art. 45 Abs. 1 Buchst. b DORA.

[141] Vgl. Art. 45 Abs. 1 Buchst. c DORA.

[142] Vgl. zu den letzten beiden Sätzen Rn. 372 Horizontal-LL.

[143] Vgl. Art. 47 ff. DORA.

[144] Die Europäische Bankenaufsichtsbehörde (EBA), die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA) sowie die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) werden unter dem Begriff „Europäische Aufsichtsbehörden" (ESA) zusammengefasst. Vgl. ErwG 7 DORA.

[145] Art. 49 Abs. 1 UAbs. 1 DORA.

[146] Vgl. Art. 49 Abs. 1 UAbs. 2 DORA.

[147] Vgl. *Albakri/Boiten/Lemos,* APF 2019 [2, S. 28]; *Balz/Sinn,* ZfgK 2023 [9, S. 222, 223–224]; *Krautscheid/Nash,* BaFin Perspektiven 2020 [44, S. 35, 38].

lichen Rahmen gibt, weiter ausbauen – dies gilt insbesondere auf der bisher noch vernachlässigten europäischen Ebene. „Cyber-Sicherheit ist eine so große Herausforderung, dass die Unternehmen gemeinsam Verantwortung übernehmen müssen.“[148]

Funding Open Access funding enabled and organized by Projekt DEAL.

Interessenkonflikt G. Waschbusch und B. Schlenker geben an, dass kein Interessenkonflikt besteht.

Literatur

1. Albakri A, Boiten E, de Lemos R (2018) Risks of Sharing Cyber Incident Information, in: Proceedings of the 13th International Conference on Availability, Reliability and Security. ACM, New York, S. 1–10 https://doi.org/10.1145/3230833.3233284
2. Albakri A, Boiten E, Lemos R de (2019) Sharing Cyber Threat Intelligence Under the General Data Protection Regulation, in: Naldi M, Italiano GF, Rannenberg K, Medina M, Bourka A (hrsg.) Privacy Technologies and Policy. 7th Annual Privacy Forum, APF 2019, Rome, Italy, June 13–14, 2019, Proceedings Springer, Cham, S. 28–41. https://doi.org/10.1007/978-3-030-21752-5_3
3. Alexander C (2024) GeschGehG § 2 Begriffsbestimmungen, in: Köhler H, Bornkamm J, Feddersen J (hrsg.) Gesetz gegen den unlauteren Wettbewerb. GeschGehG, PAngV, UKlaG, DL-InfoV, P2B-VO, 42. Aufl. C.H. Beck, München, S. 2020–2059
4. Allianz für Cyber-Sicherheit (o. J.) Teilnehmer. https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Ueber-uns/Teilnehmer/teilnehmer_node.html. Zugegriffen: 1. März 2024
5. Allianz für Cyber-Sicherheit (2022) Allianz für Cyber-Sicherheit. BSI-BroAfCS18/001, Bonn
6. Ann C (2014) Geheimnisschutz – Kernaufgabe des Informationsmanagements im Unternehmen. GRUR 116(1):12–16
7. Arning MA, Rothkegel T (2022) DS-GVO Art. 4 Begriffsbestimmungen, in: Taeger J, Gabel D (hrsg.) DSGVO – BDSG – TTDSG. Kommentar, 4. Aufl. Fachmedien Recht und Wirtschaft in Deutscher Fachverlag GmbH, Frankfurt am Main
8. Artikel-29-Datenschutzgruppe (2014) Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG. 844/14/EN – WP 217. https://www.datenschutzstelle.li/application/files/2915/5914/1746/WP217_Opinion62014LegitimateInterest.pdf. Zugegriffen: 1. März 2024
9. Balz B, Sinn M (2023) TIBER-DE: Eine Erfolgsgeschichte zum Schutz kritischer Infrastrukturen im Finanzsektor. ZfgK 76(5):222–225
10. Bausewein C (2023) Der Hackerparagraph und das Dilemma der Schwachstellenforschung, in: Bernzen AK, Fritzsche J, Heinze C, Thomsen O (hrsg.) Das IT-Recht vor der (europäischen) Zeitenwende? Tagungsband DSRI-Herbstakademie 2023 XII, 1. Aufl. OlWIR, Edewecht, S. 313–323
11. BCBS (2018) Cyber-resilience: Range of practices. https://www.bis.org/bcbs/publ/d454.pdf. Zugegriffen: 1. März 2024

[148] *Dietsche,* Börsen-Zeitung 2019 [22, S. 8].

12. bitkom (2010) Cloud Computing – Was Entscheider wissen müssen. Ein ganzheitlicher Blick über die Technik hinaus – Positionierung, Vertragsrecht, Datenschutz, Informationssicherheit, Compliance – Leitfaden. https://www.bitkom.org/sites/main/files/file/import/BITKOM-Leitfaden-Cloud-Computing-Was-Entscheider-wissen-muessen.pdf. Zugegriffen: 1. März 2024
13. Borges G, Steinrötter B (2023) Art. 6 Rechtmäßigkeit der Verarbeitung, in: Borges G, Hilber M (hrsg.) BeckOK IT-Recht, 12. Aufl. C.H. Beck, München
14. Brabetz S (2023) Sichere Finanzen mit dem Digital Operational Resilience Act. Bank und Markt (7):312–314
15. Brisch K, Rexin L (2019) Sicherheit durch Technik: Cyber-Threat-Plattformen in Deutschland. CR 35(9):606–617. https://doi.org/10.9785/cr-2019-350917
16. BSI (2012) Eckpunktepapier – Sicherheitsempfehlungen für Cloud Computing Anbieter. Mindestanforderungen in der Informationssicherheit – BSI-Bro12/314. https://www.bsi.bund.de/dok/6622126. Zugegriffen: 30. Juni 2023
17. BSI (2023) IT-Grundschutz-Kompendium, Edition 2023, Bundesanzeiger-Verlag, Köln
18. CIRCL (o. J.) MISP – Open Source Threat Intelligence Platform. https://www.circl.lu/services/misp-malware-information-sharing-platform/. Zugegriffen: 1. März 2024
19. Clausmeier D (2023) Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). ICLR 4(1):79–90. https://doi.org/10.1365/s43439-022-00076-5
20. CSSA (o. J.) Cyber Security Sharing & Analytics (CSSA). https://cssa.de/. Zugegriffen: 1. März 2024
21. CSSA (2022) Satzung. Zuletzt geändert durch Beschluss vom 08.11.2022. https://cssa.de/static/CSSA_Satzung.pdf. Zugegriffen: 1. März 2024
22. Dietsche B (2019) Cyber-Sicherheit – allein geht es nicht. Börsen-Zeitung (151):8
23. Droege-Knaup J (2022) Grenzüberschreitende Probleme? Grenzüberschreitende Lösungen – durch DORA. https://www.bafin.de/ref/19617918. Zugegriffen: 1. März 2024
24. ECUC (o. J.) About us. https://ecuc.group/about-us/. Zugegriffen: 1. März 2024
25. ECUC (o. J.) FAQ. https://ecuc.group/faq/. Zugegriffen: 1. März 2024
26. ECUC (o. J.) Membership. https://ecuc.group/membership/. Zugegriffen: 1. März 2024
27. ECUC (o. J.) Our objectives. https://ecuc.group/our-objectives/. Zugegriffen: 1. März 2024
28. ECUC (2022) Position Paper – Requirements for standardisation of compliant use of public cloud technology in regulated European Financial Institutions (FIs) – Version 2.1. https://ecuc.group/papers/ECUC_Position_Paper_Sep_2022_v2.1.pdf. Zugegriffen: 1. März 2024
29. ENISA (2022) ENISA Threat Landscape for Ransomware Attacks. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks. Zugegriffen: 1. März 2024
30. ENISA (2023) ENISA Threat Landscape 2023. July 2022 to June 2023. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends. Zugegriffen: 1. März 2024
31. Glaser C (2023) Digital Operational Resilience Act. Vorschriften für das Risikomanagement werden harmonisiert. FLF (6):270–274
32. Glinke A (2021) GeschGehG § 2 Nr 1 Geschäftsgeheimnis – 4. Wirtschaftlicher Wert der Information, in: Keller E, Schönknecht M, Glinke A (hrsg.) Geschäftsgeheimnisschutzgesetz, 1. Aufl. C.H. Beck, München, S. 154–158
33. Grund F (2022) „IT-Sicherheit: Versicherer und EbAVs müssen resilienter werden". Interview mit Dr. Frank Grund vor der Veranstaltung IT-Aufsicht bei Versicherungen und Pensionsfonds. https://www.bafin.de/ref/19617974. Zugegriffen: 1. März 2024
34. Harte-Bavendamm H (2020) § 2 Begriffsbestimmungen in: Harte-Bavendamm H, Ohly A, Kalbfus B (hrsg.) GeschGehG – Gesetz zum Schutz von Geschäftsgeheimnissen. Kommentar, 1. Aufl. C.H. Beck, München, S. 197–253
35. Heberlein H (2018) Art. 6 Rechtmäßigkeit der Verarbeitung, in: Ehmann E, Selmayr M (hrsg.) DS-GVO. Datenschutz-Grundverordnung: Kommentar, 2. Aufl. C.H. Beck, LexisNexis, München, Wien, S. 203–234
36. Herbst T (2024) Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten, in: Kühling J, Buchner B (hrsg.) Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. Kommentar, 4. Aufl. C.H. Beck, München, S. 265–292
37. Herdes D (2018) Daten im Konzern: Datenschutz im B2C Bereich, in: Taeger J (hrsg.) Rechtsfragen Digitaler Transformationen. Gestaltung digitaler Veränderungsprozesse durch Recht – Tagungsband Herbstakademie 2018, 1. Aufl. OlWIR, Edewecht, S. 207–218
38. Hiéramente M, Golzio JO (2018) Die Reform des Geheimnisschutzes aus Sicht der Compliance-Abteilung – Ein Überblick. CCZ 11(6):262–267

39. Höfer C (2018) Regierungsentwurf zum Geschäftsgeheimnisgesetz (GeschGehG) aus Geschäftsführersicht: Pflicht zum „Geschäftsgeheimnis-Management". GmbHR (22):1195–1198
40. Hofmarcher D (2020) Das Geschäftsgeheimnis. Der neue Schutz von vertraulichem Know-how und vertraulichen Geschäftsinformationen, 1. Aufl. MANZ'sche Verlags- und Universitätsbuchhandlung, Wien
41. Hoppe D, Momtschilow M, Lodemann M et al. (2022) Kapitel 1 Materielles Recht – B. Begriffsbestimmungen, in: Hoppe D, Oldekop A (hrsg.) Geschäftsgeheimnisse. Schutz von Know-how und Geschäftsinformationen – Praktikerhandbuch mit Mustern, 2. Aufl. Carl Heymanns Verlag, Hürth, S. 19–105
42. Johnson C, Badger L, Waltermire D, Snyder J, Skorupka C (2016) Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150. https://doi.org/10.6028/NIST.SP.800-150. Zugegriffen: 1. März 2024
43. Khan D-E (2023) Art. 101 AEUV [Kartellverbot], in: Geiger R, Khan D-E, Kotzur M, Kirchmair L (hrsg.) EUV, AEUV. Vertrag über die Europäische Union, Vertrag über die Arbeitsweise der Europäischen Union – Kommentar, 7. Aufl. C.H. Beck, München, S. 556–571
44. Krautscheid A, Nash A (2020) Wie sich Deutschlands Banken gegen Cyberkriminalität rüsten. BaFin Perspektiven (1):35–41
45. Krcmar H (2016) § 1 Technische Grundlagen des Cloud Computing, in: Borges G, Meents JG (hrsg.) Cloud Computing. Rechtshandbuch, 1. Aufl. C.H. Beck, München, S. 1–17
46. Krüger S, Wiencke J, Koch A (2020) Der Datenpool als Geschäftsgeheimnis. GRUR 122(6):578–584
47. Lang V, Bollinger D (2022) Der Schutz von Geschäftsgeheimnissen in der Kreditwirtschaft. WM 76(46):2218–2224
48. Licht D (2020) EU-Beihilferecht und Unternehmensbesteuerung. Reihe Bilanz-, Prüfungs- und Steuerwesen, 1. Aufl. Bd. 58. Erich Schmidt Verlag, Berlin
49. McGuire M-R (2018) Geheimnisschutz: In vier Schritten zur angemessenen Maßnahme. IPRB (9):202–206
50. Mell P, Grance T (2011) The NIST Definition of Cloud Computing. NIST Special Publication 800-145. http://purl.fdlp.gov/GPO/gpo17628. Zugegriffen: 1. März 2024
51. MISP (o. J.) MISP Features and Functionalities. https://www.misp-project.org/features/. Zugegriffen: 1. März 2024
52. Nettesheim M (2021) 5. Teil. Wirtschaftsordnung der Europäischen Union, § 18. Wirtschaftsverfassung und Wirtschaftspolitik, in: Oppermann T, Classen CD, Nettesheim M (hrsg.) Europarecht. Ein Studienbuch, 9. Aufl. C.H. Beck, München, S. 320–340
53. Ohly A (2019) Das neue Geschäftsgeheimnisgesetz im Überblick. GRUR 121(5):441–451
54. Petrlic R, Sorge C, Ziebarth W (2022) Datenschutz. Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, 2. Aufl. Springer Vieweg, Wiesbaden https://doi.org/10.1007/978-3-658-39097-6
55. Renner C (2023) GeschGehG § 2 Begriffsbestimmungen, in: Borges G, Hilber M (hrsg.) BeckOK IT-Recht, 12. Aufl. C.H. Beck, München
56. Robrahn R, Bremert B (2018) Interessenskonflikte im Datenschutzrecht. Rechtfertigung der Verarbeitung personenbezogener Daten über eine Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO. ZD 9(7):291–297
57. Roßnagel A (2019) DSGVO Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten, in: Simitis S, Hornung G, Spiecker gen. Döhmann I (hrsg.) Datenschutzrecht. DSGVO mit BDSG, 1. Aufl. Nomos, Baden-Baden
58. Säcker FJ (2023) Kapitel 1. Grundlagen – A. Die rechtspolitischen Grundlagen des Wettbewerbsrecht, in: Säcker FJ, Bien F, Meier-Beck P, Montag F (hrsg.) Münchener Kommentar zum Wettbewerbsrecht – Kartellrecht, Beihilfenecht, Vergaberecht – Band 1/1: Europäisches Wettbewerbsrecht, 4. Aufl. C.H. Beck, München, S. 7–21
59. Schulz S (2022) DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung, in: Gola P, Heckmann D (hrsg.) DS-GVO / BDSG. Datenschutz-Grundverordnung – VO (EU) 2016/679 – Bundesdatenschutzgesetz – Kommentar, 3. Aufl. C.H. Beck, München, S. 292–358
60. Sohr K, Kemmerich T (2023) Kapitel 3. Technische Grundlagen der Informationssicherheit, in: Kipker D-K (hrsg.) Cybersecurity. Rechtshandbuch, 2. Aufl. C.H. Beck, München, S. 49–115
61. Sousa e Silva N (2014) What exactly is a trade secret under the proposed directive? JIPLP 9(11):923–932. https://doi.org/10.1093/jiplp/jpu179
62. Spindler G, Dalby L (2019) Art. 6 Rechtmäßigkeit der Verarbeitung, in: Spindler G, Schuster F (hrsg.) Recht der elektronischen Medien. Kommentar, 4. Aufl. C.H. Beck, München, S. 555–569
63. Sterling J (2022) European Cloud User Coalition schafft europäischen Standard. Die Bank (8):70–71

64. Taeger J (2022) DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung, in: Taeger J, Gabel D (hrsg.) DSGVO – BDSG – TTDSG. Kommentar, 4. Aufl. Fachmedien Recht und Wirtschaft in Deutscher Fachverlag GmbH, Frankfurt am Main, S. 273–347
65. vmware (o. J.) Threat Intelligence. https://www.vmware.com/topics/glossary/content/threat-intelligence.html. Zugegriffen: 1. März 2024
66. Voigt P, Herrmann V, Grabenschröer JF (2019) Das neue Geschäftsgeheimnisgesetz – praktische Hinweise zu Umsetzungsmaßnahmen für Unternehmen. BB 68(4):142–147
67. Voskamp F, Klein D (2023) Kapitel 7. Datenschutz, in: Kipker D-K (hrsg.) Cybersecurity. Rechtshandbuch, 2. Aufl. C.H. Beck, München, S. 269–304
68. Wagner-von Papp F (2023) Kapitel 2. Artikel 101 AEUV – D. Horizontale Vereinbarungen, in: Säcker FJ, Bien F, Meier-Beck P, Montag F (hrsg.) Münchener Kommentar zum Wettbewerbsrecht – Kartellrecht, Beihilfenecht, Vergaberecht – Band 1/1: Europäisches Wettbewerbsrecht, 4. Aufl. C.H. Beck, München, S. 757–835
69. Waschbusch G (2020) Stichwort „Level Playing Field“, in: Gramlich L, Gluchowski P, Horsch A, Schäfer K, Waschbusch G (hrsg.) Gabler Banklexikon (K–Z): Bank – Börse – Finanzierung, 15. Aufl. Springer Gabler, Wiesbaden, S. 1323 https://doi.org/10.1007/978-3-658-26757-5
70. Waschbusch G, Schlenker B, Kiszka S (2023) IKT-Risiken und Bankenaufsichtsrecht. Eine Analyse der regulatorischen Anforderungen an das IKT-Risikomanagement in Banken unter besonderer Berücksichtigung der BAIT und des DORA. Reihe Wettbewerb und Regulierung von Märkten und Unternehmen, 1. Aufl. Bd. 60. Nomos, Baden-Baden
71. Wuermeling J (2022) Digitalisierung und die Zukunft der Banken. ZfgK 75(21):1072–1075
72. Wunderlich S (2018) Die Allianz für Cyber-Sicherheit: Netzwerke schützen Netzwerke, in: Bartsch M, Frey S (hrsg.) Cybersecurity Best Practices, 1. Aufl. Springer, Wiesbaden, S. 65–72 https://doi.org/10.1007/978-3-658-21655-9_6
73. Ziechnaus M (2019) Geschäftsgeheimnisgesetz: Neue Handlungsfelder für geschäftsführende Organe. ZfgK 72(20):1053–1054

Gerd Waschbusch Inhaber des Lehrstuhls für Betriebswirtschaftslehre, insb. Bankbetriebslehre der Universität des Saarlandes

Ben Schlenker Wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Betriebswirtschaftslehre, insb. Bankbetriebslehre der Universität des Saarlandes