EU-Verordnung

ZUGANG ZU FINANZDATEN („OPEN FINANCE“)

cep**Dossier** Nr. 8/2024

Hintergrund | Ziel | Betroffene

Hintergrund: Am 28. Juni 2023 legte die EU-Kommission Vorschläge für eine Verordnung über einen Rahmen für den Zugang zu Finanzdaten vor [COM(2023) 360, Financial Data Access Regulation, FIDA]. Der Ausschuss für Wirtschaft und Währung (ECON-Ausschuss) im Europäischen Parlament beschloss am 18. April 2024 seinen Bericht zu dem Kommissionsvorschlag (s. hier). Am 4. Dezember 2024 hat nun der Rat ein Mandat für Verhandlungen mit dem Europäischen Parlament über die FIDA Verordnung erteilt (s. hier).

Ziel: Die Kommission will mit FIDA Verordnung Regeln für den Zugang, die gemeinsame Nutzung und die Verwendung bestimmter Kategorien von kundenbezogenen Finanzdaten aufstellen, um ein sogenanntes „Open Finance“-Ökosystem zu etablieren.

Betroffene: Finanzinstitute (FI), also etwa Banken, Versicherungen und Vermögensverwalter; Anbieter von sogenannten Finanzinformationsdiensten (FISP); Kunden von FI und FISP.

Hinweis: Dieses cep**Dossier** gibt einen Überblick über das Verhandlungsmandat des Rates. Für einen Überblick und eine Bewertung des Kommissionsvorschlags s. cep**Analyse** Nr. 3/2024.

Kurzdarstellung

► **Anwendungsbereich**

Erfasste Akteure

– Die Verordnung gilt für drei verschiedene Gruppen von Akteuren: Dateninhaber, Kunden und Datennutzer [Art. 2 Abs. 2, Art. 3 Nr. 2, 5–8].
  - „Dateninhaber“ sind Finanzinstitute, die die Daten ihrer Kunden („Kundendaten“) erheben, speichern und verarbeiten [Art. 3 Nr. 5]. „Finanzinstitute“ (FI) sind insbesondere [Art. 3 Nr. 8 i.V.m. Art. 2 Abs. 2 lit. a–n]
    - Banken,
    - Versicherungen und Versicherungsvermittler,
    - Zahlungsinstitute und E-Geld-Institute,
    - Wertpapierfirmen,
    - Anbieter von Kryptowerte-Dienstleistungen,
    - Verwalter von Investmentfonds (AIFM und OGAW), und
    - Einrichtungen der betrieblichen Altersversorgung (IORP), sofern sie private Altersvorsorgeprodukte verwalten.
  - „Kunden“ sind die Nutzer – natürliche und juristische Personen – von Finanzprodukten und -dienstleistungen. In Bezug auf Versicherungen sind damit die Versicherten bzw. die Versicherungsnehmer gemeint. [Art. 3 Nr. 2]
  - „Datennutzer“ sind sowohl FI als auch sogenannte „Finanzinformationsdienstleister (FISP)“, die rechtmäßigen Zugang zu „Kundendaten“ haben. Dafür müssen sie die Erlaubnis eines Kunden erhalten haben [Art. 3 Nr. 2]. „FISP“ sind Einrichtungen, die nach der Verordnung eine Zulassung erhalten haben, um als Datennutzer fungieren und „Finanzinformationsdienste“ auf Basis von „Kundendaten“ erbringen zu dürfen [Art. 3 Nr. 7].

– FI können als Dateninhaber, Datennutzer oder beides fungieren, während FISPs nur als Datennutzer fungieren können.

Ausgenommene Akteure

– Diese Verordnung gilt u.a. nicht für [Art. 2 Abs. 3]
  - bestimmte AIFM mit nur wenigen verwalteten Vermögenswerten,
  - bestimmte kleine Versicherungs- und Rückversicherungsunternehmen,
  - Einrichtungen der betrieblichen Altersversorgung mit nicht mehr als 15 Versorgungsanwärtern,
  - (Rück-)Versicherungsvermittler, die Kleinst-, kleine oder mittlere Unternehmen sind, und
  - bestimmte Spezial- und Förderbanken wie die Kreditanstalt für Wiederaufbau.

Erfasste Daten

– Die Verordnung gilt sowohl für personenbezogene als auch nicht-personenbezogene „Kundendaten“ in digitaler Form, die [Erwägungsgrund 9, Art. 3 Abs. 3]
  - von FI im Rahmen ihrer Geschäftstätigkeit mit Kunden erhoben, gespeichert und verwaltet werden,

Autor: Philipp Eckhardt | eckhardt@cep.eu

- von Kunden zur Verfügung gestellt werden,
- bei der Nutzung des Finanzprodukts oder der Finanzdienstleistung durch den Kunden entstehen („Transaktionsdaten“),
- Auskunft über die Vertragskonditionen geben.

Erfasst sind jedoch nur die „Rohdaten“ [Erwägungsgrund 9].

– Die Verordnung gilt jedoch nur für bestimmte Kategorien von „Kundendaten“, darunter Daten zu [Art. 2 Abs. 1]
  - Kreditverträgen – d.h. Zahlungsaufschübe, Darlehen oder ähnliche finanzielle Zuwendungen – und Konten, inklusive Daten zum Kontostand, zu den Kreditvertragsbedingungen und zu den Transaktionen sowie Daten, die bei der Prüfung der Kreditwürdigkeit eines Unternehmens erhoben werden,
  - Ersparnissen, d.h. Festgelder, strukturierte Einlagen und Sparkonten,
  - Investitionen in Finanzinstrumenten,
  - Versicherungsanlageprodukten,
  - versicherungsbasierten individuellen Rentenprodukten,
  - Krypto-Vermögenswerten,
  - private Altersvorsorgeprodukten, inkl. Paneuropäischen Privaten Pensionsprodukten (PEPP), und
  - Nichtlebensversicherungsprodukten.
– Dies umfasst u.a. auch Daten [Art. 2 Abs. 1]
  - zu den Nachhaltigkeitspräferenzen von Kunden,
  - die im Rahmen von Eignungs- und Angemessenheitsprüfungen bei Privatkunden erhoben werden, und
  - die bei der Abfrage der Wünsche und Bedürfnisse des Kunden erhoben werden.

Ausgenommene Daten

– Die Verordnung gilt nicht für die folgenden Kategorien von Daten, nämlich „Kundendaten“ [Art. 2 Abs. 1 lit. a, lit. e, Art. 2 Abs. 3
  - zu Zahlungskonten,
  - zu Krankenversicherungsprodukten,
  - zu Personenschäden bei Nichtlebensversicherungsprodukten,
  - zu Lebensversicherungsprodukten,
  - zu Sicherungssysteme, die Teil der gesetzlichen System der sozialen Sicherheit sind,
  - zu bereits bestehenden nationale „Pension tracking systems“ (Bsp. Deutsche Rentenübersicht),
  - die im Rahmen einer Kreditwürdigkeitsprüfung im Zusammenhang mit Verbraucherkrediten erhoben werden, und
  - die als sensibel im Sinne der Datenschutzgrundverordnung [Art. 9 und 10, DSGVO, (EU) 2016/679] gelten (z.B. Gesundheitsdaten).
– Die Verordnung gilt nicht für Kundendaten, die als vertrauliche Geschäftsdaten oder Geschäftsgeheimnisse einzustufen sind, sowie für Daten, die vom Dateninhaber intern aufbereitet wurden, d.h. nicht länger als Rohdaten gelten. Auch für personenbezogene Daten von unbeteiligten Dritten gilt die Verordnung nicht. [Erwägungsgründe 9 und 10]

Wahlrecht der Mitgliedstaaten bei Kundendaten zur betrieblichen Altersvorsorge

– Die Mitgliedstaaten „können“ auch Kundendaten zu Rentenansprüchen in betrieblichen Altersversorgungssystemen in den Geltungsbereich der Verordnung aufnehmen. Tun sie dies, dann gilt diese Entscheidung für [Art. 2 Abs. 1a]
  - Einrichtungen der betrieblichen Altersversorgung (EbAV), und
  - Versicherungen, die eine Erlaubnis zum Betrieb des Geschäfts der betrieblichen Altersversorgung haben.

  Die Mitgliedstaaten können jedoch kleine EbAV und kleine Versicherer explizit davon ausnehmen [Art. 2 Abs. 1a].

► **Pflichten für Dateninhaber**

– Dateninhaber müssen ihren Kunden auf deren Anfrage Kundendaten zur Verfügung stellen. Dies muss unverzüglich, unentgeltlich, kontinuierlich und in Echtzeit geschehen. [Art. 4]
– Dateninhaber müssen Datennutzern die Kundendaten ihrer Kunden unverzüglich, kontinuierlich und in Echtzeit zur Verfügung stellen. Sie dürfen dies nur tun [Art. 5 Abs. 1]
  - auf Ersuchen eines Kunden oder eines Datennutzers, der im Auftrag des Kunden handelt, und
  - für die Zwecke und zu den Bedingungen, für die der Kunde dem Datennutzer seine Einwilligung erteilt hat.
– Dateninhaber müssen [Art. 5 Abs. 3]
  - vor der Bereitstellung von Kundendaten an einen Datennutzer sicherstellen, dass der Datennutzer nachgewiesen hat, dass der Kunde des Dateninhabers die Erlaubnis für einen solchen Datenzugriff erteilt hat; dafür kann der Dateninhaber den Kunden über Dashboards zur Bestätigung der Erlaubnis auffordern,

- Datennutzern Kundendaten in Formaten bereitstellen, die auf gemeinsamen Standards beruhen,
- die sichere Übermittlung der Kundendaten an Datennutzer zu gewährleisten und
- die Vertraulichkeit von Geschäftsgeheimnissen und geistigen Eigentumsrechten zu wahren.

– Dateninhaber sind für die Verfügbarmachung einer „Schnittstelle" zur gemeinsamen Nutzung von Kundendaten verantwortlich. Diese kann jedoch auch bereitgestellt werden von [Erwägungsgrund 24]
  - anderen Finanzinstituten oder einer Gruppe von Finanzinstituten,
  - externen IT-Anbietern,
  - Branchenverbänden oder
  - öffentlichen Einrichtungen der Mitgliedstaaten.

  Im Falle von EbAV kann sie auch in Renten-Dashboards integriert werden [Erwägungsgrund 24].
– Dateninhaber können von Datennutzern eine Vergütung für die Bereitstellung von Kundendaten verlangen. Dies gilt dann, wenn die gemeinsame Nutzung von Daten im Rahmen eines „Systems für den Austausch von Finanzdaten" (Financial Data Sharing Scheme, FDSS) erfolgt. [Art. 5 Abs. 2]

► **Pflichten für Datennutzer**

– Ist ein Datennutzer ein FI darf dieser nur auf Kundendaten zugreifen, wenn er als FI nach den für ihn einschlägigen EU-Rechtsvorschriften zugelassen wurde. Ist der Datennutzer ein FISP benötigt dieser eine Zulassung nach der FIDA Verordnung. In beiden Fällen darf der Zugang nur im Rahmen eines FDSS erfolgen. [Art. 6 Abs. 1]
– FI, die als Datennutzer fungieren wollen, müssen dies ihrer zuständigen Aufsichtsbehörde melden [Art. 6 Abs. 1].
– Datennutzer dürfen auf Kundendaten eines Kunden eines Dateninhabers nur zu den Zwecken zugreifen, für die der Kunde seine Erlaubnis erteilt hat. Die Erlaubnis muss der Kund aus freien Stücken erteilt haben, sie muss spezifisch sein, zeitlich begrenzt und die Möglichkeit zur Erlaubniserteilung hat getrennt von anderen Erklärungen oder Texten zu erfolgen. [Art. 6 Abs. 2]
– Datennutzer müssen insbesondere sicherstellen, dass [Art. 6 Abs. 2 und 4]
  - das Erlaubnisgesuch klar, objektiv, präzise und für den Kunden leicht verständlich ist,
  - Kundendaten (inklusive Backups) gelöscht werden, sobald sie für die ursprünglich zulässigen Zwecke nicht mehr benötigt werden oder wenn der Kunde seine Erlaubnis binnen 48 Stunden widerrufen und nicht wieder neu erteilt hat,
  - sie Anträge auf Datenzugang nicht in einer Weise stellen, dass der Kunde zur Zugangsgewährung ermutigt oder in unangemessener Weise gedrängt wird, die nicht in dessen besten Interesse liegt oder seine freie Entscheidungsfindung wesentlich verzerrt oder beeinträchtigt,
  - sie Kundendaten nicht zu anderen Zwecken als zur Erbringung einer von einem Kunden angeforderten Dienstleistung verarbeiten; er muss hier im besten Interesse des Kunden handeln und dies auch nachweisen können,
  - sie die Geschäftsgeheimnisse und Rechte an geistigem Eigentum der Dateninhaber und der Kunden, die Unternehmen sind, schützen; dabei dürfen sie auch kein „Reserve-Engineering" betreiben,
  - die Kundendaten sicher gespeichert, verarbeitet und übermittelt werden,
  - sie einen unrechtmäßigen Zugriff auf oder eine unrechtmäßige Übertragung von Kundendaten verhindern und die Datenschutzrechte der Verbraucher schützen,
  - sie sich bei jeder Datenabfrage gegenüber dem Dateninhaber erkenntlich zeigen und sicher mit dem Dateninhaber und dessen Kunden kommunizieren, und
  - sie Kundendaten nicht an Dritte weiterreichen.
– Kunden haben das Recht, die einem Datennutzer erteilte Erlaubnis jederzeit und unentgeltlich zu widerrufen. Ein solcher Widerruf muss gemäß den vertraglichen Verpflichtungen erfolgen, wenn die Verarbeitung der Kundendaten für die Erfüllung eines Vertrags erforderlich ist. [Art 6 Abs. 3]
– Handelt es sich bei dem Datennutzer um einen Torwächter („Gatekeeper") nach dem Gesetz über digitale Märkte (Digital Markets Act, (EU) 2022/1925, s. cep**Analyse**), darf dieser Kundendaten zu denen er Zugang erhalten hat, nicht mit anderen Daten zu dem spezifischen Kunden kombinieren [Art. 6 Abs. 4b].

► **Dashboards für Zugriffsberechtigungen**

– Dateninhaber müssen ihren Kunden Dashboards für den Zugriff auf Finanzdaten bereitstellen. Die Dashboards müssen insbesondere [Erwägungsgrund 22, Art. 8 Abs. 1-3],
  - leicht zu erreichen und benutzerfreundlich sein,
  - den Kunden jederzeit einen Überblick über bestehende Zugriffsberechtigungen gewähren und ihnen ermöglichen, die den Datennutzern erteilten Berechtigungen zu verwalten und zu überwachen, u.a. auch zu

den Kategorien der geteilten Kundendaten, den Zweck der Erlaubnis und die Dauer der Gültigkeit der Erlaubnis,
- den Kunden jederzeit und unentgeltlich ermöglichen, eine erteilte Erlaubnis zurückzuziehen oder eine zurückgezogene Erlaubnis neu zu erteilen, und
- eine Aufzeichnung der zurückgezogenen oder abgelaufenen Genehmigungen für zwei Jahre enthalten.

– Dateninhaber dürfen ihre Dashboards für Genehmigungen nicht so gestalten, dass [Erwägungsgrund 21, Art. 8 Abs. 3]
- sie die Kunden zur Erteilung oder zum Entzug von Genehmigungen ermutigen oder ungebührlich beeinflussen,
- Kunden vom Dateninhaber aufgefordert werden können, ihre Erlaubnis zu einer Datenteilung zu widerrufen, und
- der Kunde vom Dateninhaber in einer Weise manipuliert wird, dass dieser Zugriffsberechtigungen nicht in seinem eigenen Interesse erteilt.

– Dateninhaber können bei der Bereitstellung ihrer Dashboards auf [Erwägungsgrund 21]
- elektronische Identifizierungsdienste zurückgreifen, wie etwa die „Europäische Brieftasche für die Digitale Identität (European Digital Identity Wallet, s. Verordnung (EU) 2024/1183, s. cep**Analyse**], und
- auf „Datenvermittlungsdienste" – wie im Daten-Governance-Rechtsakt [DGA, Verordnung (EU) 2022/868, s. cep**Analyse**] festgelegt - stützen.

– Ein Dateninhaber muss einen Datennutzer unverzüglich über jede Änderung einer ihn betreffenden Berechtigung benachrichtigen, d.h. wenn der Kunde über das Dashboard eine Anpassung bezüglich einer Zugriffserlaubnis vornimmt. Ein Datennutzer muss seinerseits einen Dateninhaber über jede neue Erlaubnis informieren, die von einem Kunden des Dateninhabers erteilt wurde. [Art. 8 Abs. 4]

► **Anforderungen an einen verantwortungsvollen Umgang mit Daten**

– Handelt es sich bei den Kundendaten um personenbezogene Daten, so ist ihre Verarbeitung auf das Maß zu beschränken, das im Hinblick auf die Zwecke, für die sie verarbeitet werden, erforderlich ist [Erwägungsgrund 18, Art. 7 Abs. 1)].

– Kunden, die sich weigern, Daten zur Verfügung zu stellen, darf deswegen der Zugang zu Finanzprodukten und -Dienstleistungen nicht verweigert werden [Art. 7 Abs. 1]

– Die EBA und die EIOPA „müssen" Leitlinien für eine verantwortungsvolle Datenverarbeitung entwickeln. Diese gelten für Finanzprodukte und -dienstleistungen, bei denen [Art. 7 Abs. 2 und Abs. 3]
- die Kreditwürdigkeit eines Verbrauchers durchgeführt wird (EBA-Leitlinie), und
- die Risikobewertung von Verbrauchern und die Preisgestaltung für Verbraucher eine Rolle spielt, also bei Lebens- und Nicht-Lebensversicherungsprodukten (EIOPA-Leitlinie).

– Die EBA „kann" zudem Leitlinien zu anderen Finanzprodukte und -dienstleistungen erarbeiten, wenn sie dies auch Verbraucherschutzgründen für nötig erachtet [Art. 7 Abs. 2]. Auch die ESMA „kann" dies tun [Art. 7 Abs. 3a]

– Die EIOPA soll binnen zwei Jahren nach Inkrafttreten der Verordnung einen Bericht mit einer Analyse der Auswirkungen von bestimmten klimabezogenen Daten und Daten zu Naturkatastrophen auf den Versicherungssektor vorlegen. Auf Basis der Ergebnisse soll sie die oben genannte EIOPA-Leitlinie ggf. anpassen [Art. 7 Abs. 3].

► **Systeme für den Austausch von Finanzdaten (Financial Data Sharing Schemes, FDSS)**

Mitgliedschaft in einem FDSS

– Dateninhaber und Datennutzer müssen einem „Systeme für den Austausch von Finanzdaten" (FDSS) beitreten, welches den Zugang zu Kundendaten regelt. Sie können Mitglied in mehreren FDSS sein. [Art. 9]

– Mitglieder eines FDSS sind Dateninhaber, Datennutzer, Verbraucherorganisationen und -verbände. Verbraucherorganisationen und -verbände haben jedoch nur eine Beratungsfunktion im Hinblick auf Verbraucherschutzangelegenheiten. [Art. 10 Abs. 1 lit. a]

– Ein spezifischer FDSS muss diejenigen Dateninhaber und Datennutzer als Mitglieder aufnehmen, die einen „wesentlichen Anteil" des Marktes eines bestimmten Finanzprodukts bzw. einer bestimmten Finanzdienstleistung abdecken. Die EBA, die EIOPA und die ESMA müssen zur Bestimmung des „wesentlichen Anteils" Leitlinien erarbeiten. [Art. 10 Abs. 1 lit. a]

Governance eines FDSS

– Ein spezifischer FDSS muss [Art. 10 Abs. 1]
- eine faire und unparteiische Vertretung der Dateninhaber und Datennutzer bei Entscheidungs- und Abstimmungsverfahren sicherstellen,

- seine internen Regeln so gestalten, dass sie für alle Mitglieder einheitlich gelten und es keine ungerechtfertigte Vorzugsbehandlung einzelner Mitglieder gibt, und
- allen Dateninhabern und Datennutzern auf Basis objektiver Bedingungen offen stehen.

– FDSS müssen verfügen über [Art. 10 Abs. 1]
- Mechanismen zur Änderung ihrer Regeln,
- Transparenzbestimmungen,
- gemeinsame Standards für Daten und technische Schnittstellen, um einen effizienten Datenzugang zu ermöglichen,
- Regeln für die vertragliche Haftung der Mitglieder,
- Systeme für die Streitbeilegung,
- gemeinsame technische und organisatorische Mindestmaßnahmen für eine sichere Kommunikation und den sicheren Austausch von Kundendaten, und
- technische Schnittstellen mit einem angemessenen Leistungsniveau im Hinblick auf Verfügbarkeit und Leistung.

– Jedes FDSS muss einen Entschädigungsmechanismus vorsehen. Dieser soll es Dateninhabern bzw. Datennutzern ermöglichen Kunden für etwaige Datenverluste, Schäden oder Betrug finanziell zu entschädigen, für die die Dateninhaber bzw. Datennutzer verantwortlich sind [Art. 10 Abs. 1 lit. m].
– Jedes FDSS muss mit den EU-Vorschriften für Verbraucherschutz, Datenschutz, Privatsphäre und Wettbewerb im Einklang stehen [Erwägungsgrund 25].

Vergütungsfragen

– Jedes FDSS muss „Modelle“ zur Bestimmung der „maximalen“ Vergütung etablieren, die ein Dateninhaber für die Bereitstellung von Kundendaten vom Datennutzer verlangen darf. Ein solche Vergütung muss [Art. 10 Abs. 1 lit. h]
- begrenzt sein auf ein „angemessenes“ Niveau; das kann eine Marge beinhalten,
- unmittelbar mit der Bereitstellung der angeforderten Daten zusammenhängen,
- auf einer objektiven, transparenten und nicht-diskriminierenden Grundlage kalkuliert sein, und
- sich an den niedrigsten marktüblichen Werten orientieren.

– Ist der Datennutzer ein Kleinstunternehmen, ein kleines oder ein mittleres Unternehmen darf die Vergütung die Kosten für die Bereitstellung der angeforderten Daten nicht übersteigen. Dies gilt nicht, wenn der Datennutzer ein Partnerunternehmen hat oder zu verbundenen Unternehmen gehört, die nicht als Kleinstunternehmen, kleines oder mittleres Unternehmen gelten. [Art. 10 Abs. 1 lit. h]

Beschränkung der Verfügbarmachung von Kundendaten

– Ein spezifisches FDSS kann eine Beschränkung der Kundendaten beschließen, die im Rahmen des FDSS zur Verfügung gestellt werden. Das gilt für Daten, die zehn Jahre vor einem Ersuchen eines Kunden nach Zugang zu seinen Kundendaten erhoben wurden, sofern [Art. 2 Abs. 1b, Art. 10 Abs. 1 lit. h]
- diese nicht ohne Weiteres in digitaler Form verfügbar sind, oder
- nicht Teil der Vertragsbedingungen des Finanzprodukts oder der Finanzdienstleistung sind.

– Ein spezifisches FDSS kann auch einen längeren Zeitraum als 10 Jahre anwenden, wenn es angesichts der Besonderheiten der jeweiligen Datenkategorie erforderlich erscheint hält [Art. 2 Abs. 1b].
– Die Beschränkung der Verfügbarmachung von Daten greift nicht für [Erwägungsgrund 9a]
- Daten zu den Vertragsbedingungen (z. B. Preisgestaltung oder Versicherungsschutz), und
- Daten zu bereits erfüllten oder beendeten Verträgen zu Finanzprodukten und -dienstleistungen.

Unterrichtung der zuständigen Behörden und der EBA

– Dateninhaber müssen ihre zuständige nationale Behörde innerhalb eines Monats nachdem sie einem FDSS beigetreten sind, darüber unterrichten [Art. 10 Abs. 3].
– Ein FDSS muss innerhalb eines Monats nach seiner Einrichtung die zuständige nationale Behörde hierüber unterrichten. Es ist diejenige Behörde des Mitgliedstaats zuständig, in dem die drei wichtigsten Dateninhaber ansässig sind. [Art. 10 Abs. 4 und 5)]
– Die zuständige Behörde muss binnen eines Monats, ob das FDSS den Anforderungen der Verordnung genügt. Nach Abschluss der Prüfung muss sie die EBA über die Einrichtung des FDSS, dessen Hauptcharakteristika und die Teilnehmer des FDSS informieren. Das FDSS gilt dann als in allen Mitgliedstaaten anerkannt. [Art. 10 Abs. 6]
– Ein FDSS muss jede signifikante Änderung der Funktionsweise eines FDSS den zuständigen Behörden melden, insbesondere im Hinblick auf die erfassten Produkte und Dienstleistungen, die geographische Abdeckung, die Governance und die drei wichtigsten Dateninhaber [Art. 10 Abs. 6].

Zeithorizonte für die Etablierung von FDSS

– Es müssen FDSS zur Verfügung stehen [Art. 36 Abs. 2]

- 18 Monate nach dem Inkrafttreten der Verordnung im Hinblick auf Kundendaten zu
  - Kreditverträge für Verbraucher,
  - Konten,
  - Ersparnissen, und
  - KfZ-Versicherungen; dies umfasst auch Daten zur Analyse der Wünsche und Bedürfnisse der Kunden.
- 30 Monate nach dem Inkrafttreten der Verordnung im Hinblick auf Kundendaten zu
  - Wohnimmobilienkreditverträge für Verbraucher,
  - Anlagen in Finanzinstrumenten; dies umfasst auch Daten zu den Nachhaltigkeitspräferenzen der Kunden sowie Daten, die bei der Eignungs- und Angemessenheitsprüfung erhoben werden,
  - Anlagen in Kryptowerten; dies umfasst auch Daten, die bei der Eignungs- und Angemessenheitsprüfung erhoben werden, und
  - privaten Altersvorsorgeprodukten;
- 42 Monate nach dem Inkrafttreten der Verordnung im Hinblick auf Kundendaten zu
  - Kreditverträgen, die keine Verbraucher- oder Wohnimmobilienkreditverträge für Verbraucher sind,
  - einer Kreditwürdigkeitsprüfung, sofern der Kunde ein Unternehmen ist,
  - Nicht-Lebensversicherungsprodukten mit Ausnahme der Kfz-Versicherung; dies umfasst auch Daten zur Analyse der Wünsche und Bedürfnisse der Kunden und
  - Versicherungsanlageprodukten und versicherungsbasierten individuellen Rentenprodukten, dies umfasst auch Daten zu den Nachhaltigkeitspräferenzen der Kunden sowie Daten, die bei der Eignungs- und Angemessenheitsprüfung erhoben werden.

– Wurden der EBA sechs Monate nach dem jeweiligen Zeitpunkt – 18 Monate, 30 Monate bzw. 42 Monate – für eine oder mehrere Kategorien von Kundendaten kein FDSS gemeldet und ist dies auch absehbar nicht zu erwarten, kann die Kommission die FIDA Verordnung mittels eines delegierten Rechtsakts ergänzen und die Modalitäten selbst festlegen, nach denen die Dateninhaber den Datennutzern diese Kategorie(n) von Kundendaten bereitstellen müssen. [Art. 11]

► **Zulassung und Betriebsbedingungen von FISP**

– Eine juristische Person darf nur dann als FISP auf Kundendaten zugreifen, wenn sie von der zuständigen nationalen Behörde des Mitgliedstaats ihrer Niederlassung, zugelassen wurde. In ihrem Zulassungsantrag müssen sie insbesondere angeben [Art. 12 Abs. 1 und 2]
  - die Art des Finanzinformationsdiensts, den sie erbringen wollen,
  - die Art des beabsichtigten Zugriffs auf Kundendaten,
  - ihren Geschäftsplan,
  - ihre Regelungen zur Unternehmensführung und ihre internen Kontrollmechanismen,
  - eine Beschreibung darüber, wie sie den organisatorischen Anforderungen der Verordnung nachkommen wollen,
  - ihre Verfahren für die Überwachung von Sicherheitsvorfällen, deren Behandlung, Weiterverfolgung und Meldung (in Einklang mit den Anforderungen der DORA-Verordnung (EU) 2022/2554, s. cep**Analyse**),
  - ihre Vorkehrungen zur Aufrechterhaltung des Geschäftsbetriebs und
  - ein Sicherheitskonzept.
– FISP müssen über eine Berufshaftpflichtversicherung oder eine vergleichbare Garantie verfügen, die sie insbesondere in die Lage versetzt, eine mögliche Haftung aufgrund grober Fahrlässigkeit, eines unbefugten oder betrügerischen Datenzugriffs oder -gebrauchs abzudecken [Art. 12 Abs. 3].
– Neben juristischen Personen dürfen auch Unternehmen, die keine juristischen Personen sind, Finanzinformationsdienste erbringen. Dies gilt jedoch nur, wenn ihre Rechtsform einen gleichwertigen Schutz der Interessen Dritter gewährleistet, und sie einer ihrer Rechtsform entsprechenden Aufsicht unterliegen. [Art. 12 Abs. 2]
– „Kontoinformationsdienstleister“ im Sinne der Zahlungsdienste-Richtlinie 2015/2366/EU (s. cep**Analyse**) dürfen nur auf die Kundendaten zugreifen, wenn sie als FISP zugelassen wurden [Art. 12 Abs. 4].
– Will ein Torwächter („Gatekeeper“) oder ein Unternehmen, das im Besitz eines Torwächters ist bzw. von diesem kontrolliert wird, einen Finanzinformationsdienst erbringen, ist der Erhalt einer Zulassung als FISP an eine zusätzliche spezifische Bewertung gebunden [Art. 12 Abs. 4a, Details s. nächster Abschnitt].

► **Spezifische Befugnisse der zuständigen Behörden bezüglich Torwächtern („Gatekeeper“)**

– Torwächter oder Unternehmen, die im Besitz eines Torwächters sind bzw. von diesen kontrolliert werden (im Folgenden: Gatekeeper), die als Datennutzer fungieren, müssen sich innerhalb von sechs Monaten nach Inkrafttreten der FIDA Verordnung einer spezifischen Vorabbewertung unterziehen. Diese wird von einer

zuständigen Behörde durchgeführt, wobei diese mit den drei ESAs –EBA, EIOPA und ESMA – und ggf. der Kommission kooperiert. [Art. 18b]

– Die Behörde muss die Untersuchung auch durchführen, wenn [Art. 18b]
  - der Gatekeeper sich nach der FIDA Verordnung als FISP zulassen will, oder
  - ein Datennutzer, der bis dato kein Gatekeeper ist, zu einem Gatekeeper wird.
– Gatekeeper dürfen erst dann als Datennutzer fungieren oder eine Zulassung als FISP erhalten, wenn die zuständige Behörde die spezifischen Vorabbewertung abgeschlossen und eine endgültige Entscheidung gefällt hat [Art. 18b].
– Im Rahmen der spezifischen Vorabbewertung analysiert die Behörde [Art. 18b]
  - den Geschäftsplan des Gatekeepers, die Funktionsweise, die Dienste und die Tätigkeiten des Gatekeepers als Datennutzer und den Umfang der Tätigkeit des Gatekeepers im Hinblick auf die Zahl erreichter Kunden,
  - die durch den Zugang des Gatekeepers zu Kundendaten entstehenden Netzwerkeffekte und datengesteuerten Vorteile;
  - ob der Gatekeeper nachgewiesen über ausreichende Sicherheitsvorkehrungen verfügt,
  - ob der Gatekeeper nachgewiesen über ausreichende IT-, Governance- und organisatorische Schutzmaßnahmen verfügt und jederzeit und dauerhaft gewährleistet ist, dass der Gatekeeper die Kundendaten von anderen Daten getrennt hat.
– Die zuständige Behörde hat 60 Arbeitstage Zeit für die spezifische Vorabbewertung. Spätestens zehn Arbeitstage nach Abschluss ihrer Bewertung übermittelt sie eine Kopie der Bewertung an die EBA, ESMA bzw. die EIOPA. Daraufhin haben die EBA, ESMA bzw. die EIOPA 60 Tage Zeit zu dieser Bewertung Stellung zu nehmen. Weicht diese von der Bewertung der zuständigen Behörde ab, sollte sie dies ausführlich begründen. Sodann hat die zuständige Behörde maximal 30 Arbeitstage Zeit für den finalen Abschluss der Bewertung, deren Ergebnis sie dem Gatekeeper sodann unverzüglich mitteilen muss. [Art. 18b]
– Gelingt es dem Gatekeeper die spezifische Vorabuntersuchung zu überstehen, muss die zuständige Behörde ihm erlauben, als Datennutzer fungieren zu dürfen bzw. eine Zulassung als FISP zu erhalten. Gelingt es dem Gatekeeper nicht, hat dieser die Möglichkeit binnen 30 Arbeitstagen die Unzulänglichkeiten anzugehen. Erfüllt der Gatekeeper auch dann die Anforderungen nicht, muss die Behörde es dem Gatekeeper verbieten, als Datennutzer fungieren zu dürfen bzw. darf ihn nicht als FISP zulassen. [Art. 18b]

► **Zeitpunkt der Anwendung der Verordnung**

Die Verordnung soll stufenweise Anwendung finden („phase in approach“) [Erwägungsgrund 53]. Sie gilt jeweils sechs Monate nachdem die entsprechenden FDSS zur Verfügung stehen müssen (s. oben), also entweder 24 Monate, 36 Monate oder 48 Monate nach Inkrafttreten der Verordnung [Art. 36 Abs. 2].