Digitaler Euro und Datenschutz

Eine datenschutzrechtliche Betrachtung der Umsetzungskonzepte des digitalen Euro

Dr. Daniel Schmid | Akademischer Rat a.Z. | Juristische Fakultät der Universität Augsburg

04. Januar 2021

LR 2021, Seiten 1 bis 15 (insgesamt 15 Seiten)

I. Einleitung

Am 12. Oktober 2020 veröffentlichte die Europäische Zentralbank (EZB) einen Bericht[1] über den sog. „digitalen Euro". Der Bericht wurde von einer Task Force erstellt, die im Januar 2020 von dem Regierungsrat der EZB eingesetzt wurde. In diesem Bericht wird u.a. auf Fragen der Erforderlichkeit, des Nutzens, des rechtlichen Rahmens und der technischen Umsetzung des digitalen Euro eingegangen.

Der digitale Euro ist eine sog. „central bank digital currency (CBDC)", also eine digitale Währung einer Zentralbank, und somit eine Verbindlichkeit des Eurosystems, die in digitaler Form als Ergänzung zu Bargeld und Zentralbankeinlagen erfasst wird. Der digitale Euro würde eine weitere Möglichkeit sein, den Euro auszuliefern und wäre keine neue Parallelwährung. Die EZB legt sich noch nicht auf eine technische Umsetzung des digitalen Euro fest; sie möchte vielmehr im Rahmen einer Testphase bis Mitte 2021 die Frage beantworten, ob die Arbeit an der Umsetzung des digitalen Euro fortgesetzt werden soll.[2] Die Bürger der Europäischen Union werden derzeit im Rahmen einer Umfrage an der Frage der Einführung des digitalen Euro beteiligt.[3]

Der Bericht über den digitalen Euro erläutert diverse Konzepte für die technische Umsetzung des digitalen Euro, u.a. werden Ansätze für eine Online- und eine Offline-Nutzung des digitalen Euro betrachtet. Bei der Schaffung des digitalen Euro sollen gewisse durch die Task Force erarbeiteten Prinzipien[4] eingehalten werden.

[1] *European Central Bank (ECB),* Report on a digital euro (letzter Aufruf: 31.12.2020).
[2] *ECB,* Fn. 1, S. 1 ff.
[3] *Heise online News,* EZB startet Bürgerumfrage zu digitalem Euro (letzter Aufruf: 31.12.2020).
[4] *ECB,* Fn. 1, S. 2, 48 ff.

Dieser Beitrag stellt zunächst die von der Task Force genannten Gründe für die Einführung des digitalen Euro vor (II.). Danach werden die diversen, in dem Bericht aufgeworfenen Konzepte des digitalen Euro betrachtet (III.). Anschließend erfolgt eine Einschätzung, welche datenschutzrechtlichen Implikationen mit den jeweiligen Umsetzungskonzepten verbunden sind (IV.). Schließlich folgt ein kurzes Fazit (V.).

II. Gründe für die Einführung des digitalen Euro

Es stellt sich die Frage, warum die EZB neben Bargeld und Zentralbankeinlagen den digitalen Euro anbieten möchte. Die Task Force führt in ihrem Bericht dazu an, dass die Ausgabe des digitalen Euro eine Möglichkeit sein könnte, die Digitalisierung der Wirtschaft zu fördern und die Entwicklung innovativer europäischer Lösungen in allen möglichen Branchen zu unterstützen.[5] Daneben könnte ein digitaler Euro die Antwort auf den Rückgang der Nutzung von Bargeld sein.[6] Mit der Einführung des digitalen Euro könnte die EZB der Gefahr entgegentreten, dass der europäische Finanzmarkt durch das großflächige Aufkommen einer außereuropäischen digitalen Zentralbankwährung oder privater Kryptowährungen, wie bspw. Bitcoin oder Libra, an Stabilität einbüßt.[7] Die Einführung des digitalen Euro könnte außerdem auch eine Notwendigkeit oder ein Vorteil in geldpolitischer Hinsicht sein, weil die EZB den Zinssatz für den digitalen Euro festlegen könnte.[8] Der digitale Euro könnte weiterhin dazu dienen, negative Auswirkungen auf die Bereitstellung von Zahlungsdiensten bspw. durch Cyber-Attacken, Naturkatastrophen, Pandemien oder andere extreme Vorfälle zu minimieren.[9] Letzten Endes könnte die Einführung des digitalen Euro die internationale Rolle des Euro stärken und Verbesserungen bezüglich der Gesamtkosten und des ökologischen Fußabdrucks der Geld- und Bezahlsysteme bewirken.[10]

III. Technische Umsetzung des digitalen Euro

Für die Einführung des digitalen Euro kommen laut Task Force diverse technische Umsetzungskonzepte in Betracht. Die Task Force legt sich noch nicht auf ein spezifisches Umsetzungskonzept fest, sondern lotet zunächst vielmehr die diversen Umsetzungsmöglichkeiten aus. Da bei der technischen Umsetzung des digitalen Euro möglichst viele der oben erwähnten Prinzipien[11] umgesetzt werden sollen, kommen zwei grundlegende Umsetzungsarten des digitalen Euro in Betracht: offline und online. Beide Umsetzungsarten könnten aber gleichzeitig angeboten werden und könnten kompatibel

[5] *ECB*, Fn. 1, S. 9 f.
[6] *ECB*, Fn. 1, S. 10 f.
[7] *ECB*, Fn. 1, S. 11 f.
[8] *ECB*, Fn. 1, S. 12 f.
[9] *ECB*, Fn. 1, S. 13 f.
[10] *ECB*, Fn. 1, S. 14 f.
[11] *ECB*, Fn. 1, S. 2, 48 ff.

ausgestaltet werden. Eine derartige Kompatibilität würde dann aber eine Synchronisation zwischen der Offline- und der Online-Umsetzung des digitalen Euro erfordern.[12]

1. Offline-Umsetzung

Die Offline-Umsetzung des digitalen Euro könnte bspw. folgendermaßen aussehen: Person A lädt auf ein vertrauenswürdiges Hardware-Modul (bspw. eine Smart-Card oder ein tragbares Gerät) einen Teil der ihr in ihrem Online-Konto bzw. -Account zugeordneten digitalen Euro herunter. Person A geht in das Geschäft der Person B und möchte dort einen Artikel erwerben. Beim Bezahlvorgang hält Person A ihr Hardware-Modul an das Bezahlterminal der Person B und der Kaufpreis wird durch eine Direktverbindung (bspw. über Near Field Communication, kurz NFC) zwischen Hardware-Modul und Bezahlterminal von Person A an Person B offline transferiert. In regelmäßigen Abständen verbindet Person B das Bezahlterminal mit dem Internet und lädt die darauf offline gespeicherten digitalen Euro in ihr Online-Konto bzw. in ihren Online-Account hoch.[13]

2. Online-Umsetzung

Die Online-Umsetzung des digitalen Euro könnte webbasiert erfolgen. Somit wäre für die Online-Nutzung des digitalen Euro kein spezielles Endgerät erforderlich; vielmehr könnten PCs, Notebooks und Smartphones genutzt werden. Bei der Online-Infrastruktur gibt es vier Umsetzungskonzepte, die man in zwei Gruppen einteilen kann: a) unter Nutzung einer zentralen Infrastruktur und b) unter Nutzung einer dezentralen Infrastruktur. Da das Back-End letztlich aber immer von der EZB kontrolliert werden soll, hätte selbst die im Report „dezentral" genannte Infrastruktur eine zentrale Komponente.[14]

a) Zentrale Infrastruktur

Bei der zentralen Infrastruktur zeigt die Task Force zwei Umsetzungsmöglichkeiten auf: einen direkten Zugang zum digitalen Euro bei der EZB selbst oder einen vermittelten Zugang über von der EZB überwachte Intermediäre (die wie im bisherigen Bankensystem die einzelnen Bankfilialen wären). Findet zwischen zwei Endkunden ein Transfer von digitalen Euro statt, würde dieser Vorgang bei einer zentralen Infrastruktur von einem Dritten, namentlich der EZB bzw. den Intermediären, validiert.[15]

[12] *ECB*, Fn. 1, S. 26, 34 f.
[13] *ECB*, Fn. 1, S. 31 f.
[14] *ECB*, Fn. 1, S. 26 f., 29 ff.
[15] *ECB*, Fn. 1, S. 29 f., 37 ff.

aa) Direktes Modell

Bei dem direkten Zugang zu der EZB (im Folgenden als „direktes Modell" bezeichnet) würde die EZB selbst den digitalen Euro direkt an die Endkunden ausgeben. Die Endkunden hätten also bei der EZB selbst ein Online-Konto bzw. einen Online-Account. In diesem Szenario könnten – wie auch im Intermediär-Modell (siehe III. 2. a) bb)) – Intermediäre eingesetzt werden. Diese wären aber allenfalls eine Art Wächter über den Zugang der Endkunden zur EZB.[16]

bb) Intermediär-Modell

Bei dem indirekten Zugang über Intermediäre (im Folgenden als „Intermediär-Modell" bezeichnet) würde die EZB weiterhin nur mit von ihr überwachten Intermediären direkt interagieren. Die Intermediäre würden als Abwicklungsagenten fungieren und Transaktionen im Auftrag ihrer jeweiligen Endkunden anweisen. Die EZB hätte auch bei diesem Modell weiterhin die volle Kontrolle über den digitalen Euro. Die Anzahl an Verbindungen zwischen den Gegenstellen und der EZB wäre – im Gegensatz zum direkten Modell – aber auf die Anzahl der beteiligten Intermediäre beschränkt.[17]

Die Task Force hält das Intermediär-Modell für vorzugswürdig, da die EZB bei diesem Ansatz keine neue Infrastruktur aufbauen müsste. Die EZB könnte vielmehr die schon bestehende Infrastruktur zwischen ihr und den Intermediären aus dem bestehenden Banksystem nutzen.[18]

b) Dezentrale Infrastruktur

Bei der dezentralen Infrastruktur sind wiederum zwei Umsetzungsmöglichkeiten denkbar: direkter Zugang der Endkunden zu dem digitalen Euro oder ein hybrides Modell. Da aber die Kontrolle über das Back-End immer bei der EZB liegen soll, ist selbst bei den dezentralen Modellen immer eine zentrale Komponente enthalten. Der Bericht erkennt offenbar diese Divergenz selbst, indem er davon spricht, dass eine Infrastruktur mit „etwas Dezentralisierung" erreicht werden könne.[19]

aa) Endkunden-Modell

Der direkte Zugang der Endkunden in einer „dezentralen" Infrastruktur mit der EZB als Back-End (im Folgenden als „Endkunden-Modell" bezeichnet) könnte entweder auf der Blockchain-

[16] *ECB*, Fn. 1, S. 38.
[17] *ECB*, Fn. 1, S. 39.
[18] *ECB*, Fn. 1, S. 26.
[19] *ECB*, Fn. 1, S. 39.

Technologie[20] oder auf lokalen Speichermedien (bspw. durch die Nutzung von Prepaid Karten oder Smartphone-Funktionen, siehe auch Offline-Nutzung, III. 1.) aufsetzen. Bei diesem Modell würde der Transfer digitaler Euro nicht – wie bei den zentralen Modellen – von einem Dritten validiert. Vielmehr müsste die Validierung des Transfers des digitalen Euro zwischen Transaktionssender und -empfänger stattfinden.[21]

bb) Hybrid-Modell

Das Hybrid-Modell zeichnet sich dadurch aus, dass die Blockchain-Technologie auf Ebene der Intermediäre zum Einsatz kommt. Hier findet also die Validierung der Transfers von digitalen Euro über eine Blockchain-Infrastruktur der Intermediäre statt.[22]

IV. Datenschutzrechtliche Einschätzung

Im Folgenden wird eine datenschutzrechtliche Einschätzung der Umsetzungs-Modelle für den digitalen Euro gegeben. Datenschutzrechtlicher Maßstab für die Verarbeitung von personenbezogenen Daten durch die EZB ist die Verordnung (EU) 2018/1725[23]. Auf Verarbeitungsvorgänge personenbezogener Daten durch die Intermediäre findet die Datenschutz-Grundverordnung (DS-GVO)[24] Anwendung.

1. Datenverarbeitungsvorgänge bei der Nutzung des digitalen Euro

Bevor eine datenschutzrechtliche Einschätzung erfolgen kann, müssen zunächst die Datenverarbeitungsvorgänge betrachtet werden, die im Zusammenhang mit dem digitalen Euro vonstattengehen.

Der erste Schritt für eine Person, die den digitalen Euro als Zahlungsmittel verwenden möchte, ist das Eröffnen eines Online-Kontos bzw. -Accounts bei der EZB (beim direkten Modell und Endkunden-Modell) oder bei einem von der EZB überwachten Intermediär (beim Intermediär-Modell und Hybrid-Modell). Dabei muss die Person regelmäßig personenbezogene Daten, wie bspw. ihren Namen, ihre Anschrift bzw. ihre Mail-Adresse, angeben. Bei der Eröffnung des

[20] Zum Datenschutz bei Einsatz der Blockchain-Technologie für Bezahlvorgänge: siehe *Schmid*, in: Maume/Maute (Hrsg.), Rechtshandbuch Kryptowerte, 2020, § 16.
[21] *ECB*, Fn. 1, S. 40 f.
[22] *ECB*, Fn. 1, S. 41.
[23] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG.
[24] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

Online-Kontos bzw. -Accounts werden also durch die EZB oder durch die Intermediäre personenbezogene Daten des Nutzers erhoben.

Weitere Datenverarbeitungsvorgänge finden bei dem Transfer von digitalen Euro statt. Beim direkten Modell und beim Endkunden-Modell verarbeitet die EZB die personenbezogenen Daten vom Transaktionssender und -empfänger, beim Intermediär-Modell und beim Hybrid-Modell die jeweiligen Intermediäre, die jeweils zwischen Transaktionssender und -empfänger und der EZB geschaltet sind.

Bei der Offline-Nutzung des digitalen Euro findet nur dann eine Verarbeitung von personenbezogenen Daten statt, wenn die Hardware-Geräte den Transfervorgang in irgendeiner Weise aufzeichnen und bspw. neben der Summe an digitalen Euro, die übertragen wurde, auch die Geräte-ID der von Transaktionssender -und -empfänger verwendeten Geräte und den Zeitpunkt der Transaktion speichern.

2. Anwendungsbereich der VO (EU) 2018/1725 bzw. der DS-GVO

a) Sachlicher Anwendungsbereich

aa) Verarbeitung von personenbezogenen Daten

Damit die jeweiligen datenschutzrechtlichen Normen der VO (EU) 2018/1725 bzw. der DS-GVO anwendbar sind, muss der sachliche Anwendungsbereich der VO (EU) 2018/1725 bzw. der DS-GVO eröffnet sein. Der sachliche Anwendungsbereich ist für die Verarbeitungsvorgänge der EZB in Art. 2 VO (EU) 2018/1725 und für die Verarbeitungsvorgänge der Intermediäre in Art. 2 DS-GVO geregelt. Die sachliche Anwendbarkeit der VO (EU) 2018/1725 und der DS-GVO ist jeweils dann gegeben, wenn personenbezogene Daten verarbeitet werden. Eine Verarbeitung ist jeder Vorgang im Zusammenhang mit den personenbezogenen Daten, von dem Erheben der personenbezogenen Daten über Zwischenschritte wie Übermittlung oder Nutzung bis hin zur Löschung der Daten (Art. 3 Nr. 3 VO (EU) 2018/1725 bzw. Art. 4 Nr. 2 DS-GVO).

bb) Vorliegen von personenbezogenen Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person, den sog. „Betroffenen", beziehen (Art. 3 Nr. 1 Hs. 1 VO (EU) 2018/1725 bzw. Art. 4 Nr. 1 Hs. 1 DS-GVO). Daten, die sich auf eine identifizierte Person beziehen, benennen diese konkret.[25] Ist die Person nicht konkret benannt, kann trotzdem ein Personenbezug bestehen, wenn die Person identifizierbar ist. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer

[25] *Gola*, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 4.

Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 3 Nr. 1 Hs. 2 VO (EU) 2018/1725 bzw. Art. 4 Nr. 1 Hs. 2 DS-GVO). Eine Person ist also dann identifizierbar, wenn die Ermittlung der Identität der Person – möglicherweise über mehrere Zwischenschritte – möglich ist.[26] Bei der Frage nach der Identifizierbarkeit sind nach der Rechtsprechung des EuGH[27] nicht nur die Kenntnisse und Möglichkeiten des Verarbeiters selbst zu berücksichtigen, sondern darüber hinaus auch Zusatzwissen von dritten Personen, auf das der Verarbeiter ohne großen Aufwand zugreifen kann. Außerdem sind Informationen Dritter einzubeziehen, wenn der Verarbeiter über rechtliche Mittel verfügt, auf diese Daten zuzugreifen.[28]

cc) Anonymität und Pseudonymität

Die VO (EU) 2018/1725 und die DS-GVO finden keine Anwendung auf anonyme Daten. Anonymität liegt im datenschutzrechtlichen Sinne aber nur dann vor, wenn der Datenverarbeiter die Zuordnung der Daten zu einem Betroffenen nicht (mehr) vornehmen kann.[29] Ist eine Zuordnung noch möglich, liegen pseudonyme Daten vor. Gemäß Art. 3 Nr. 6 VO (EU) 2018/1725 bzw. Art. 4 Nr. 5 DS-GVO liegt eine Pseudonymisierung von Daten vor, wenn die Verarbeitung personenbezogener Daten in einer Weise vorgenommen wird, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Somit liegen bei einer Pseudonymisierung von Daten weiterhin personenbezogene Daten vor, sodass auf Verarbeitungsvorgänge dieser Daten die VO (EU) 2018/1725 bzw. die DS-GVO sachlich Anwendung findet.

dd) Sachlicher Anwendungsbereich bei der Online-Umsetzung

Beim Anlegen eines Online-Kontos bzw. -Accounts bei der EZB (beim direkten Modell und Endkunden-Modell) bzw. bei den Intermediären (beim Intermediär-Modell und Hybrid-Modell) werden Daten des Endkunden, wie bspw. sein Name, seine Anschrift bzw. seine die Mail-Adresse, erhoben, die den Endkunden identifizieren. Es handelt sich also bei den erhobenen Daten um personenbezogene Daten. Auch bei den Online-Transaktionen von digitalen Euro werden personenbezogene Daten erhoben. Dies ist selbst dann der Fall, wenn bei der Durchführung der Transaktionen nicht Klarnamen verwendet werden, sondern bspw. eine Kontonummer, da für die EZB bzw. für die Intermediäre eine Zuordnung der Kontonummer zu

[26] *Gola*, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 5.
[27] *EuGH*, ZD 2017, 24.
[28] *EuGH*, ZD 2017, 24 Rn. 49.
[29] Erwägungsgrund 26 DS-GVO.

einer natürlichen Person (dem Endkunden) möglich ist und damit der Endkunde identifiziert werden kann. Somit ist für diese Verarbeitungsvorgänge der sachliche Anwendungsbereich der VO (EU) 2018/1725 bzw. der DS-GVO eröffnet.

ee) Sachlicher Anwendungsbereich bei der Offline-Umsetzung

Ob auch bei Offline-Transaktionen der sachliche Anwendungsbereich eröffnet ist, hängt von der konkreten technischen Umsetzung ab. Werden durch die Hardware-Module beim Transfer von digitalen Euro neben der Summe der transferierten digitalen Euro keine weiteren Daten, wie bspw. die Geräte-ID der beteiligten Geräte oder der Zeitpunkt der Transaktion übertragen, werden keine personenbezogenen Daten beim Transfer verarbeitet. Der Transfer findet dann also anonym statt und die VO (EU) 2018/1725 bzw. die DS-GVO findet daher keine Anwendung. Selbst durch den Einsatz von Big Data-Anwendungen könnten Transaktionssender und Transaktionsempfänger nicht bestimmt werden. Bei einer Offline-Umsetzung des digitalen Euro, bei der bei einem Transfer allein die Summe der transferierten Euro übertragen wird, können die EZB bzw. die Intermediäre nur die Gesamtsumme der hoch- bzw. heruntergeladenen digitalen Euro der Transaktionssender und -empfänger nachvollziehen, nicht aber die Transferhistorie. Wenn ein Endkunde nur eine Teilsumme der heruntergeladenen digitalen Euro an eine andere Person überträgt und nicht die vollständige Summe, sind für die EZB bzw. die Intermediäre die einzelnen mit dem heruntergeladenen digitalen Euro durchgeführten Transaktionen nicht mehr nachvollziehbar.

Die Situation ist anders zu beurteilen, wenn beim Transfer der digitalen Euro die Geräte-ID der am Transfer beteiligten Hardware-Module, der Zeitpunkt des Transfers und die Summe der Transaktion auf den Hardware-Modulen gespeichert werden und beim Synchronisationsvorgang entweder zur EZB oder zu den Intermediären übertragen werden. Aus diesen gespeicherten Daten können die EZB bzw. die Intermediäre nachvollziehen, welcher Endkunde zu welchem Zeitpunkt welche Summe an digitalen Euro an welchen anderen Endkunden transferiert hat. Bei dieser Art von Offline-Umsetzung wären die auf den Hardware-Modulen gespeicherten Daten personenbezogene Daten und die VO (EU) 2018/1725 bei einer Verarbeitung der personenbezogenen Daten durch die EZB bzw. die DS-GVO bei einer Verarbeitung der personenbezogenen Daten durch die Intermediäre anwendbar.

b) Räumlicher Anwendungsbereich

Da die VO (EU) 2018/1725 gem. ihres Art. 2 nur für die Verarbeitung personenbezogener Daten durch alle Organe und Einrichtungen der Union gilt, wird durch diese Norm automatisch der räumliche Anwendungsbereich eingegrenzt.

Die DS-GVO ist dagegen räumlich anwendbar, wenn personenbezogene Daten im Rahmen der Tätigkeit einer Niederlassung innerhalb der Europäischen Union verarbeitet werden

(Sitzlandprinzip[30] bzw. Niederlassungsprinzip[31], Art. 3 Abs. 1 DS-GVO), oder wenn ein nicht in der Europäischen Union niedergelassener Verantwortlicher oder Auftragsverarbeiter seine Waren oder Dienstleistungen auf die Europäische Union ausrichtet und betroffenen Personen anbietet oder das Verhalten der betroffenen Personen beobachtet (Marktortprinzip[32], Art. 3 Abs. 2 DS-GVO).

Der räumliche Anwendungsbereich der DS-GVO ist somit mit der datenschutzrechtlichen Stellung der Beteiligten verknüpft. Damit ist der räumliche Anwendungsbereich davon abhängig, wer bei den Verarbeitungsvorgängen Verantwortlicher oder Auftragsverarbeiter ist. Erfolgen die Datenverarbeitungsvorgänge im Rahmen der Tätigkeiten einer Niederlassung des Verantwortlichen oder des Auftragsverarbeiters bzw. bieten diese ihre Waren oder Dienstleistungen den betroffenen Personen in der Europäischen Union an, ist die DS-GVO räumlich anwendbar.

3. Datenschutzrechtliche Stellung der Beteiligten

a) Beteiligte nach der VO (EU) 2018/1725 und der DS-GVO

Die VO (EU) 2018/1725 und die DS-GVO kennen bei der Verarbeitung personenbezogener Daten als Beteiligte den Betroffenen, den für die Verarbeitung Verantwortlichen, den Auftragsverarbeiter und den Dritten.

Betroffener ist die identifizierte oder identifizierbare Person, deren Daten verarbeitet werden (Art. 3 Nr. 1 VO (EU) 2018/1725 bzw. Art. 4 Nr. 1 DS-GVO). Unter diesen Personenkreis können auch Nicht-EU-Bürger fallen, wenn eine Verarbeitung der personenbezogenen Daten der Betroffenen durch Verantwortliche oder Auftragsverarbeiter innerhalb des räumlichen Anwendungsbereichs stattfindet.[33]

Verantwortlicher ist das Organ oder die Einrichtung der Union oder die Generaldirektion oder sonstige Organisationseinheit bzw. die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, das bzw. die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 3 Nr. 8 VO (EU) 2018/1725 bzw. Art. 4 Nr. 7 DS-GVO). Verantwortlicher ist also, wer die faktische Bestimmungsmacht über die Zwecke und Mittel hat.[34] Der Zweck der Verarbeitung ist dabei das erwartete Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet, also das „Warum". Das Mittel der

[30] *Piltz*, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 3 Rn. 5.
[31] *Klar*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 3 Rn. 2.
[32] *Piltz*, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 3 Rn. 5; *Klar*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 3 Rn. 3.
[33] *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 4 Nr. 1 Rn. 3.
[34] *Art. 29-Datenschutzgruppe*, WP 169, S. 1 und 11 ff. (zuletzt aufgerufen 31.12.2020); *Martini/Weinzierl*, NVwZ 2017, 1251 (1253).

Verarbeitung ist die Art und Weise, wie ein Ergebnis oder Ziel erreicht wird, also das „Wie".[35] Die Entscheidungsmacht über die Zwecke der Verarbeitung führt grundsätzlich zu einer Einordnung des Datenverarbeiters als für die Verarbeitung Verantwortlichen, während eine Entscheidung über die Mittel nur dann die Verantwortung für die Verarbeitung impliziert, wenn über wesentliche Aspekte der Mittel entschieden wird. Daher ist es durchaus möglich, dass der Auftragsverarbeiter über die technischen und organisatorischen Mittel entscheidet.[36] Wenn zwei oder mehrere Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung festlegen, sind diese gemeinsam Verantwortliche i.S.v. Art. 28 VO (EU) 2018/1725 bzw. Art. 26 DS-GVO.

Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 3 Nr. 12 VO (EU) 2018/1725 bzw. Art. 4 Nr. 8 DS-GVO). Auftragsverarbeiter verarbeiten ebenso wie Verantwortliche personenbezogene Daten. Der Unterschied zwischen Auftragsverarbeiter und Verantwortlichen besteht darin, dass Auftragsverarbeiter nicht über die Zwecke und nur in beschränktem Maße über die Mittel der Verarbeitung bestimmen können. Außerdem unterliegen Auftragsverarbeiter den Weisungen des Verantwortlichen.[37]

Dritter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten (Art. 3 Nr. 14 VO (EU) 2018/1725 bzw. Art. 4 Nr. 10 DS-GVO).

b) Offline-Modell

Würde die technische Umsetzung des Offline-Modell so ausgestaltet, dass personenbezogene Daten erhoben werden und die VO (EU) 2018/1725 bzw. die DS-GVO sachlich anwendbar sind (siehe IV. 2. a)), wären Transaktionssender und -empfänger die Betroffenen, da ihre personenbezogenen Daten erhoben werden. Je nachdem, ob bei der EZB oder bei den Intermediären das Online-Konto bzw. der Online-Account des digitalen Euro besteht, ist die EZB oder der jeweilige Intermediär der datenschutzrechtlich Verantwortliche, da diese die Zwecke und Mittel der Datenverarbeitungsvorgänge festlegen.

c) Direktes Modell

Beim direkten Modell ist die EZB Verantwortliche sowohl für die Verwaltung der Nutzerkonten, als auch für die durchgeführten Transaktionen des digitalen Euro, da die EZB die Zwecke und

[35] *Art. 29-Datenschutzgruppe*, WP 169, S. 16 (zuletzt aufgerufen 31.12.2020).
[36] *Art. 29-Datenschutzgruppe*, WP 169, S. 17 f. (zuletzt aufgerufen 31.12.2020).
[37] *Art. 29-Datenschutzgruppe*, WP 169, S. 30 f. (zuletzt aufgerufen 31.12.2020).

die Mittel für diese Datenverarbeitungsvorgänge festlegt. Werden Intermediäre als eine Art Wächter für den Zugang zur EZB eingesetzt, sind diese Auftragsverarbeiter, da sie nur den Zugang zur EZB durchleiten und nicht selbst die Zwecke und Mittel von etwaigen Datenverarbeitungsvorgängen bestimmen. Die Endkunden sind schließlich die Betroffenen, da ihre personenbezogenen Daten verarbeitet werden.

d) Intermediär-Modell

Beim Intermediär-Modell gibt es zwei Verantwortliche, nämlich die jeweiligen Intermediäre und die EZB. EZB und die Intermediäre sind dabei aber nicht gemeinsam Verantwortliche nach Art. 28 VO (EU) 2018/1725 bzw. Art. 26 DS-GVO, da die Intermediäre und die EZB nicht dieselben Zwecke und Mittel für die Verarbeitung verfolgen. Es finden vielmehr getrennt voneinander zwei Datenverarbeitungsvorgänge statt, nämlich zum einen Vorgänge zwischen Endkunden und den jeweiligen Intermediären, die sowohl im Rahmen der Verwaltung der Kundendaten als auch bei Transaktionen stattfinden, und zum anderen Vorgänge zwischen den jeweiligen Intermediären und der EZB. Die Intermediäre sind für erstere die Verantwortlichen, während die EZB für letztere Verantwortliche ist. Dies ist darin begründet, dass die Intermediäre die Zwecke und Mittel der Verarbeitungsvorgänge mit den personenbezogenen Daten der Endkunden selbst bestimmen. Da letztlich die EZB den digitalen Euro ausgibt und für Verarbeitungsvorgänge, die diesen betreffen, die Mittel und Zwecke gegenüber den Intermediären bestimmt, ist aber ebenfalls die EZB Verantwortliche. Die Endkunden sind auch hier wieder die Betroffenen.

e) Endkunden-Modell

Die EZB legt als der Initiatorin einer zentralen Blockchain[38] mit ihrem Back-End die Zwecke und die Mittel für die Datenverarbeitungsvorgänge fest, die innerhalb der Blockchain, deren Teilnehmer die Endkunden sind, durchgeführt werden. Neben den Verarbeitungsvorgängen bei Transaktionen fällt darunter auch die Verwaltung der Kundendaten. Bei dem Endkunden-Modell initiiert zwar der jeweilige Transaktionssender die Transaktion und legt fest, an welchen Transaktionsempfänger er welche Summe übertragen möchte. Letztlich kann der Transaktionssender aber nicht frei die Mittel des Transfers von digitalen Euro wählen, vielmehr stellt die EZB dem Transaktionssender die Mittel über das Back-End zur Verfügung. Die EZB kann außerdem jederzeit die Programmierung der Blockchain ändern oder dem Endkunden den Zugriff auf die Blockchain entziehen. Daher ist die EZB als Verantwortliche anzusehen.[39] Werden auch hier wiederum Intermediäre als Art Wächter eingesetzt, sind diese Auftragsverarbeiter.

[38] Da die EZB das Back-End stellt, liegt hier keine dezentrale Blockchain vor, auch wenn die Transaktionen von Transaktionssender und -empfänger validiert werden.
[39] So auch *Finck*, EDPL 2018, 17 (26); *Martini/Weinzierl*, NVwZ 2017, 1251 (1254).

f) Hybrid-Modell

Das Hybrid-Modell kann mit der Durchführung von On-Chain-Transaktionen auf einer zentralen Blockchain unter Nutzung von Trading-Plattformen verglichen werden.[40] Da die EZB über das Back-End die Zwecke und Mittel festlegt (siehe IV. 3. e)), ist die EZB Verantwortliche. Die Intermediäre dagegen bestimmen nicht die Zwecke und Mittel der Datenverarbeitung. Die Intermediäre sind aber auch nicht Betroffene, da nicht ihre eigenen Daten, sondern die personenbezogenen Daten der Endkunden verarbeitet werden. Vielmehr sind Intermediäre in dieser Konstellation auch wieder Auftragsverarbeiter, die Endkunden wiederum die Betroffenen.

4. Zulässigkeit der Datenverarbeitung

a) Erlaubnistatbestände in der VO (EU) 2018/1725 und in der DS-GVO

Die VO (EU) 2018/1725 und die DS-GVO folgen dem Grundsatz des Verbotsprinzips mit Erlaubnisvorbehalt. Das bedeutet, dass grundsätzlich jede Verarbeitung von personenbezogenen Daten einer natürlichen Person unzulässig ist. In der VO (EU) 2018/1725 sind in Art. 5, in der DS-GVO sind in Art. 6 Erlaubnistatbestände geregelt, bei deren Vorliegen eine Verarbeitung personenbezogener Daten zulässig ist.

Grundsätzlich käme für alle Modelle als Erlaubnistatbestand eine Einwilligung des Betroffenen gem. Art. 5 Abs. 1 lit. d) VO (EU) 2018/1725 bzw. Art. 6 Abs. 1 lit. a) DS-GVO in Betracht. Die Voraussetzungen einer wirksamen Einwilligung sind in Art. 7 VO (EU) 2018/1725 bzw. Art. 7 DS-GVO geregelt. Demnach muss der Betroffene freiwillig im Rahmen einer informierten Entscheidung in die Verarbeitung seiner personenbezogenen Daten einwilligen. Problematisch bei einer Einwilligung ist allerdings, dass sie jederzeit widerrufbar ist, was zur Folge hat, dass Verarbeitungsvorgänge, die nach Ausüben des Widerrufs der Einwilligung durchgeführt werden, nicht mehr auf Basis des Erlaubnistatbestandes der Einwilligung durchgeführt werden dürfen. Um die Betroffenen nicht zu verwirren (wenn ein weiterer Erlaubnistatbestand für die Verarbeitung besteht), sollten Verarbeitungsvorgänge – wenn möglich – aufgrund dieses Gesichtspunkts auf andere Erlaubnistatbestände gestützt werden.

Hierfür in Betracht kämen Art. 5 Abs. 1 lit. c) VO (EU) 2018/1725 bzw. Art. 6 Abs. 1 lit. b) DS-GVO und Art. 5 Abs. 1 lit. b) VO (EU) 2018/1725 bzw. Art. 6 Abs. 1 lit. c) DS-GVO. Gem. Art. 5 Abs. 1 lit. c) VO (EU) 2018/1725 bzw. Art. 6 Abs. 1 lit. b) DS-GVO ist eine Verarbeitung auch dann rechtmäßig, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist. Das kommt immer dann in Betracht, wenn zwischen Verantwortlichem und Betroffenen ein Vertragsverhältnis besteht und im Rahmen dessen die Verarbeitung der personenbezogenen Daten des Betroffenen erforderlich ist, weil andernfalls

[40] Siehe für Details: *Schmid*, in: Maume/Maute (Hrsg.), Rechtshandbuch Kryptowerte, 2020, § 16 Rn. 42.

der Verantwortliche seinen Pflichten aus dem Vertrag mit dem Betroffenen nicht nachkommen könnte. So ist es bspw. bei dem Kauf einer Ware über das Internet erforderlich, dass der Verkäufer den Namen und die Anschrift des Käufers verarbeitet, um seiner Verpflichtung auf Übergabe und Übereignung der Kaufsache aus dem Kaufvertrag nachkommen zu können.

Gem. Art. 5 Abs. 1 lit. b) VO (EU) 2018/1725 bzw. Art. 6 Abs. 1 lit. c) DS-GVO ist eine Verarbeitung auch dann rechtmäßig, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, welcher der Verantwortliche unterliegt. In Betracht kommen hier bspw. die Verarbeitung von personenbezogenen Daten mit dem Zweck, Geldwäsche oder Terrorismusfinanzierung zu verhindern. Unter diesen Erlaubnistatbestand fällt bspw. auch die Übertragung von personenbezogenen Daten an die EZB, damit sie ihrer Funktion als Bankenaufsicht nachkommen kann.

Für die Rechtfertigung der Verarbeitung der Daten bei der EZB kommt ferner Art. 5 Abs. 1 lit. a) VO (EU) 2018/1725 in Betracht, wonach eine Verarbeitung auch dann rechtmäßig ist, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in der Ausübung öffentlicher Gewalt erfolgt, die dem Organ oder der Einrichtung der Union übertragen wurde. Unter diesen Erlaubnistatbestand fallen bspw. Verarbeitungen, die erforderlich sind, damit die EZB ihrer Bankenaufsichtsfunktion nachgehen kann.

b) Offline-Modell

Bei einer Umsetzung des Offline-Modells, bei der personenbezogene Daten verarbeitet werden (siehe IV. 2. a)), kämen als Erlaubnistatbestände Art. 5 Abs. 1 lit. c) VO (EU) 2018/1725 bzw. Art. 6 Abs. 1 lit. b) DS-GVO in Betracht. Die Frage ist, ob die Verarbeitungsvorgänge im Rahmen einer Offline-Umsetzung für die Erfüllung des Vertrags zwischen dem Nutzer und der EZB bzw. den Intermediären erforderlich sind. Da eine Offline-Umsetzung auch ohne die Verarbeitung von personenbezogenen Daten der Transaktionssender und -empfänger umsetzbar wäre, ist die Verarbeitung der personenbezogenen Daten bei Offline-Bezahlungsvorgängen nicht zwingend erforderlich für die Erfüllung des Vertrags.

Als weitere Erlaubnistatbestände kämen Art. 5 Abs. 1 lit. b) VO (EU) 2018/1725 bzw. Art. 6 Abs. 1 lit. c) DS-GVO in Betracht, wenn die Verarbeitungsvorgänge bspw. der Verhinderung von Geldwäsche oder der Finanzierung von Terrorismus dienen.

c) Direktes Modell

Verarbeitet die EZB als Verantwortliche die Daten der Endkunden, findet auf diese Datenverarbeitungsvorgänge nicht die DS-GVO Anwendung, sondern die VO (EU) 2018/1725. Als Erlaubnistatbestand kommt dabei Art. 5 Abs. 1 lit. c) VO (EU) 2018/1725 in Betracht, da die EZB beim Eröffnen des Online-Kontos bzw. -Accounts mit dem Endkunden einen Vertrag über gewisse Leistungen als Zahlungsdienstleister schließt und die Erhebung und Verarbeitung der

personenbezogenen Daten der Endkunden im Rahmen der Verwaltung der Kundendaten und der Durchführung der Transaktionen von digitalen Euro erforderlich für die Erfüllung dieses Vertrags ist. Als weiterer Erlaubnistatbestand kommt aber auch erneut Art. 5 Abs. 1 lit. b) VO (EU) 2018/1725 in Betracht.

d) Intermediär-Modell

Verarbeiten die Intermediäre als Verantwortliche die Daten der Endkunden, findet auf diese Datenverarbeitungsvorgänge die DS-GVO Anwendung. Als Erlaubnistatbestand für die Verarbeitungsvorgänge bei den Intermediären kommt Art. 6 Abs. 1 lit. b) DS-GVO in Betracht, da die Intermediäre beim Eröffnen des Online-Kontos bzw. -Accounts mit dem Endkunden einen Vertrag über gewisse Leistungen als Zahlungsdienstleister schließen und die Erhebung und Verarbeitung der personenbezogenen Daten der Endkunden im Rahmen der Verwaltung der Nutzerdaten und der Durchführung der Transfers von digitalen Euro erforderlich für die Erfüllung dieses Vertrags ist. Des Weiteren kommt wiederum Art. 6 Abs. 1 lit. c) DS-GVO in Betracht.

Die Verarbeitungsvorgänge der EZB könnten dagegen nach Art. 5 Abs. 1 lit. a) VO (EU) 2018/1725 gerechtfertigt sein, um ihrer Aufgabe bei der Bankenaufsicht nachkommen zu können.

e) Endkunden-Modell

Als Erlaubnistatbestand kommt hier Art. 5 Abs. 1 lit. c) VO (EU) 2018/1725 in Betracht, da die EZB beim Eröffnen des Online-Kontos bzw. -Accounts im Rahmen der zentralen Blockchain mit dem Endkunden einen Vertrag über gewisse Leistungen als Zahlungsdienstleister schließt und die Erhebung und Verarbeitung der personenbezogenen Daten der Endkunden im Rahmen der Verwaltung der Kundendaten und der Durchführung der Transfers von digitalen Euro erforderlich für die Erfüllung dieses Vertrags ist, auch wenn die Transaktionen direkt zwischen den Endkunden durchgeführt und validiert werden. Als weiterer Erlaubnistatbestand kommt auch Art. 5 Abs. 1 lit. b) VO (EU) 2018/1725 in Betracht.

f) Hybrid-Modell

Als Erlaubnistatbestand kommt hier Art. 5 Abs. 1 lit. c) VO (EU) 2018/1725 in Betracht, da auch hier die Verarbeitung der Daten sowohl für das Management der Endkunden-Daten als auch für die Durchführung der Transfers von digitalen Euro zur Erfüllung des Zahlungsdienstleistungsvertrag erforderlich ist. Ebenfalls könnte eine Verarbeitung nach Art. 5 Abs. 1 lit. b) VO (EU) 2018/1725 gerechtfertigt sein.

V. Fazit

Einer Einführung des digitalen Euro stehen – im Gegensatz zu bspw. einer Währung auf Basis einer dezentralen Blockchain wie Bitcoin oder Ethereum[41] – keine datenschutzrechtlichen Bedenken entgegen. Bei der entsprechenden technischen Umsetzung der Offline-Variante ist sogar eine anonyme Bezahlweise denkbar.

Bei den Online-Umsetzungsmodellen kommen als Erlaubnistatbestand Art. 5 Abs. 1 lit. c) VO (EU) 2018/1725 bzw. Art. 6 Abs. 1 lit. b) DS-GVO in Betracht, da die Endkunden vor Nutzung des digitalen Euro entweder einen Vertrag mit der EZB oder mit einem der Intermediäre abschließen müssen und diese die jeweiligen Verarbeitungsvorgänge zur Erfüllung ihrer Pflichten aus den Verträgen mit den Endkunden vornehmen müssen. Daneben kommen auch noch Art. 5 Abs. 1 lit. b) VO (EU) 2018/1725 bzw. Art. 6 Abs. 1 lit. c) DS-GVO in Betracht für Datenverarbeitungsvorgänge, die bspw. der Verhinderung von Geldwäsche und Finanzierung von Terrorismus dienen.

Abschließend sei noch erwähnt, dass die EZB bzw. die Intermediäre trotz Einschlägigkeit eines datenschutzrechtlichen Erlaubnistatbestandes in der Lage sind, ein genaues Profil über die erfolgten Transaktionen eines jeden Endkunden zu erstellen. Dabei müssen sie die in Art. 4 VO (EU) 2018/1725 bzw. Art. 5 DS-GVO enthaltenen datenschutzrechtlichen Grundsätze – wie bspw. Zweckbindung und Datenminimierung – beachten.

[41] Siehe für Details: *Schmid*, in: Maume/Maute (Hrsg.), Rechtshandbuch Kryptowerte, 2020, § 16 Rn. 1 ff., 44 ff, 103.