

Informationen über die DekaBank Deutsche Girozentrale und ihre Kryptowerte-Dienstleistungen ("Kundeninformation für Kryptowerte")



Fassung September 2026

Gemäß der Vorgaben aus Art. 75 Abs. 3, 66 Abs. 3, 72 Abs. 2 der Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (kurz: MiCAR) erteilt die DekaBank hiermit folgende Informationen im Zusammenhang mit der Erbringung von Kryptowerte-Dienstleistungen:

A. Informationen zur Verwahrstrategie und zu den Sicherheitssystemen

Die DekaBank bietet Kunden eine sichere und verlässliche Lösung zur Verwahrung von Kryptowerten an. Dabei steht die Einhaltung hoher Sicherheitsstandards und gesetzlicher Vorgaben, insbesondere der europäischen MiCAR-Verordnung im Mittelpunkt.

1. Unternehmensprofil und Geschäftstätigkeit

Als zentraler Finanzdienstleister der Sparkassen-Finanzgruppe baut die DekaBank ihr digitales Angebot gezielt aus und integriert die Verwahrung von Kryptowerten als festen Bestandteil ihrer Digitalisierungsstrategie.

Die DekaBank übernimmt für ihre Kunden die Verwahrung und Verwaltung von zugelassenen Kryptowerten. Dabei verwahrt die Bank auch die zugehörigen privaten kryptographischen Schlüssel, die für den Zugriff und die Übertragung dieser Werte notwendig sind. Für die Verwahrung nutzt die DekaBank eigene technische Systeme und wendet hohe Sicherheitsstandards an. Bei der von der DekaBank bereitgestellten Sammelverwahrung werden die Kryptowerte mehrerer Kunden gemeinsam in einer sogenannten Omnibus Wallet verwahrt.

Neben der Verwahrung bietet die DekaBank ihren Kunden auch die Möglichkeit, Transaktionen mit Kryptowerten durchzuführen, sowohl innerhalb der Bank als auch zu externen Wallets. Dabei bleibt der direkte Zugriff auf die Blockchain der DekaBank vorbehalten, was zusätzliche Sicherheit bietet. Kunden geben ihre Transaktionsaufträge über die Kundenportale, d.h. Deka Easy Access („DEA“) für institutionelle Kunden und die App Sparkasse („S-App“) für nicht-institutionelle Kunden ein. Die DekaBank übernimmt daraufhin die technische Umsetzung der Transaktion. Nach dem Kauf eines Kryptowerts durch den Kunden werden die Kryptowerte zunächst auf eine speziell erzeugte Proxy Wallet übertragen. Nach erfolgreicher Prüfung erfolgt die Umbuchung in die zentrale Verwahrung der DekaBank. Die Möglichkeit zur Einlieferung von extern erworbenen Kryptowerten in die Verwahrung der DekaBank steht ausschließlich institutionellen Kunden zur Verfügung. Zum Schutz der Kunden gelten bei Auslieferungen an externe Wallets hohe Sicherheitsstandards. In diesem Fall werden Transaktionen erst freigegeben, nachdem die Identität des Kunden sowie die Zieladresse eindeutig festgestellt wurde und von dem empfangenden Anbieter von Kryptowerte-Dienstleistungen wurde.

2. Governance und interne Zuständigkeit

Die DekaBank hat klare Zuständigkeiten, Zugriffsrechte und Kontrollprozesse für die Kryptoverwahrung definiert. Dazu zählen ein internes Kontrollsystem mit Mehr-Augen-Prinzip, rollenbasierte Workflows und automatisierte Abläufe zur

Absicherung des Geschäftsbetriebs. Es bestehen organisatorische Maßnahmen zur Risikovermeidung, etwa durch technische und manuelle Kontrollen, die Einhaltung regulatorischer Vorgaben (z. B. Geldwäscheprävention) sowie regelmäßige Bewertungen der zu berücksichtigenden Risiken. Die DekaBank stellt durch eine sorgfältige Prüfung, Auswahl und laufende Überwachung sicher, dass Drittanbieter über robuste Sicherheits- und Kontrollsysteme verfügen. Zudem werden im Rahmen eines umfassenden Vertragsmanagements (z.B. durch das zentrale Auslagerungsmanagement) klare Anforderungen an Sicherheitsstandards und Berichtspflichten in den Verträgen mit Drittanbietern festgelegt. Alle Mitarbeitenden in den relevanten Organisationseinheiten sind zu den regulatorischen, technischen und prozessbezogenen Anforderungen geschult und verfügen über die erforderlichen Qualifikationen.

3. Kundenzugang und Kommunikationswege mit dem Kunden

Die DekaBank stellt ihre Kryptoverwahrung ausschließlich Kunden in Deutschland zur Verfügung. Interessierte Kunden können sich über die Website oder über die jeweiligen Kundenportale (DEA, S-App) über die Kryptoverwahrung informieren. Für die Inanspruchnahme der Kryptoverwahrdienstleistung wird ein umfassendes Kundenonboarding durchgeführt, das vertragliche und organisatorische Schritte umfasst. Das Onboarding beinhaltet zudem die Einhaltung der gesetzlichen Kundensorgfaltspflichten sowie die technische Einrichtung von Kryptokonten und Benutzerzugängen sowie den Abschluss eines entsprechenden Vertrags zur Erbringung der Kryptoverwahrdienstleistung in Form der Sonderbedingungen für Kryptowerte.

Die Haftungsanforderungen nach Art. 75 Abs. 8 MiCAR sind in diesen Sonderbedingungen umgesetzt. Danach haftet die DekaBank für den Verlust von Kryptowerten, sofern dieser auf ihr zurechenbare Vorfälle zurückzuführen ist.

Eine Haftung besteht hingegen nicht für Ereignisse außerhalb des Einflussbereichs der DekaBank. Hierzu zählen insbesondere Fälle höherer Gewalt sowie sogenannte Blockchainereignisse, also technische oder systemische Störungen der Distributed-Ledger-Technologie, auf die die DekaBank keinen Einfluss hat.

Die DekaBank legt großen Wert auf eine transparente und vertrauensvolle Zusammenarbeit mit ihren Kunden. Dazu gehört, dass alle Schritte klar kommuniziert und nachvollziehbar sind. Die dem Kunden für die Kommunikation mit der DekaBank zur Verfügung stehenden Kommunikationskanäle sollen eine kontinuierliche, sichere und dokumentierte Kundeninteraktion ermöglichen. Das Kundenportal (DEA bzw. die S-App) fungiert als zentrale Plattform für die Kommunikation und Interaktion mit dem Kunden. Über das Portal kann der Kunde der DekaBank Weisungen erteilen, Nachrichten senden und empfangen, Dokumente einsehen und wichtige Informationen zu seinen Konten und Transaktionen abrufen.

Informationen über die DekaBank Deutsche Girozentrale und ihre Kryptowerte-Dienstleistungen ("Kundeninformation für Kryptowerte")



Fassung September 2026

4. Sicherheitsmechanismen der Kryptoverwahrung und Verwaltung

Die DekaBank setzt auf ein mehrstufiges Sicherheitskonzept, um ihre Dienstleistungen im Bereich der Kryptoverwahrung technisch, organisatorisch und prozessual abzusichern. Ziel ist es, verwahrte Kryptowerte vor Verlust, Missbrauch und unbefugtem Zugriff zu schützen.

Für die Verwahrung der Kryptowerte nutzt die DekaBank Multi-Signature-Wallets, die für Transaktionen mehrere Signaturen erfordern. Zusätzlich kommen physische Sicherheitsgeräte sowie zertifizierte Hardware Security Module (HSM) zum Einsatz, um die Private Keys sicher zu verwahren. Zur zusätzlichen Absicherung verwendet die DekaBank Proxy-Wallets, die für jede eingehende Transaktion individuell und einmalig erstellt werden. Erst nach eingehender Prüfung über die Zuordnung und die Konformität der Kryptowerte erfolgt die Übertragung in die zentrale Omnibus-Wallet, in denen die Vermögenswerte verschiedener Kunden gemeinsam verwahrt, aber systemseitig den jeweiligen Kunden eindeutig zugeordnet werden. Jede Blockchain erhält eine eigene Omnibus-Wallet für die Sammelverwahrung, wobei die interne Zuordnung in den Systemen der DekaBank erfolgt. Durch die über die Bestandsführungssysteme der DekaBank erfolgende individuelle Zuordnung der Kryptowerte an den jeweiligen Kunden sind die Kryptowerte der Kunden kraft Gesetzes nach Maßgabe der Vorschriften des Gesetzes zur Aufsicht über Märkte für Kryptowerte (nachfolgend „**KMAG**“) vor der Insolvenz der DekaBank zu Gunsten des Kunden geschützt. Die Kryptowerte der Kunden werden strikt getrennt von den Eigenbeständen der DekaBank verwahrt. Die DekaBank tritt ausschließlich als Verwahrstelle auf, ohne Zugriff oder Anspruch auf Kryptowerte des Kunden.

Für den Fall technischer Störungen oder unerwarteter Zwischenfälle hat die DekaBank umfassende Notfall- und Wiederherstellungspläne etabliert. Alle damit einhergehenden Maßnahmen werden regelmäßig auf Aktualität und Geeignetheit geprüft und bei Bedarf angepasst. Darüber hinaus hat die DekaBank Aufzeichnungs- und Archivierungsvorgehen implementiert, die ebenfalls die Wiederherstellung der Daten sichern. Um die Einhaltung aller Sicherheitsmaßnahmen sicherzustellen, führt die DekaBank regelmäßige Risikoanalysen durch und überwacht sämtliche Prozesse. Technisch ist die Infrastruktur durch moderne Schutzmaßnahmen, wie Firewalls, Verschlüsselung und Zugriffskontrollen geschützt. Transaktionen unterliegen einem mehrstufigen Freigabeprozess, wobei bei höheren Beträgen oder unbekannten Empfängern zusätzliche Kontrollstufen (z.B. Sechsen-Prinzip) angewendet werden.

Die DekaBank informiert ihre Kunden bereits vor Vertragschluss sowie fortlaufend während der Geschäftsbeziehung über alle relevanten Aspekte der Kryptoverwahrung. Über das Kundenportal erhalten Kunden Einsicht in ihre aktuellen Kryptobestände und Transaktionen. Ergänzend dazu wird mindestens vierteljährlich und auf Anfrage ein Bericht über die vom Kunden verwahrten Kryptopositionen und -transfers bereitgestellt. Auf Anfrage erhalten Kunden Zugang zu allen kundenbezogenen Informationen und Daten, die im

Zusammenhang mit der Kryptoverwahrung aufgezeichnet werden.

Kunden können jederzeit die Rückgabe von verwahrten Kryptowerten verlangen. Die Rückgabe erfolgt im Rahmen einer Auslieferung der Kryptowerte. Eine Rückgabe von privaten kryptografischen Schlüssel, die zur Sicherung der Kryptowerte genutzt werden, ist aufgrund der gewählten Omnibus-Verwahrung ausgeschlossen.

Bei einer Auslieferung transferiert die DekaBank die Kryptowerte auf Weisung des Kunden (i) sofern es sich bei dem Empfänger um einen Kunden der DekaBank handelt, für den die DekaBank Kryptowerte verwahrt, auf das Kryptokonto des Empfängers bei der DekaBank bzw. (ii) an die Wallet des entsprechenden Kryptowerte-Dienstleisters des Empfängers.

Für ausgehende Transfers von Kryptowerten an externe Wallets gelten strenge Anforderungen. Der die Auslieferung anweisende Kunde muss gegenüber der DekaBank seine Identität verifizieren und die Ziel-Wallet-Adresse bestätigen, um sicherzustellen, dass die Transaktion rechtmäßig und sicher durchgeführt werden kann. Die Auslieferung erfolgt ausschließlich an Wallets, die von zugelassenen Kryptowerte-Dienstleistern verwaltet werden.

5. Hinweis auf Rechtskonformität und Aktualisierungen

Die DekaBank stellt sicher, dass ihre Dienstleistungen im Bereich der Kryptoverwahrung jederzeit den geltenden gesetzlichen Vorgaben entsprechen. Dafür werden interne Prozesse regelmäßig überprüft und bei Bedarf angepasst. Mithilfe moderner Compliance-Systeme gewährleistet die DekaBank die Einhaltung gesetzlicher Vorgaben und arbeitet dabei eng und transparent mit den zuständigen Aufsichtsbehörden zusammen. Die Strategie zur Kryptoverwahrung wird mindestens einmal pro Jahr aktualisiert oder kurzfristig angepasst, sobald sich (rechtliche) Rahmenbedingungen wesentlich ändern.

B. Risikohinweise

Die Investition in Kryptowerte ist mit erheblichen Risiken verbunden, die teilweise außerhalb der Kontrolle der DekaBank liegen. Investitionen in Kryptowerte sind hochriskant und können zum vollständigen Verlust des eingesetzten Kapitals führen. Kryptowerte unterliegen keiner Einlagensicherung und keinem gesetzlichen Anlegerentschädigungssystem. Die nachfolgenden Risikohinweise dienen dem Zweck, Kunden auf die wesentlichen Risiken im Zusammenhang mit der Verwahrung, dem Handel und Transaktionen mit Kryptowerten und kryptografischen Instrumenten hinzuweisen. Diese Auflistung ist nicht abschließend und deckt nicht alle möglichen Risiken ab, die sich durch technologische, regulatorische oder marktwirtschaftliche Veränderungen ergeben können. Kunden wird daher empfohlen, sich eingehend über potenzielle Risiken zu informieren und, falls erforderlich, unabhängigen steuerlichen, rechtlichen und finanziellen Rat einzuholen.

Informationen über die DekaBank Deutsche Girozentrale und ihre Kryptowerte-Dienstleistungen ("Kundeninformation für Kryptowerte")



Fassung September 2026

Blockchain-Technologie

Die Blockchain-Technologie stellt eine noch relativ junge und daher nur begrenzt erprobte technologische Innovation dar. Kryptowerte wie Bitcoin basieren auf dieser Technologie. Es besteht das Risiko, dass die Blockchain-Technologie durch technische Probleme oder äußere Einflüsse in ihrer Funktionsfähigkeit beeinträchtigt wird. Darüber hinaus könnten Fortschritte in der Kryptographie oder technologische Entwicklungen, wie beispielsweise die Einführung von Quantencomputern, die Sicherheit und Integrität von Kryptowerten gefährden. Ein weiteres Risiko besteht darin, dass die zugrunde liegende Software Schwächen oder Fehler aufweist, die im schlimmsten Fall zu einem vollständigen Verlust des Kryptowerts führen können.

Akzeptanzrisiko

Kryptowerte sind keine gesetzlich anerkannten Zahlungsmittel, und es gibt keine Verpflichtung für Anbieter von Waren und Dienstleistungen oder andere Marktteilnehmer, diese als Zahlungsmittel zu akzeptieren. Die Nutzung von Kryptowerten hängt daher maßgeblich von der Akzeptanz innerhalb der Gesellschaft und der Wirtschaft ab. Sollte die Akzeptanz von Kryptowerten zukünftig abnehmen, könnte dies zu einem erheblichen Wertverlust bis hin zum Totalverlust führen.

Wertrisiko

Im Gegensatz zu physischen Vermögenswerten wie Edelmetallen besitzen Kryptowerte keinen intrinsischen oder materiellen Wert. Ihr Marktwert wird ausschließlich durch das Verhältnis von Angebot und Nachfrage bestimmt. Ein plötzlicher oder anhaltender Rückgang der Nachfrage kann zu einem drastischen Wertverlust führen, der nicht durch einen inneren Wert begrenzt wird. Dies birgt das Risiko erheblicher Verluste bis hin zum Totalverlust.

Aufgaberisiko

Die Funktionsfähigkeit der Distributed-Ledger-Technologie, auf der viele Kryptowerte basieren, hängt bei Kryptowährungen wie Bitcoin (BTC), Bitcoin Cash (BCH), Litecoin (LTC) und Dogecoin (DOGE) stark von der Aktivität der sogenannten Miner ab. Diese Miner stellen ihre Rechenleistung für die Erstellung neuer Blöcke zur Verfügung. Sollten Miner ihre Tätigkeit einstellen – sei es aufgrund mangelnder Rentabilität, fehlender Finanzierung oder geringem Interesse – könnte dies die Funktionsfähigkeit der Technologie erheblich beeinträchtigen.

Bei Kryptowerten wie Ether (ETH), Solana (SOL), Cardano (ADA), Algorand (ALGO) oder Polygon (POL) besteht zusätzlich das Risiko, dass eine Konzentration von Eigentümern, die einen großen Teil des Netzwerks kontrollieren (z. B. 50 % des gestakten Wertes), die Netzwerksicherheit gefährdet. Ein solcher Angriff kann die Validierung von Transaktionen verhindern und die Funktionsfähigkeit des Netzwerks beeinträchtigen.

Ausführungsrisiko

Aufträge können aufgrund von Marktbedingungen oder technischen Störungen nicht oder verzögert ausgeführt werden. Zudem können Aufträge aufgrund von Störungen in der Plattformverfügbarkeit nicht oder verzögert ausgeführt werden.

Risiko der Unumkehrbarkeit von Kryptoauszahlungen

Transaktionen auf der Blockchain sind grundsätzlich unumkehrbar. Teilnehmer, die Kryptowerte auf eine Blockchain-Adresse auszahlen lassen möchten, müssen sicherstellen, dass die eingegebene Adresse korrekt ist. Fehler bei der Eingabe können dazu führen, dass die Kryptowerte unwiederbringlich verloren gehen. Ebenso besteht bei Einzahlungen das Risiko, dass eine falsche Wallet-Adresse verwendet wird, was ebenfalls zu einem Verlust führen kann. Teilnehmer sollten daher mit äußerster Sorgfalt vorgehen, um solche Fehler zu vermeiden.

Kryptoverwahrerrisiko

Im Falle einer Insolvenz des Verwahrers besteht das Risiko, dass Kryptowerte nicht oder nicht vollständig zurückgeführt werden können.

Regulatorische Risiken

Die rechtlichen Rahmenbedingungen für Kryptowerte und die zugrunde liegende Distributed-Ledger-Technologie können sich ändern. Neue gesetzliche Regelungen oder Änderungen bestehender Vorschriften können die Nutzung und den Wert von Kryptowerten negativ beeinflussen. Beispielsweise könnten strengere Vorschriften zur Verwahrung oder Nutzung von Kryptowerten dazu führen, dass technische Betreiber ihre Aktivitäten einstellen oder die Akzeptanz von Kryptowerten sinkt. Solche regulatorischen Änderungen können zu einem Wertverlust bis hin zum Totalverlust führen.

Steuerliche Risiken

Gewinne aus dem Handel mit Kryptowerten können steuerpflichtig sein. Änderungen in der steuerlichen Behandlung oder eine strengere Auslegung durch in- oder ausländische Finanzbehörden können die Steuerbelastung erhöhen und die Nettorendite verringern. Teilnehmer sollten sich über die steuerlichen Auswirkungen ihrer Investitionen im Klaren sein und gegebenenfalls steuerlichen Rat einholen.

Cybersicherheitsrisiko

Trotz der Anwendung hoher Sicherheitsstandards besteht das Risiko, dass Kryptowerte durch Cyberangriffe oder physische Angriffe verloren gehen. Sicherheitsmaßnahmen können keine vollständige Sicherheit garantieren. Ein erfolgreicher Angriff auf die IT-Infrastruktur könnte zu einem Verlust der verwahrten Kryptowerte führen, der bis hin zum Totalverlust reichen kann.

Informationen über die DekaBank Deutsche Girozentrale und ihre Kryptowerte-Dienstleistungen ("Kundeninformation für Kryptowerte")



Fassung September 2026

Manipulationsrisiko

Die Sicherheit der Distributed-Ledger-Technologie basiert auf kryptographischen Verfahren, die Manipulationen verhindern sollen. Sollten diese Verfahren oder deren Implementierungen Schwächen aufweisen, könnten Cyberangriffe oder andere Manipulationen die Funktionsfähigkeit der Technologie beeinträchtigen. Dies könnte zu einem Verlust von Kryptowerten führen, der bis hin zum Totalverlust reichen kann.

Risiko eines Mehrheitsangriffs

Bei Kryptowerten, die auf Proof-of-Work-Netzwerken basieren, besteht das Risiko eines sogenannten 51%-Angriffs. Dabei könnten Miner, die mehr als die Hälfte der Rechenleistung kontrollieren, das Netzwerk manipulieren, Transaktionen blockieren oder doppelte Ausgaben („Double Spending“) durchführen. Ein solcher Angriff könnte die Integrität des Netzwerks gefährden und zu einem Wertverlust führen. Ähnliche Risiken bestehen bei Proof-of-Stake-Netzwerken, wenn eine kleine Anzahl von Eigentümern einen Großteil des Netzwerks kontrolliert.

Transferkostenrisiko

Der Transfer von Kryptowerten zwischen Blockchain-Adressen ist mit Gebühren verbunden. Steigende Transferkosten können die Nutzung von Kryptowerten als Zahlungsmittel unattraktiver machen und somit deren Marktwert negativ beeinflussen.

Risiko einer missbräuchlichen Nutzung von Zugangsdaten

Teilnehmer, die ihre Zugangsdaten (z. B. E-Mail-Adresse, Passwort und PushTAN) nicht ausreichend schützen, laufen Gefahr, dass Dritte unbefugt auf ihre Konten zugreifen. Ein solcher Missbrauch könnte zu unautorisierten Transaktionen und erheblichen Verlusten führen. Teilnehmer sollten daher ihre Zugangsdaten und Geräte sorgfältig sichern.

Risiko einer Kreditfinanzierung

Die Finanzierung des Kaufs von Kryptowerten durch Kredite erhöht das Verlustrisiko erheblich. Neben möglichen Verlusten aus der Wertentwicklung müssen auch die Kreditkosten, insbesondere Zinsen, getragen werden. Sollte der Marktpreis der Kryptowerte sinken, könnten Teilnehmer nicht nur Verluste hinnehmen, sondern auch Schwierigkeiten haben, den Kredit zurückzuzahlen.

Höhere Risiken bei taggleichen Geschäften (Daytrading)

Das sogenannte Daytrading, bei dem Kryptowerte innerhalb eines Tages mehrfach gekauft und verkauft werden, birgt erhöhte Risiken. Die hohe Handelsfrequenz kann zu Verlusten führen, insbesondere bei unerwarteten Marktbewegungen oder unzureichender Marktkenntnis.

Risiko unvollständiger Informationen

Entscheidungen über den Kauf oder Verkauf von Kryptowerten sollten auf einer fundierten Informationsbasis getroffen werden. Teilnehmer, die auf unzureichende oder unvollständige Informationen zurückgreifen, laufen Gefahr, Fehlentscheidungen zu treffen, die zu Verlusten oder entgangenen Gewinnen führen können. Es wird empfohlen, zusätzliche Informationsquellen zu nutzen und gegebenenfalls Expertenrat einzuholen.

Hinweis: Diese Risikoinformationen sind nicht abschließend. Teilnehmer sollten sich umfassend informieren und bei Bedarf professionelle Beratung in Anspruch nehmen, um fundierte Entscheidungen zu treffen.

C. Darstellung möglicher Interessenkonflikte

Zweck, Anwendungsbereich und regulatorischer Rahmen

Mit dieser Offenlegung über Interessenkonflikte in Bezug auf ihre Kryptowerte-Dienstleistungen („**Offenlegung**“) beschreibt die DekaBank diejenigen Vorkehrungen, die sie getroffen hat, damit sich mögliche Interessenkonflikte zwischen der DekaBank, ihrer Geschäftsleitung, ihren Beschäftigten oder anderen Personen, die mit der DekaBank direkt oder indirekt durch Kontrolle verbunden sind, und Kunden oder zwischen den Kunden untereinander nicht auf die Kundeninteressen auswirken. Die DekaBank setzt damit die Anforderungen der Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCAR), insbesondere Art. 72, Art. 75 und Art. 78 MiCAR, sowie die Delegierte Verordnung (EU) 2025/1142 (die „**Delegierte Verordnung**“) um.

Damit sich mögliche Interessenkonflikte zwischen der DekaBank, ihrer Geschäftsleitung, den Beschäftigten oder anderen Personen, die mit ihr direkt oder indirekt durch Kontrolle verbunden sind, und dem Kunden oder zwischen den Kunden untereinander nicht auf die Kundeninteressen, einschließlich ihrer Nachhaltigkeitspräferenzen, auswirken, sind in den nachfolgenden Abschnitten die Dienstleistungen, Tätigkeiten oder Umstände aufgeführt, die zu Interessenkonflikten führen können sowie die Risiken im Zusammenhang mit den Interessenkonflikten und ergriffenen Vorkehrungen und Maßnahmen zur Begrenzung der festgestellten Interessenkonflikte dargestellt.

Art und die Quellen von Interessenkonflikten

In der DekaBank können Interessenkonflikte zwischen den Kunden und der DekaBank, Beschäftigten der DekaBank oder sonstigen mit diesen verbundenen Personen, bei folgenden Kryptowerte-Dienstleistungen auftreten:

- Ausführung von Aufträgen über Kryptowerte für Kunden,
- Tausch von Kryptowerten gegen einen Geldbetrag oder andere Kryptowerte,

Informationen über die DekaBank Deutsche Girozentrale und ihre Kryptowerte-Dienstleistungen ("Kundeninformation für Kryptowerte")



Fassung September 2026

- Erbringung von Transferdienstleistungen für Kryptowerte für Kunden und
- Verwahrung und Verwaltung von Kryptowerten für andere und damit verbundene Dienstleistungen.

„**Kryptowert**“ im Sinne dieser Offenlegung ist eine digitale Darstellung eines Werts oder eines Rechts, der bzw. das unter Verwendung der Distributed-Ledger-Technologie oder eine ähnlichen Technologie elektronisch übertragen und gespeichert werden kann. Unter den Begriff Kryptowerte werden gefasst Vermögenswertreferenzierter Token Art. 3 Abs. 1 Nr. 6 MiCAR (Asset-Referenced Tokens oder ART), E-Geld-Token Art. 3 Abs. 1 Nr. 7 MiCAR (E-Money Tokens oder EMT), und sonstige Token (z.B. Bitcoin, Ethereum) einschließlich Utility-Token Art. 3 Abs. 1 Nr. 9 MiCAR (z. B. Token, die Zugang zu einem spezifischen Produkt oder einer Dienstleistung gewähren).

„**Verbundene Personen**“ im Sinne dieser Offenlegung sind Anteilseigner oder Gesellschafter der DekaBank; Personen, die durch Kontrolle direkt oder indirekt mit der DekaBank oder ihren Anteilseignern oder Gesellschaftern verbunden sind; Mitglieder der Führungsgremien sowie Beschäftigte der DekaBank (Art. 1 Nr. 1 Delegierte Verordnung in Verbindung mit Art. 72 Abs. 1 Buchstabe a Ziffer i bis iv MiCAR).

Seitens der DekaBank kann es zu Interessenkonflikten kommen, wenn eine verbundene Person

- ein wirtschaftliches Interesse an einer Person, Einrichtung oder Organisation hat, deren Interessen mit denen des Anbieters von Kryptowerte-Dienstleistungen kollidieren,
- eine aktuelle Beziehung (persönlicher, beruflicher oder politischer Art) zu einer Person, Einrichtung oder Organisation hat, deren Interessen mit denen des Anbieters von Kryptowerte-Dienstleistungen kollidieren, oder innerhalb der letzten drei Jahre ab dem Zeitpunkt der Beurteilung eine derartige Beziehung hatte oder
- Aufgaben oder Tätigkeiten ausführt oder mit Zuständigkeiten betraut ist, die mit denen des Anbieters von Kryptowerte-Dienstleistungen kollidieren, oder einer Person mit Funktionen oder Aufgaben unterstellt ist, die mit denen des Anbieters von Kryptowerte-Dienstleistungen kollidieren.

Ferner kann es zu Interessenkonflikten kommen, wenn die DekaBank oder eine verbundene Person

- mit den jeweiligen an der Ausführung von Kryptoaufträgen beteiligten Marktteilnehmern, insbesondere den Handelsplätzen oder sonstigen Dienstleistern im Zusammenhang mit Kryptowerten Kooperationen eingegangen ist, Auslagerungsverträge abgeschlossen hat, oder Lizenzrechte für geistiges Eigentum vergeben oder erworben hat,
- für die Ausführung von Kryptoaufträgen nur einen Ausführungsplatz anbietet oder
- die Kryptowerte-Dienstleistung, die die Bank als Kommissionärin ausführt, d.h. der Erwerb oder die Veräußerung der Kryptowerte, auch außerhalb einer Handelsplattform im eigenen Namen für Rechnung des Kunden erbringt.

Es können Interessenkonflikte auch dadurch auftreten, dass

- der DekaBank oder verbundenen Personen Informationen vorliegen, die zum Zeitpunkt eines Kundengeschäfts noch nicht öffentlich bekannt sind,
- die DekaBank oder eine verbundene Person Finanzinstrumente eines in die Kryptowerte-Dienstleistung der Bank eingebundenen Kryptowerte-Dienstleisters gezeichnet oder Darlehen an diesen ausgereicht hat,
- Mitarbeiter der DekaBank eine erfolgsbezogene Vergütung erhalten,
- die DekaBank oder eine verbundene Person aus politischen, persönlichen oder ökonomischen Gründen ein Interesse an einem bestimmten Ausgang einer Transaktion bzw. der Erbringung der Kryptowerte-Dienstleistung haben, verbundene Personen oder andere Personen auf Rechnung der verbundenen Personen Persönliche Transaktionen durchführen, z. B. weil Anreize zur Bevorzugung eines bestimmten Kryptowertes bei Analyse, Auftragsannahme oder Auftragsausführung vorliegen oder Grundsätze oder Ziele, die den Umsatz, das Volumen oder den Ertrag der Geschäfte unmittelbar oder mittelbar betreffen aufgestellt werden.

Risiken im Falle von Interessenkonflikten

Die Realisierung eines oder mehrerer der vorstehend genannten Interessenkonflikte, die nicht wie nachstehend beschrieben durch geeignete Maßnahmen der DekaBank verhindert oder gehandhabt werden können, könnte dazu führen, dass die von der DekaBank erbrachte Kryptowerte-Dienstleistung nicht im besten Interesse des Kunden erbracht werden kann. Ursächlich könnte z.B. sein, dass die DekaBank oder eine verbundene Person

- auf Kosten des Kunden wahrscheinlich einen finanziellen Gewinn erzielt, einen finanziellen Verlust vermeidet oder einen anderen Vorteil erhält,
- ein anderes Interesse am Ergebnis einer für den Kunden erbrachten Krypto-Dienstleistung oder einer im Namen des Kunden getätigten Transaktion hat als der Kunde,
- einen finanziellen oder sonstigen Anreiz hat, die Interessen eines oder mehrerer Kunden über die Interessen eines anderen Kunden zu stellen,
- die gleiche Geschäftstätigkeit ausübt wie der Kunde oder
- aktuell oder künftig von einer nicht mit dem Kunden identischen Person in Verbindung mit einer für den Kunden erbrachte Dienstleistung einen Anreiz in Form von finanziellen oder nichtfinanziellen Vorteilen oder Dienstleistungen erhält.

Strategien und Verfahren zu Interessenkonflikten

Zur weitgehenden Vermeidung dieser Interessenkonflikte ist die DekaBank Teil einer mehrstufigen Organisation mit entsprechender Aufgabenverteilung zwischen Sparkassen, Landesbanken und Dienstleistern.

Informationen über die DekaBank Deutsche Girozentrale und ihre Kryptowerte-Dienstleistungen ("Kundeninformation für Kryptowerte")



Fassung September 2026

Die DekaBank als Kryptowerte-Dienstleister selbst wie auch ihre Mitarbeiter sind entsprechend den gesetzlichen Grundlagen verpflichtet, Kryptowerte-Dienstleistungen ehrlich, redlich und professionell im Interesse der Kunden zu erbringen und Interessenkonflikte, soweit möglich, zu vermeiden.

Die DekaBank stellt durch ihre Strategien und Verfahren sicher, dass die Risiken für eine Verletzung der Interessen der DekaBank oder seiner Kunden abgewendet oder angemessen begrenzt werden kann. Hierfür hat die DekaBank eine Compliance-Organisation mit angemessenen Ressourcen eingerichtet, die für die Umsetzung, Aufrechterhaltung und Überprüfung der Strategien und Verfahren zur Vermeidung von Interessenkonflikten verantwortlich ist. Zudem hat die DekaBank klare organisatorische Verantwortlichkeiten für die Ermittlung, Vermeidung, Regelung und Offenlegung von Interessenkonflikten geschaffen. Die Strategien und Verfahren umfassen insbesondere folgende Maßnahmen:

- Unverzügliche Meldung potentieller oder eingetretener Interessenkonflikte an den benannten internen Meldekanal; zentrale Erfassung und geeignete Eskalationswege.
- Die Einrichtung von Vertraulichkeitsbereichen mit Informationsbarrieren (sogenannten „Chinese Walls“), das heißt virtuelle bzw. tatsächliche Barrieren zur Beschränkung des Informationsflusses.
- Gesonderte interne Kontrolle der relevanten Personen, deren Hauptaufgaben in der Ausübung von Tätigkeiten im Namen von Kunden oder der Erbringung von Kryptowerte-Dienstleistungen für Kunden bestehen, bei denen kollidierende Kunden- oder Institutsinteressen berührt sein können.
- Beseitigung direkter Vergütungsverknüpfungen zwischen Personen oder Organisationseinheiten, wenn nachweisbare Gründe bestehen, dass hierdurch Interessenkonflikte entstehen könnten.
- Sicherstellung, dass verbundene Personen mit externen Geschäftstätigkeiten im Zusammenhang mit der DekaBank keinen unangemessenen Einfluss innerhalb der DekaBank auf diese Tätigkeiten ausüben.
- Prävention bzw. Kontrolle der gleichzeitigen oder unmittelbar nachfolgenden Einbeziehung einer verbundenen Person in verschiedene Kryptowerte-Dienstleistungen oder Tätigkeiten, wenn dies ein ordnungsgemäßes Konfliktmanagement beeinträchtigen könnte.
- Zuweisung kollidierender Tätigkeiten oder Transaktionen an unterschiedliche Personen zur Sicherstellung einer funktionalen Trennung.
- Festlegung der Verantwortung der Mitglieder des Leitungsorgans, andere Mitglieder über einschlägige Angelegenheiten zu informieren und in Fällen tatsächlicher oder möglicher Interessenkonflikte an Beschlussfassungen nicht mitzuwirken.
- Verhinderung, dass Mitglieder des Leitungsorgans Führungspositionen bei konkurrierenden Kryptowerte-Dienstleistern außerhalb derselben Gruppe bekleiden.

- Verhinderung und Kontrolle des Informationsaustauschs zwischen verbundenen Personen in konfliktträchtigen Tätigkeiten, wenn dies die ordnungsgemäße Wahrnehmung ihrer Verantwortlichkeiten gegenüber der DekaBank beeinträchtigen könnte; hierzu zählen Beobachtungs-/Sperrlisten, Insiderlisten und Überwachung der Mitarbeitergeschäfte.
- Alle Mitarbeiter, bei denen im Rahmen ihrer Tätigkeit Interessenkonflikte auftreten können, sind zur Offenlegung aller ihrer Geschäfte in Kryptowerten verpflichtet.
- Einführung und Überwachung von Regelungen über die Annahme von Zuwendungen und sonstigen Vorteilen.
- Schulung der Mitarbeiter.
- Überwachung der Einhaltung der Kundeninteressen bei Ausgestaltung und Umsetzung von Vertriebsvorgaben.
- Berücksichtigung der Kundeninteressen im Rahmen unserer Produktfreigabeverfahren und -überwachung.

Persönliche Transaktionen

Die DekaBank wird unverzüglich über jegliche persönliche Transaktion benachrichtigt, bevor die Entscheidung über die Durchführung der Transaktion getroffen wird.

„**Persönliche Transaktionen**“ im Sinne dieser Offenlegung sind Transaktionen gemäß Artikel 6 Abs. 1 der Delegierten Verordnung, die zu einer Position oder Risikoposition in Bezug auf Kryptowerte führen und von oder im Namen einer verbundenen Person durchgeführt werden.

- Compliance-relevante Mitarbeitende müssen ihre Geschäfte in Kryptowerten und die zur Abwicklung genutzten Wallets gegenüber dem Bereich Compliance offenlegen
- Persönliche Geschäfte unterliegen der Überwachung durch den Bereich Compliance der DekaBank
- Die DekaBank zeichnet alle an die DekaBank gemeldeten oder von der DekaBank identifizierten persönlichen Transaktionen auf, einschließlich aller Genehmigungen und Verbote solcher Geschäfte.

Verantwortung der Geschäftsleitung

Der Vorstand der DekaBank ist für die Festlegung, Annahme und Umsetzung dieser Strategien und Verfahren zu Interessenkonflikten verantwortlich. Der Vorstand bewertet und überprüft regelmäßig deren Wirksamkeit und beseitigt etwaige diesbezügliche Mängel.

Berichterstattung an die Geschäftsleitung

Der Vorstand wird jährlich vom Bereich Compliance über die Umsetzung, die Pflege und Überprüfung dieser Verhaltensregeln sowie die Einhaltung der maßgeblichen Vorschriften und Auffälligkeiten durch Vorlage eines Berichts informiert.

Informationen über die DekaBank Deutsche Girozentrale und ihre Kryptowerte-Dienstleistungen ("Kundeninformation für Kryptowerte")



Fassung September 2026

Umgang mit unvermeidbaren Interessenkonflikten

Sind Interessenkonflikte in Einzelfällen ausnahmsweise nicht durch die obige Aufgabenteilung oder unsere Compliance-Organisation vermeidbar, werden diese den Kunden offengelegt. Auf Wunsch des Kunden wird die DekaBank weitere Einzelheiten zu diesen möglichen Interessenkonflikten zur Verfügung stellen.

Wenn Sie weitergehende Fragen zu unserem Umgang mit Interessenkonflikten im Zusammenhang mit Kryptowerte-Dienstleistungen haben, steht Ihnen unsere Haus gerne unter der E-Mail-Adresse service.krypto@deka.de zur Verfügung.