

Germany

Christian Schmies*

Hengeler Mueller, Frankfurt

christian.schmies@hengeler.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

The legal framework for fintech business in Germany is heavily influenced by European legislation. Depending on the services offered, they may qualify as a regulated activity either under German financial regulatory laws, which often implement European legislation, or may be directly subject to the European crypto markets regulation.

The German Banking Act (*Kreditwesengesetz* – KWG) and the German Investment Institution Act (*Wertpapierinstitutsgesetz* – WpIG) provide for licensing requirements for banking and investment services. The catalogue of regulated activities in some respects goes beyond the underlying European directives. For example, in Germany, any form of lending on a commercial basis, including lending to corporates, is subject to a licensing requirement, as is leasing and factoring business. Payment services are subject to a licensing requirement under the German Payment Services Supervisory Act (*Zahlungsdiensteaufsichtsgesetz* – ZAG) which implements the European Payment Services Directive II; the management of investment funds is regulated under the German Capital Investment Code (*Kapitalanlagegesetzbuch* – KAGB) which implements the European UCITS Directive and the Alternative Investment Fund Managers Directive.

The Regulation (EU) 2023/1114 on Markets in Crypto Assets (MiCAR) provides for licensing requirements for crypto asset services, which are not already regulated by the traditional financial market framework. Thus, MiCAR applies to crypto assets that do not qualify as financial instruments under the Directive 2014/65/EU on markets in financial instruments (MiFID II).

Given the comprehensive and still expanding nature of financial regulation, careful analysis of applicable regulatory regimes is indispensable prior to starting any fintech business in Germany.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

With the implementation of MiCAR into German law, crypto assets (*Kryptowerte*) within the meaning of the KWG and WpIG are now defined in accordance with and primarily regulated pursuant to MiCAR. MiCAR provides for a uniform regulatory regime of operators of crypto asset services, which became subject to a European Union-wide licence and ongoing prudential and good conduct requirements under MiCAR. MiCAR was accompanied by national German legislation in the Act on the Digitalisation of Financial Markets (*Finanzmarktdigitalisierungsgesetz*), which, inter alia, introduced the German Crypto Markets Supervision Act (*Kryptomärkteaufsichtsgesetz* – KMAG).

German legislation now expressly differentiates between crypto assets within the scope of MiCAR and cryptographic instruments (*Kryptografische Instrumente*) which are outside the scope of MiCAR. The latter are still subject to German financial regulatory laws set out in the KWG and the WpIG. The national law provisions on cryptographic instruments function as a catch-all provision

* Christian is a partner in the Frankfurt office of Hengeler Mueller, focusing on banking and financial regulatory matters. He advises credit institutions, investment companies and other financial market participants as well as non-financial enterprises. A particular focus of his work is advising companies on payment services and giving advice on innovative technologies in the financial sector (fintech), in particular in payment services and asset management.

for crypto assets not regulated under MiCAR: ie, crypto assets that qualify as financial instruments pursuant to MiFID II. Cryptographic instruments:

- are neither issued nor guaranteed by any central bank or public entity;
- do not have the statutory status of a currency or money; but
- based on agreements or actual practice, are accepted by natural or legal persons as means of exchange or payment or serve investment purposes; and
- can be transferred, stored or traded electronically.

Entities engaging in custody business regarding such cryptographic instruments, eg, by providing certain wallet services, require a licence as a financial services institution under the KWG or as an investment firm under the WpIG. The qualified cryptocustody business (*qualifiziertes Kryptoverwahrgeschäft*) is defined as the safekeeping, safeguarding or administration of cryptographic instruments and the safeguarding of private keys, which serve to hold, store or transfer cryptographic instruments, crypto securities (*Kryptowertpapiere*) within the meaning of the German Electronic Securities Act (*Gesetz über elektronische Wertpapiere – eWpG*) or crypto fund units within the meaning of the German Regulation on Crypto Fund Units (*Verordnung über Kryptofondsanteile – KryptoFAV*). Offering wallet services for cryptographic instruments will typically be characterised as qualified cryptocustody business and therefore require a licence under the KWG or the WpIG if provided commercially or on a scale that requires a commercially organised business undertaking.

Licensed entities are subject to ongoing prudential requirements, including own funds and business organisation requirements, and supervision by German financial regulators BaFin and Deutsche Bundesbank. In addition, they are subject to ongoing regulatory requirements, including the need to establish a proper business organisation and governance (eg, suitability of managing directors, establishment of internal control functions, etc) and certain disclosure requirements.

Similarly, the operation of a crypto securities register (*Kryptowertpapierregister*) used to issue crypto securities pursuant to the eWpG requires a licence pursuant to the KWG or the WpIG.

Particularly since the introduction of licensing requirements for cryptocustody business in 2021, crypto service providers have gained increased regulatory attention. Over time, BaFin has increased resources and developed a good understanding of the crypto market, its major players and business models. In terms of priorities, it seems that BaFin has a particularly close look at the AML compliance of crypto service providers.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment service providers in Germany require a licence under the ZAG. The ZAG sets out an exhaustive list of regulated payment services, all related to money in cash, bank accounts or e-money. For such business activities, ZAG sets out certain requirements, inter alia, as to the qualification of management, capital requirements and risk management.

In the administrative practice, a number of minimum requirements regarding IT security and IT risk management of payment service providers have been established (BaFin circular on Payment Services Supervisory Requirements for the IT of Payment and E-Money Institutions (*Zahlungsdienstaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten* or ZAIT)). These have however been replaced by the European Digital Operational Resilience Act (DORA). Germany has not made use of the option of Article 32 of the second EU Payment Services Directive (PSD2) to introduce a simplified form of PSP.

In principle, the general licensing requirements for all types of payment services providers are the same, with the exception that companies exclusively providing account information services do not require a licence but a mere registration with BaFin. By the end of 2022, there were 81 companies domiciled in Germany with a licence for payment services or e-money business. Credit institutions (ie, banks) are still major players in the market for payment services in Germany, which may account for the relatively small number of companies licensed under the regime for payment service providers.

4. Special support for fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

There are no national special programmes supporting fintech and fintech startups. Neither German legislators nor the German regulators have created a special sandboxing regime for fintechs and rather follow the approach ‘same business, same risks, same regulation’.

However, financial regulators and policymakers are generally receptive to fintech innovation and technology-driven new entrants to the financial services markets. This has manifested itself in various ways. In 2017, the German Ministry of Finance established the German FinTech Council, which advises the ministry on fintech matters. Moreover, the Ministry of Finance documents its interest in fintech, among others, by organising events. BaFin has also significantly intensified its fintech-related activities recently and, among others, provides dedicated information for various fintech business types on its website.

One regulatory sandbox, which applies to the fintech ecosystem and is directly applicable in Germany, is Regulation (EU) 2022/858 (DLTR). The DLTR provides for a regulatory sandbox with regard to financial instruments that are issued, recorded, transferred and stored using distributed ledger technology. The regulation introduces a special regime that allows for certain exemptions from the traditional financial markets framework for market infrastructures based on distributed ledger technology.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Open banking generally refers to the opening of payment accounts for data-based payment services of third-party service providers. The ZAG implements PSD2, which, among others, addresses open banking by establishing rules referring to payment initiation and account information services.

As payment initiation services (*Zahlungsauslösedienste*) and account information services (*Kontoinformationsdienste*) qualify as payment services under the ZAG, any operator of these services is required to obtain a licence or, in case of account information services, registration.

Moreover, under the ZAG and the specifying Commission Delegated Regulation (EU) 2018/389, providers of payment initiation and account information services are obliged, inter alia, to meet a high standard of customer data protection and to ensure secure communication via appropriate interfaces.

6. Regulation of virtual asset service providers.

Virtual asset service providers are by now mostly regulated by European law.

As described above, the European law and the national law differentiate between crypto assets that qualify as financial instruments pursuant to MiFID II and crypto assets within the scope of MiCAR: the former being subject to the traditional financial markets framework and its national implementation acts and the latter being subject to the European crypto markets framework. Therefore, with the exception of the aforementioned qualified custodianship business (*qualifiziertes Kryptoverwahrsgeschäft*), and the operation of a crypto securities register (*Kryptowertpapierregister*), national German law only provides ancillary regulation of virtual assets service providers.

Complementary to MiCAR, the Crypto Markets Supervision Act (*Kryptomärkteaufsichtsgesetz – KMAG*) stipulates, eg, the competence of BaFin and Deutsche Bundesbank to supervise entities licensed pursuant to MiCAR, further specifies the licensing procedure, and implements a disclosure regime.

Institutes that publicly offer asset-referenced tokens or seek their admission to trading, publicly offer e-money tokens or seek their admission to trading, and crypto asset service providers are subject to MiCAR and the KMAG. Crypto asset services include:

- the provision of custody and administration of crypto assets,
- the operation of a trading platform for crypto assets,
- the provision of advice or portfolio management on crypto assets; or
- the provision of transfer services for crypto assets on behalf of clients.

Virtual assets service providers that provide qualified custodianship business (*qualifiziertes Kryptoverwahrsgeschäft*) or operate a crypto securities register (*Kryptowertpapierregister*) are regulated as either financial services providers pursuant to the KWG or investment firms pursuant to the WpIG, as described above.

7. AML and the Travel Rule in crypto asset transactions.

Both financial services institutions and crypto asset service providers are subject to AML regulations under the German Money Laundering Act (*Geldwäschegesetz – GwG*) and – from 10 July 2027 – the Regulation (EU) 2024/1624 on money laundering (AMLR). They are obliged to establish

effective risk management, including the performance of risk analysis and the establishment of internal security measures, which, among others, requires the appointment of a money laundering reporting officer (MLRO). Furthermore, obliged entities must perform know your customer (KYC) checks, engage in proper transaction monitoring and file suspicious activity reports with the German Financial Intelligence Unit.

German lawmakers on a national level initially implemented the Travel Rule in the German crypto asset transfer regulation (*Kryptowertetransferverordnung*) as proposed by the Financial Action Task Force (FATF) on 21 June 2019. The Travel Rule is essentially a regulatory instrument to track the flow of crypto assets requiring operators of crypto services involved in the transfer of crypto assets, such as cryptocustodians, to exchange (personal) information with other operators of such crypto services.

With the amendment of the Regulation (EU) 2023/1113 on the transfer of funds (TFR 3) and the inclusion of crypto transfers therein, the national crypto asset transfer regulation ceased to apply. The TFR3 requires the crypto asset service provider of the originator of a transfer to provide information on the originator and the beneficiary of a transfer to the crypto asset service provider of the beneficiary. The crypto asset service provider of the beneficiary must implement effective procedures to detect whether any required information is missing and verify the accuracy of the provided information before making the crypto assets available to the beneficiary. Under German law, the GwG now explicitly requires crypto asset service providers to take appropriate measures to fulfil the requirements of TFR 3.

Further, TFR 3 requires Member States to address the risks associated with transfers of crypto assets directed to or originating from self-hosted addresses. To fulfil this obligation, the German legislator introduced Section 15a GwG, which requires service providers that execute such transfers to determine and assess the risk of money laundering, terrorist financing and circumvention of financial sanctions associated with the executed transfer and take appropriate risk mitigation measures.

8. Enforcement and cross-border recognition of tokenisation and structuring of secured transactions involving crypto assets.

German civil law so far does not provide for a specific comprehensive legal framework for the tokenisation of assets, ie, the transformation of – particularly non-digital – assets (eg, real estate) into digital tokens. In 2021, legislation introducing ‘electronic securities’ was introduced by the eWpG. Tokenisation is possible within the scope of the eWpG. However, under the eWpG, tokenisation is limited to financial instruments. There is so far no broader legislation allowing, for example, to avoid statutory form requirements for the transfer of certain assets such as real estate by a ‘tokenisation’ of such assets.

The eWpG encompasses the issuance of electronic bearer bonds, bearer shares and registered shares. It differentiates between two types of electronic securities registers: the central securities register (*zentrales Wertpapierregister*) and the crypto securities register (*Kryptowertpapierregister*). While the former is mainly used to dematerialise the traditional book-entry system of central securities depositories, the latter utilises distributed ledger technology for the issuance of electronic securities. Further, the eWpG applies correspondingly to electronically issued fund unit certificates, which may

be issued by using distributed ledger technology pursuant to the German Regulation on Crypto Fund Units (*Verordnung über Kryptofondsanteile* – KryptoFAV). The eWpG differentiates two types of registration. Either the security is registered in the name of the investor (*Einzeleintragung*) or in the name of an intermediary (*Sammeleintragung*). To be tradeable on a trading venue, the securities must be registered in the name of a central securities depository.

Electronic securities within the scope of the eWpG are by law deemed to be objects (*Sache*) for property law purposes. Because of this statutory fiction, a security interest in an electronic security registered in the name of an intermediary may be created by applying the property law principles governing security interests in traditional, intermediary-held securities. For electronic securities registered in the name of the investor, the eWpG stipulates the additional requirement to register the creation of the security interest in the electronic securities register.

Whether a German court would recognise a governing law clause in a crypto asset-related contract is dependent on the scope of the choice of law. While the parties of a contract are generally free to choose the law applicable to the contract itself pursuant to the Regulation (EC) No 593/2008 (Rome I Regulation), the law applicable to *in rem* rights in a crypto asset cannot be chosen by the parties. The law governing the *in rem* rights in a crypto asset is to be determined objectively according to the relevant provisions of private international law. The private international law of crypto assets is subject to ongoing discussions in the German legal literature and, as of the time of writing, is not entirely clear. Some clarity exists with regard to crypto securities, to which the conflict of laws rules for securities, Section 17a of the German Safe Custody Act (*Depotgesetz* – DepotG) and Section 32 eWpG apply.

Should the governing law be German law, *in rem* rights to a crypto asset are only recognised in electronic securities within the scope of the eWpG and electronic securities issued under a foreign law, which are held in book-entry form with the German central securities depository. Hence, due to the limited possibility of tokenisation under German law, a careful analysis of the law governing the *in rem* rights in a crypto asset is crucial.

9. Litigation and jurisdiction on crypto assets: legal implications of disputes involving crypto assets.

Among parties who are not consumers, a party's submission to a foreign court by means of a jurisdiction clause is generally binding and enforceable under German law. Should the parties agree on the competence of a court of another Member State of the EU, the Regulation (EU) No 1215/2012 (Brussels Ia Regulation) on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters applies; should the parties agree on the competence of a court of another member state of the Lugano Convention or the Hague Convention on Choice of Court Agreements, said conventions apply. Pursuant to the Brussels Ia Regulation, Lugano Convention and the Hague Convention on Choice of Court Agreements a jurisdiction clause establishes an exclusive place of jurisdiction unless the parties agree otherwise.

Only if no other convention or treaty on matters of jurisdiction is applicable, the German Code of Civil Procedure (*Zivilprozessordnung* – ZPO) applies to the validity of a jurisdiction clause, making the ZPO's scope of application in these matters rather small. Pursuant to national law, merchants (*Kaufleute*) within the meaning of the German Commercial Code (*Handelsgesetzbuch* – HGB)

are free to submit themselves to a foreign jurisdiction. If the parties do not qualify as merchants, the ZPO requires at least one party to not have a general place of jurisdiction (*allgemeiner Gerichtsstand*) in Germany and the jurisdiction clause to be agreed on in written form or orally under written confirmation. However, while the prorogation of a foreign court's competence is valid pursuant to the ZPO, the exclusive jurisdiction of a German court cannot be derogated. Therefore, should the ZPO apply, exclusive jurisdiction clauses are not effective insofar the exclusive jurisdiction of a German court is derogated.



the global voice of
the legal profession®

International Bar Association

Chancery House
53-64 Chancery Lane
London WC2A 1QS
United Kingdom
Tel: +44 (0)20 7842 0090
Fax: +44 (0)20 7842 0091
Email: editor@int-bar.org
www.ibanet.org