

Austria

Stephan Heckenthaler
Binder Grösswang, Vienna
heckenthaler@bindergroesswang.at

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

There is no special fintech or financial innovation legal framework established in Austria. There is also no legal definition of fintechs available.

However, the Austrian regulator, the Financial Market Authority (Finanzmarktaufsichtsbehörde or FMA) has publicly expressed its understanding of fintech companies. According to the FMA, companies that are active in the field of financial market technologies are commonly understood as fintechs. Fintechs typically focus on information technology-based financial innovations, which are mostly – but not exclusively – developed by companies that do not hold regulatory licences, include interfaces to undertakings that hold regulatory licences and may bring sustainable changes to the existing way of functioning of the financial sector.

Depending on the services offered and whether these services qualify as regulated financial services, fintechs active in Austria might – like all other companies – be subject to a licence requirement under the Austrian financial regulatory laws. The Austrian regulator has adopted a technology-neutral approach in this regard, which means that it is not the involved technology that is decisive, but the activity as such (substance over form).

The Austrian Banking Act (*Bankwesengesetz* or BWG) and the Austrian Securities Supervision Act (*Wertpapieraufsichtsgesetz 2018* or 'WAG 2018') provide for licensing requirements for regulated banking and investment services. The Austrian Payment Services Act (*Zahlungsdiensteengesetz 2018* or 'ZaDiG 2018') provides for licensing requirements for regulated payment services. The management of investment funds or alternative investment funds is subject to a licensing requirement under the Austrian Investment Funds Act (*Investmentfondsgesetz* or InvFG) or the Alternative Investment Funds Manager Act (*Alternatives Investmentfonds Manager-Gesetz* or AIFMG). The provision of crypto asset services in Austria is now subject to a licensing requirement under Regulation (EU) 2023/1114 (the European Regulation on Markets in Crypto-Assets or 'MiCAR').

If securities or investments are publicly offered and where there is no applicable exemption available, the requirement to publish a prospectus is required. Prior to starting any fintech business in Austria, we recommend conducting a thorough legal analysis to determine whether any regulated services might be carried out and whether a licence, registration or prospectus requirement would apply. FMA is generally strict, and any unauthorised provision of regulated services can result in high administrative fines.

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

The European Union legislator has adopted MiCAR, which entered into force on 29 June 2023. This regulation establishes an entirely new framework for the regulation of crypto asset services.

Article 3 (1), no 5 of MiCAR defines a crypto asset as 'a digital representation of a value or a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology'.

Article 3 (1), no 15 of MiCAR further defines crypto asset service providers (CASPs) as legal persons or other undertakings whose occupation or business is the provision of one or more crypto asset services to clients on a professional basis, and that is allowed to provide crypto asset services.

Currently, the digital euro is planned to be issued by the European Central Bank (ECB) as a central bank digital currency (CBDC). It is designed to coexist with the market for private euro-denominated stablecoins and other crypto assets regulated under MiCAR. The digital euro itself is not a subject of the regulation of MiCAR.

Since 1 March 2022, income from cryptocurrencies in Austria has been classified as income from capital assets under section 27b of the Income Tax Act (EStG). The taxation applies to both current income (such as interest income from lending or mining) and income from realised capital gains resulting from the sale or exchange for other assets other than cryptocurrencies. The trade of a crypto asset against another crypto asset is not subject to taxation.

Investors are mainly protected in the EU through the MiCAR with mandatory white papers and fair marketing, licensing and conduct rules for CASPs, stronger rights for stablecoins, a market abuse regime and the anti-money laundering (AML) 'Travel Rule' (see also section 7).

The accompanying legislation for MiCAR in Austria was enacted through the MiCAR Implementation Act, which designates the FMA as the competent supervisory authority. The FMA is also responsible for the passporting of MiCAR licences to Austria and vice versa.

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

Payment service providers are regulated in Austria based on the implementation of EU directives 2007/64/EC ('PSD1') and 2015/2366 ('PSD2') in ZaDiG 2018.

In line with PSD2, ZaDiG 2018 sets out an exhaustive list of regulated payment services, including:

- incoming and outgoing payment transactions;
- payment transactions involving the granting of credit;
- payment instrument transactions;
- money remittance transactions;
- account information services; and
- payment initiation services.

To provide regulated payment services, payment service providers are required to obtain a licence as a payment institution under ZaDiG 2018. Payment institutions are subject to a range of supervisory requirements, such as requirements relating to own funds and risk management, suitability of directors and reporting. These requirements are based on those that apply to credit institutions. Austria has not made use of the option of Article 32 of the PSD2 to introduce a simplified form of payment institutions.

Providers that provide payment services based on payment instruments that can be used only in a limited way, such as the acquisition of goods or services only in the premises of the instrument issuer or within a limited network or for a limited range of goods or services, are exempted from the scope of ZaDiG 2018 and do not need to obtain a licence. This 'limited network exclusion' stems from PSD2 and especially applies for store cards, fuel cards, membership cards, public transport cards, parking tickets, meal vouchers or vouchers for specific services.

It is noted that purely technical services are not subject to a licence requirement under ZaDiG 2018. However, PSD2 has introduced the regulation of account information services and payment initiation services that until then have been considered purely technical services.

The regulatory framework relating to payment services has been under review, and amendments are on their way. The drafts of PSD3 and a new directly applicable Payment Services Regulation (PSR) were published in June 2023. The current proposal of the European Parliament provides for a 24-month transposition period, meaning that PSD3 must be transposed into national law by spring 2028 at the latest. The PSR automatically enters into force 20 days after its publication in the *Official Journal of the European Union*, but will not take effect until 21 months later.

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.

The Austrian regulator FMA has established the FinTech Point of Contact, which may be contacted by fintechs to ask specific questions relating to licensing requirements, the obligation to publish a prospectus, compliance or AML regulations. FMA made clear that this is not intended to substitute legal advice, but it will give guidance on specific questions.

The FMA further established a special sandbox regime for fintechs in September 2020. A fintech may apply for admission to the sandbox to the FMA and, after admission, operate its business model in a test phase with a licence in the sandbox. If the test is successful, the fintech leaves the sandbox for regular supervision. It is also an objective of the sandbox to deepen the regulator's knowledge about innovations in the financial market.

The sandbox involves four stages: once the FMA has admitted a fintech to the sandbox, the second, pre-support stage, starts. In this stage, FMA experts agree with the fintech on test parameters, milestones and a timetable for the test. Potential restrictions and conditions attached to the licence are discussed. The pre-support stage is concluded with the grant of a licence or registration, and the entity is allowed to provide its regulated services within the scope of the test licence or registration. In the third stage, the actual test phase, the fintech provides its services and is supervised in doing so. In regular management meetings, the test parameters and milestones are discussed. In the last stage, the test phase is evaluated, and the fintech exits the sandbox and is transferred to regular supervision.

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

The term 'open banking' generally refers to services where financial data can be shared between different parties using application programming interfaces (APIs). In particular, data can be shared between payment service providers and third-party service providers. Open banking is therefore not a specific technology, but a new way of offering customers a wider choice of products and services.

PSD2 is the main European legislative body that addresses open banking by requiring payment services providers to grant third-party service providers access to their customers' payment accounts. They must provide access through a secure interface to customers' account information, and the ability to trigger payments via third-party service providers. Consequently, ZaDiG 2018, implementing PSD2 in Austria, is the most important legal act in Austria when it comes to open banking.

Under ZaDiG 2018, two new payment services have been introduced: payment initiation services (*Zahlungsauslösedienste*) and account information services (*Kontoinformationsdienste*). To provide payment initiation services, a licence as a payment institution has to be obtained. As regards account information services, a mere registration with the FMA is sufficient. The most important services offered to customers in this regard are:

- payment initiation services (PISPs): at the request of the customer, a transaction is initiated in relation to a payment account held with another payment service provider;
- account information services (AISPs): at the request of the customer, consolidated information about payment accounts with various payment service providers is made available to them by the account information service; and
- payment instrument issuing service provider (PIISP): a third-party issuer enquires about the availability of an amount of money from the account-managing payment service provider.

The European Commission has recently published a package of legislative proposals concerning financial data access and payments, which will, among other things, replace PSD2. Since the introduction of PSD2 in 2015, the payment market has undergone significant changes globally and in Europe, including in Austria.

As already covered in section 3, the EU legislator proposes to amend and modernise PSD2 with a new Payment Services Directive ('PSD3') and to introduce a directly applicable regulation on payment services – the PSR. One of the aims of the package is to improve competitiveness of open banking services. However, in our view, the new regulatory proposal does not introduce radical innovations, but rather a fine-tuning of the existing regime.

6. Regulation of virtual asset service providers.

With MiCAR, the EU is introducing a unified legal framework for the crypto asset market for the first time. This framework applies to both traditional financial institutions and new players in the crypto ecosystem. Crypto asset services in Austria are no longer subject to a registration requirement under the Austrian Financial Markets Anti-Money Laundering Act, since MiCAR

entered into force. To obtain a regulated status recognised at the European level, these players must meet a set of specific requirements.

The following activities are defined as 'crypto asset services' and are covered by MiCAR:

- providing custody and administration of crypto assets on behalf of clients;
- operation of a trading platform for crypto assets;
- exchange of crypto assets for funds;
- execution of orders for crypto assets on behalf of clients;
- placing of crypto assets;
- reception and transmission of orders for crypto assets on behalf of clients;
- providing advice on crypto assets;
- providing portfolio management on crypto assets; and
- providing transfer services for crypto assets on behalf of clients.

Providers of these services are defined as CASPs. Offering these services generally requires authorisation under MiCAR. Regulations on corporate governance must be outlined in the application, along with proof of proper and appropriate business organisation.

The FMA is the enforcement authority in Austria.

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

The monitoring of transfers of virtual assets in Austria is primarily governed by Regulation (EU) 2023/1113 (the 'new Funds Transfer Regulation'), which came into force on 30 December 2024.

It prohibits anonymous transactions and obliges providers of crypto services to comply with the 'Travel Rule'. This means that providers of crypto services are obliged to record and disclose information about the originators and beneficiaries of their crypto transfers.

According to the regulation, providers of crypto services are obliged to carry out specific due diligence obligations. These include verifying the identity of the sender and recipient, ensuring the accuracy of the information transmitted, recording and storing this data, and the identifiability of self-hosted addresses. Incomplete or incorrect information may result in the rejection, re-transfer or suspension of the crypto transfer.

Violations of these obligations may result in sanctions imposed by the Member States. These are aimed at crypto service providers who repeatedly fail to provide required information or fail to keep records properly. Compliance is monitored by the competent authorities.

The obligations apply to both domestic and cross-border transactions. For transfers abroad, particularly to third countries, specific regulations apply. The regulation ensures the harmonisation

of previous rules of individual Member States at the EU level, thereby facilitating and making cross-border money transfers between Austria and other EU countries safer.

The regulation is directly applicable and enforceable.

In Austria, the FMA is responsible for monitoring compliance with these obligations. In the area of the payment system supervision, the Austrian National Bank (OeNB) also has competences.

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

Real estate cannot be tokenised directly, as a land registry entry is required to acquire a property. Tokenisation is therefore only possible through indirect structures, such as when a corporation acquires the property and the shares in that corporation are tokenised.

Security tokens are regulated by the Austrian Capital Markets Act, the Austrian Securities Supervision Act and the second Markets in Financial Instruments Directive ('MiFID II'). E-money tokens, asset-referenced tokens and utility tokens are regulated in the MiCAR. The regulation of decentralised finance (DeFi) instruments is not entirely clear, since crypto asset services that are provided in a fully decentralised manner without any intermediary should be excluded from the MiCAR.

Under Austrian law, the principle of the possessory pledge generally applies. In any case, a public notice must be issued in order to validly establish a security interest. The issue of when a security interest is created in on-chain technologies is the subject of broad debate and has not yet been settled by the courts or regulated by legislation. However, a draft bill on digital securities and digital assets has been proposed, which suggests establishing a central securities register and creating a security interest upon registration in that register.

Currently, the standard procedure for enforcing a security interest in a crypto asset is foreclosure. Other options include a forced sale or a regular sale of the collateral, though the latter is only possible for pledged units, not for seized units.

In Austria, the rules of the Rome I Regulation primarily apply to the recognition of foreign choice of law clauses. In principle, the principle of party autonomy is respected and foreign choice of law clauses are recognised and enforced by Austrian courts. In the case of crypto assets, essentially the same rules on choice of law apply as for other assets. However, consumer protection provisions and the barrier of public policy (*ordre public*) must be considered.

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

In Austria, agreements on jurisdiction are generally permissible and legally binding under Austrian law.

However, this is largely superseded by the Brussels Ia Regulation, which is directly applicable in Austria. The place of residence of the parties is not decisive, only that the jurisdiction of a court within the EU has been agreed upon. Courts outside the EU are not covered by this.

Such jurisdiction shall be exclusive unless the parties have agreed otherwise. They are enforceable. The agreement conferring jurisdiction shall be:

- in writing or evidenced in writing;
- in a form which accords with practices that the parties have established between themselves; or
- in accordance with international commercial practice.

Regarding crypto assets, it should be noted that this does not apply to consumer transactions. Agreements on other jurisdictions with consumers are only legally binding if:

- it is entered into after the dispute has arisen;
- the consumer is allowed to bring proceedings in courts other than those indicated in section 4 of the Brussels Ia Regulation; or
- if the agreement is entered by the consumer and the other party to the contract, both of whom are at the time of conclusion of the contract domiciled or habitually resident in the same Member State, provided that such an agreement is not contrary to the law of that Member State.

Section 104 JN applies to domestic matters. The agreement must relate to a specific legal dispute or to legal disputes arising from a specific legal relationship and must be documented. Certain legal matters like customer transactions are also excluded here. It is also possible to agree on an exclusive place of jurisdiction.

10. Intellectual property (IP) and crypto assets: legal protection, ownership, enforcement and monetisation of IP rights related to digital and virtual assets.

In Austria, there is no specific category of IP rights for crypto assets. Protection may exist for individual components (code, content, brand/name, design, technology, database or trade secrets) through the usual legal instruments. Ownership and enforcement follow the underlying IP right. Monetisation is possible through licences, assignments, franchising/white label arrangements or service models (eg, software as a service (SaaS)/API). Holding a token or non-fungible token (NFT) does not, by itself, create or transfer any IP; any licence or assignment must be expressly agreed (on or offchain).

Copyright law

Computer programs (source and object code) are protected by copyright if they constitute the author's own intellectual creation, according to harmonised EU law. Creative content such as music, text, art, or three-dimensional (3D) models referenced by NFTs is likewise generally protected by copyright. Databases may be protected as copyright works if the selection or arrangement of their contents reflects the author's own intellectual creation. Mere compilations of facts are not protected as works. Simple databases that do not meet this threshold may nevertheless

be protected under the *sui generis* database right – a related right – where there has been a substantial investment in obtaining, verifying or presenting the contents.

Trademark law

Names of coins, tokens, protocols or a cryptocurrency brand, and/or graphical elements (eg logos) can be protected as trademarks if they are sufficiently distinctive. Trademarks do not protect code, content or functionality.

Patent law

Patent protection is available only for technical inventions; it is not the 'crypto asset' as such that is patentable, but subject matter relating to crypto assets/blockchains that provides a technical solution to a technical problem. Computer-implemented inventions are protectable if they deliver a further technical effect beyond a mere business or mathematical method (eg, novel consensus mechanisms, network security or protocol-level scaling), provided that they meet novelty, inventive step and industrial applicability.

Unfair competition law

The Unfair Competition Act (Gesetz gegen den unlauteren Wettbewerb or 'UWG') can be used to counter freeriding and misleading practices – such as lookalike tokens with confusing branding or imitative database frontends – where the conduct constitutes unfair imitation, in particular by causing avoidable deception as to commercial origin, taking unfair advantage of another's reputation or unduly hindering a competitor. Systematic freeriding on another's efforts may be deemed parasitic and can supplement copyright, trademark, patent or contract claims.



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