

Belgium

Audrey Zegers

Counsel, Altius

Audrey.zegers@altius.com

Elias Nys

Associate, Altius

Elias.nys@altius.com

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

General

The Fintech sector is gaining increasing importance in the Belgian market. Belgium's Fintech industry covers a broad range of products and services, the most common ones being related to payments, lending, insurance, crypto assets and capital markets.

There is no legal definition of Fintech under Belgian law. Fintech (Financial technology) generally refers to start-ups or established firms that use technology to offer innovative processes, products or services in the financial sector. Today, there is also no single legal framework in place governing Fintech entities in Belgium, and so no specific "Fintech license". Depending on their business model and on the nature of the services and products offered, Fintechs and their activities may be subject to a diverse set of financial laws and regulations.

The Belgian legal framework is largely determined by legislative initiatives on a European level that are either directly applicable or transposed and implemented into Belgian law. These essentially comprise:

- **Credit institutions:** the Act of 25 April 2014 on the legal status and supervision of credit institutions (Banking Act).
- **Consumer and mortgage credit providers:** Book VII of the Code of Economic Law.
- **Insurance companies:** the Act of 13 March 2016 on the legal status and supervision of insurance or reinsurance companies (the Solvency II Law) and the Act of 4 April 2014 on insurance.
- **Payment institutions and Electronic money institutions:** the Act of 11 March 2018 on the legal status and supervision of payment institutions and electronic money institutions, access to the business of payment service providers and to the activity of issuing electronic money, and access to payment systems (the "Act of 11 March 2018") and Book VII of the Code of Economic Law.
- **Investment firms:** the Act of 25 October 2016 on the access to the investment services activity and the status and supervision of portfolio management and investment advisory companies, the Act of 25 April 2014 on the legal status and supervision of credit institutions and the Act of 2 August 2002 on the supervision of the financial sector and on financial services.
- **Financial intermediaries:** Book VII of the Code of Economic Law, the Act of 4 April 2014 on insurance and the Act of 22 March 2006 on intermediation in banking services and investment services and the distribution of financial instruments.
- **Crowdfunding service providers:** Regulation 2020/1503 on European crowdfunding service providers for business and the Act of 18 December 2016 on the recognition and definition of crowdfunding and containing various provisions on finance.

- **Credit servicers:** the Act of 20 December 2024 transposing Directive (EU) 2021/2167 of the European Parliament and of the Council of 24 November 2021 on credit servicers and credit purchasers, and amending Directives 2008/48/EC and 2014/17/EU.
- **Crypto-asset service providers:** the Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA).

These are further complemented by executive (Royal) decrees and soft law such as guidelines, circulars and communications issued by our Belgian regulators, the FSMA and NBB.¹

The regulatory financial services framework and the supervisory structure may be overwhelming for new Fintech players. However, various initiatives have been taken by our regulators to make Belgium a fintech-friendly jurisdiction.

Public offers of investment instruments

Public offers of investment instruments in Belgium are regulated by the Act of 11 July 2018 on public offers of investment instruments and the admission of investment instruments to trading on a regulated market ("Prospectus Act"). The Prospectus Act fully implements the Prospectus Regulation (2017/1129) in Belgium but also provides some further gold-plating. Prospectus and/or information note requirements may apply, not only to offerings of transferable securities, but also to offerings of other investment instruments. "Investment instruments" include all types of instruments permitting to carry out a financial investment, regardless of the underlying assets. In practice, this is important, for example, for the offer and admission to trading of certain types of crypto, debt or real estate assets.

Deposit taking

Only credit institutions may receive deposits from the public in Belgium or solicit the public in Belgium in view of receiving deposits. Credit institutions are regulated by the Belgian Act of 25 April 2014 relating to the status and supervision of credit institutions and stockbroking firms.

Lending

It is interesting to note that lending is not a regulated activity as such in Belgium. However, when developing lending as a professional activity, certain licensing and registration requirements as well as mandatory legal provisions may apply depending on the type of clientele that are being targeted.

Following the European law model, Fintech companies offering credit services to consumers have to take into account Belgium's strictly regulated consumer credit framework. Registration as a consumer or mortgage credit provider or intermediary with the FSMA is required, depending on

¹ Belgium has a "Twin Peaks" supervisory architecture. Since April 2011, the supervision of the financial sector and financial markets is shared between the Financial Services and Markets Authority ("FSMA") and the National Bank of Belgium ("NBB").

the intended activities. Strict information, conduct and publicity rules apply. Like in many other jurisdictions, the “buy now, pay later” (BNPL) model has increasingly been capturing consumer interest in Belgium. However, the Belgian regulatory framework often remains an obstacle in the set up of such business models.

Furthermore, when providing lending activities to small and medium-sized companies on the Belgian market, Fintech will also have to take into account mandatory legislation that aims to protect these companies. These mandatory requirements include code of conduct rules, specific information requirements, suitability tests, limitations on prepayment indemnities and nullity penalties on certain termination clauses.

Crowdfunding and peer-to-peer lending

Various types of crowdfunding platforms exist on the Belgian market:

- platforms through which the public can make a donation for a project or enterprise;
- reward-based platforms, which are platforms through which investors deposit money to receive a type of non-financial compensation;
- crowd-lending platforms, which are platforms through which investors invest in a project or enterprise through a loan (also referred to as loan-based crowdfunding); and
- equity-based crowdfunding platforms, which are platforms through which investors invest in a project or enterprise through a contribution in capital in consideration for a participation in the profits.

Since 2017, some of these crowdfunding platforms are regulated under Belgian Law. Since the entry into force of the European harmonising framework in this context, the activities of Belgian crowd-lending and equity-based crowdfunding service providers are regulated by Regulation (EU) 2020/1503 of 7 October 2020 on European crowdfunding service providers for business (“Crowdfunding Regulation”) as supplemented by the Belgian Act of 18 December 2016 on the recognition and definition of crowdfunding and containing various provisions on finance (the “Crowdfunding Act”). Belgian crowdfunding service providers must obtain an authorisation from the FSMA, meet certain organisational requirements, and comply with conduct and information rules (including the provision of key information sheets).

Offers of investment instruments to the public without the involvement of a crowdfunding service provider, might be subject to other financial regulations. For example, if the offer exceeds certain thresholds, then prospectus or information note requirements might apply (see also the section above on public offers).

It is interesting to note that for peer-to-peer lending, the Belgian regulatory framework currently does not explicitly authorise crowdfunding by direct lending by consumers to consumers (as individuals are not allowed to make a public call to borrow money). Nevertheless, there are platforms on the Belgian market that facilitate peer-to-peer lending, such as Mozzeno. Such platforms have a licence as a consumer credit provider and stand between the consumer-investor

and the consumer-borrower. To allow the consumers to (indirectly) invest in peer-to-peer lending, such players issue debt notes in line with the applicable prospectus/information note requirements.

AML/KYC

In Belgium, strict AML and KYC requirements apply not only to financial institutions but also to certain non-financial entities.

Fintech companies subject to these obligations, including crypto-asset service providers and payment institutions, must:

- conduct customer due diligence (CDD) proportionate to each customer's risk profile;
- continuously monitor transactions; and
- report any suspicious transactions to the Belgian Financial Intelligence Processing Unit (Cellule de Traitement des Informations Financières / CTIF-CFI).

The FSMA and the NBB remain vigilant in supervising AML compliance across the fintech sector. Both have issued detailed guidelines, including interpretative notes, and regularly update them on their website. In their publications, the regulators emphasize the need for a robust, risk-based approach — particularly for digital businesses that onboard customers remotely.

Cybersecurity and digital resilience

In today's rapidly evolving financial services landscape, cybersecurity and digital resilience have become critical priorities, especially for fintech companies that often predominantly operate online. As financial institutions increasingly rely on digital platforms to deliver services, they face growing exposure to cyber threats, operational disruptions, and data breaches.

Evolving regulatory frameworks on both sector-wide and the financial sector level, such as the EU's Digital Operational Resilience Act (DORA) and the NIS2 Directive, underline the importance of a proactive approach to ICT risk management.

For financial entities specifically, the Digital Operational Resilience Act (DORA) is a European Union regulation designed to enhance their digital resilience. Effective from 17 January 2025, DORA aims to ensure that banks, insurance companies, investment firms, and other financial entities can withstand and recover from ICT-related disruptions, including cyberattacks and system failures. The assessment and the control of cyber and ICT risks have become key priorities for the NBB in the exercise of its supervision of financial institutions. The NBB has closely been involved in the development of the draft text of DORA as well as the implementing technical standards. Both the NBB and FSMA have also issued further guidance on the implementation of DORA.

Artificial intelligence

Artificial Intelligence (AI) is rapidly transforming the financial sector, particularly through the rise of fintech companies. From automating credit assessments to detecting fraud and personalising financial services, AI tools are becoming central to the digital strategies of both startups and established financial institutions. As this technology becomes more embedded in decision-making processes, the regulatory landscape is evolving to keep pace, most notably through the EU Artificial Intelligence Act (AI Act).

The AI Act is a comprehensive legal framework regulating artificial intelligence. The AI Act sets a common framework for the use and supply of AI systems in the EU. The new act offers a classification for AI systems with different requirements and obligations tailored to a 'risk-based approach'. Some AI systems presenting 'unacceptable' risks are prohibited. A wide range of 'high-risk' AI systems that can have a detrimental impact on people's health, safety or on their fundamental rights are authorised, but subject to a set of requirements and obligations to gain access to the EU market. AI systems posing limited risks because of their lack of transparency will be subject to information and transparency requirements, while AI systems presenting only minimal risk for people will not be subject to further obligations. The regulation also lays down specific rules for general purpose AI (GPAI) models and lays down more stringent requirements for GPAI models with 'high-impact capabilities' that could pose a systemic risk and have a significant impact on the internal market.

Although the AI Act is a general, non-sector-specific regulation, it does address certain financial use cases. In particular, AI systems used for credit scoring or risk assessment in the insurance sector are explicitly classified as high-risk, due to their impact on individuals' access to financial resources or services. As a result, such systems must (in principle) comply with the Act's full range of obligations for high-risk AI systems.

To avoid overlap with existing financial regulations, the AI Act acknowledges that many requirements may already be met through compliance with sectoral legislation (eg, CRD/CRR, Solvency II). Therefore, institutions such as credit institutions and insurance undertakings, which are already subject to detailed governance and risk management rules, are presumed to comply with certain AI Act obligations. However, less strictly regulated entities, such as financial intermediaries or consumer credit providers, may not benefit from this presumption and will need to ensure full compliance with the AI Act independently.

Importantly, all other general provisions of the AI Act continue to apply across the financial sector. This makes the AI Act a new and essential piece of legislation that financial institutions, including fintechs must take into account when deploying AI-based solutions in the EU market. Mid-2024, Fintech Belgium published a report on how the Belgian financial services sector embraces the rise of AI and AI regulation in the market.² According to the report, market research demonstrates significant AI adoption within Belgium's financial sector. Predictive AI is widely implemented, with 84% of institutions utilising it for applications such as customer segmentation, fraud detection, and risk modelling.

2 <https://www.fintechbelgium.be/news/first-belgian-ai-barometer-reveals-transformative-impact-on-financial-institutions>

While enthusiasm for AI remains high, several key challenges continue to shape its further development. Priority areas include data privacy, data security, and data quality. At the same time, institutions are grappling with regulatory uncertainty.

Survey results indicate that financial institutions consider existing regulations to be lagging behind the rapid pace of AI innovation. Nevertheless, they do not currently view these regulatory gaps as significant barriers to innovation within the sector. The findings also suggest that, although the regulatory landscape remains somewhat unclear, financial institutions are still actively investing in and deploying AI solutions. This sustained interest may reflect confidence that the evolving regulatory framework, and particularly the introduction of the AI Act, will ultimately provide greater clarity and stability.

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

Existing financial legislation applicable to crypto assets:

Crypto assets come in all forms, sizes and shapes. Depending on their structure, underlying rights, the way they are issued, etc, it is possible that the assets themselves and services associated with them are regulated by existing financial legislative frameworks that were already in place and that are not directly targeted at the regulation of crypto assets. For example, crypto assets may be classified as a security within the meaning of the Prospectus Regulation or as an investment instrument within the meaning of the Belgian Prospectus Act. Depending on how the asset is classified, other legislation may also apply, such as the rules established by MiFID II if the crypto assets are financial instruments.

Financial legislation directed at crypto assets:

MiCA

Since the beginning/mid 2022, certain virtual currency service providers were subject to a regulatory regime in Belgium. The regulatory regime applied to providers of services for the exchange between virtual currency and fiat currency and providers of custodian wallets. It is interesting to note that the FSMA was unable to grant any registrations under this national regime, as no complete file attesting to an applicant's ability to comply with all the legal and regulatory conditions required to obtain such a registration had been submitted.

Since the entry into force of Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto assets ("MiCA"), this national regime has expired.

MiCAR establishes a comprehensive regulatory framework for crypto-assets within the EU, which:

- regulates the issuance, trading and public offering of crypto-assets, including transparency and disclosure requirements;

- introduces licensing for crypto-asset service providers and issuers of asset-referenced tokens and electronic money tokens;
- clarifies the regulatory obligations for issuers of asset-referenced tokens and electronic money tokens, as well as crypto-asset service providers, including consumer protection rules related to the issuance, trading, exchange, and custody of crypto-assets;
- enhances confidence in crypto-asset markets by introducing a market abuse regime that prohibits market manipulation and insider trading; and
- defines the powers, including the cooperation and sanctions framework, available to competent authorities.

Since 30 December 2024, MiCA is directly and fully applicable in all European Union Member States, without needing to be transposed into national law. However, the MiCA provides for a transitional regime for crypto-asset service providers that provided their services in accordance with the national law of an EU Member State before 30 December 2024. The latter may continue to do so in that Member State until 1 July 2026 or until they are granted or refused an authorisation, whichever is sooner.

It is important to note that in Belgium, the competent regulatory authority for overseeing the application of MiCA provisions and the entities within its scope has yet to be appointed under national law. It is expected that the FSMA will be designated as the competent authority, as it was already responsible for supervising the pre-MiCA national regime for virtual currency service providers.

Virtual currency and Crypto publicity

The FSMA issued a Regulation on the marketing of virtual currencies that entered into force on 17 May 2023. This Regulation has three main aspects:

1. the basic principle that advertisements must be accurate and not misleading;
2. advertisements must contain mandatory information that points out the main risks; and
3. mass media campaigns must be notified to the FSMA in advance.

Since the entry into force of MiCA (see above), advertisements that are circulated or published when offering crypto-assets to the public and admitting them to trading, as well as advertisements made by crypto-asset service providers, are governed by this legislative framework. Those provisions are directly applicable in Belgian law and take precedence over the provisions of the FSMA's Regulation.

If the advertisements fall outside the scope of MiCA, they continue to be subject to the Regulation. This is the case, for example, for:

- advertisements disseminated for distributing virtual currencies to consumers in Belgium by persons who do not provide crypto-asset services. This way, influencers or intermediaries who disseminate advertisements when distributing virtual currencies to consumers in Belgium remain subject to the Regulation;

- advertisements disseminated when offering to the public virtual currencies that qualify as crypto-assets with no identifiable issuer. This way, advertisements for the offer to the public of bitcoins for example, remain subject to the Regulation.

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

Payment services are a regulated activity in Europe and Belgium. In Belgium, the PSD2 framework was implemented by the Act of 11 March 2018 on the legal status and supervision of payment institutions and electronic money institutions, access to the business of payment service providers and to the activity of issuing electronic money, and access to payment systems (the “Act of 11 March 2018”) and by the Code of Economic Law (“CEL”). Under the applicable legal framework, payment services can only be provided by certain licensed institutions, such as licensed payment institutions. In addition, certain rules govern the relationship between the payment service provider and its customers and users (especially for consumers) and the execution of payment transactions.

To summarise, PSD2 as implemented by the Act of 11 March 2018, lists the following as regulated payment services:

- (i) services enabling cash to be placed on a payment account;
- (ii) services enabling cash withdrawals from a payment account;
- (iii) the execution of payment transactions;
- (iv) the execution of payment transactions where the funds are covered by a credit line;
- (v) the issuing of payment instruments and/or acquiring of payment transactions;
- (vi) money remittance;
- (vii) payment initiation services;
- (viii) account information services.

Some service providers in the market evade the regulatory regime by structuring their operations and services in a specific way and partnering with licenced service providers. Others make use of exemptions under the law, such as the limited network exemption, whereby no licence as a payment institution is required as the relevant payment instrument meets a specific limited need and allows payment transactions for the purchase of goods or services and can only be used (i) within a limited network of merchants or (ii) for a very limited number of goods or services.

A recent challenge for both banks and innovative payment service providers is and will continue to be the gradual implementation of the Instant Payments Regulation (“IPR”) that entered into force on 8 April 2024. Amongst other, this European regulation aims to promote the use of instant credit transfers, both within and across national borders. The IPR requires payment service providers to ensure that all payment service users in the EU can place payment orders for instant credit transfers in euros and receive instant credit transfers in euros. Another innovation of the IPR is a “verification of Payee” or “VoP” service. In a nutshell, payer’s PSPs are required to offer VoP in relation to

the payee to whom the payer intends to send a credit transfer – i.e. a service for matching the IBAN with the name of the payee/intended recipient of the funds. The latter is expected to have a positive impact in decreasing online payment fraud in the EU that in recent years has severely increased for both consumers and businesses.

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

Although some market players and authors have lobbied for it, Belgium has not yet implemented a financial regulatory sandbox. To our knowledge, there are no plans to introduce such a sandbox in the near future. Nevertheless, our Belgian regulators have identified Fintech as an important theme in today's financial markets and as an important focus of their supervisory activities. They acknowledge that the financial regulatory framework plays a key role in accommodating both innovation and safety within the industry.

Initiatives have been taken to make Belgium a Fintech-friendly jurisdiction. Since 2016, our regulators have been working together to inform market players active in Belgium about the regulation and supervision of innovative financial services and products. In that context, they have launched a joint Fintech contact point, offering Fintech companies the opportunity to contact them directly for the following purposes:

- an explanation of specific supervisory rules, policies and authorisation procedures;
- assistance in navigating the supervisory landscape; and
- information on potential supervisory issues, for example when developing an innovative financial concept.

An important principle employed by our regulators in its licensing procedures and supervision of Fintechs and start-ups in general, is the principle of proportionality. Our regulators aim to consider the nature, size and complexity of a startup's activities and related risks when assessing compliance with legal requirements.

Furthermore, an important platform promoting and supporting the Belgian fintech sector is FinTech Belgium. Apart from promoting the Belgian fintech sector in Belgium and abroad, FinTech Belgium seeks to establish an ongoing dialogue with financial regulators, in order to take into account the Fintech specificities in the regulatory environment and to improve the appreciation by the regulators of the benefits that Fintechs bring to consumers.

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

There is no comprehensive regulation on open banking that is specific to Belgium.

The concept of open banking, where banks and payment service providers share payment account data with other service providers to allow new and different services based on the information shared, has been one of the focus points of the recent legislation on payments at the European level.

Although open banking existed before PSD2 in Belgium, it took place in a largely unregulated environment. PSD2 gave open banking a stable regulatory framework in Belgium, by introducing payment initiation and account information services to its scope and imposing an obligation on banks to facilitate access to payment data for new service providers via a secure interface.

Since PSD2 Belgian Fintechs have been able to leverage PSD2's open banking rules to create innovative solutions. According to a survey conducted by the European open banking platform, Tink, Belgium's bank executives are the most positive in Europe about open banking, with over 87% seeing it as a positive development.³ Open Banking has allowed Belgian banks to develop other income streams by providing extra services such as digital partnerships with telecoms companies (see Beats, a cooperation between Belfius and Proximus).

Nevertheless, there are still some hurdles and limits to open banking in Belgium. Although PSD2 has laid the foundations for open banking, Fintechs still need to obtain a license as a payment institution with the NBB to be able to benefit from the open banking framework. Despite great efforts on the NBB's part, the licensing procedure is still often seen as a brake on the development of new services as it remains a time-consuming and complex procedure for Fintechs.

It is also an issue that some banks still refuse to share their customer data with third-party providers due to an alleged lack of security.

Another downside of the current open banking framework is that some banks are still using their own not-standardised APIs, which sometimes are not compatible with Fintechs' APIs. This means that Fintechs often have had to build several bank-specific APIs, which is again costly and time-consuming.

In June 2023, the European Commission introduced a new package of draft legislative text focused on further developing the payment landscape and legislation at European level which to this date is still being discussed. This initiative makes a number of targeted amendments to the open banking framework to improve its functioning, while avoiding radical changes that might destabilise the market or generate significant further implementation costs. Hopefully this new package, once adopted and implemented in Belgium, will bring the necessary changes to improve the Belgian regulatory and market conditions.

3 The Open Banking revolution – Tink – 2021

6. Regulation of virtual asset service providers: How are virtual asset service providers (VASPs) regulated in your jurisdiction? Please describe the applicable legal and regulatory framework governing the licensing, registration, or authorisation of VASPs, including any specific laws, regulations, or guidelines. Indicate whether there are distinct categories or definitions of VASPs under domestic law, and what types of activities (eg, exchange, custody, transfer) are subject to regulation. Who is the enforcement authority?

Belgium has established a comprehensive regulatory framework for crypto asset businesses. The Financial Services and Markets Authority (FSMA) is the competent authority responsible for the supervision of crypto asset service providers (CASPs). Prior to the entry into application of Regulation (EU) 2023/1114 on Markets in Crypto assets ('MiCA'), the FSMA was responsible for the registration of VASPs under Belgian law.

Under the former Belgian VASP regime (which was in force from May 2022 to 30 December 2024), registration with the FSMA was required for providers of exchange services between virtual currencies and fiat currencies; exchange services between virtual currencies; and custodial wallet providers. The regime was primarily focused on anti-money laundering (AML) compliance and required applicants to establish an appropriate compliance framework; demonstrate that shareholders satisfied fit and proper requirements; and register with the FSMA before commencing activities in Belgium.

Since MiCA has become fully applicable, the regulatory framework has expanded considerably. Whereas the Belgian VASP regime merely required registration and focused primarily on AML compliance, MiCA introduces a comprehensive authorisation regime for CASPs. In addition to AML obligations and fit and proper requirements, CASPs are now subject to, among other things:

- initial capital and own funds requirements;
- enhanced governance and organisational requirements;
- prudential and conduct of business rules;
- safeguarding and segregation of clients' crypto assets and funds;
- outsourcing, conflict of interest and complaint handling requirements;
- operational resilience and ICT risk management obligations; and
- detailed disclosure and reporting obligations.

One of the principal advantages of the MiCA regime is the introduction of an EU passport. While a VASP registration under Belgian law only permitted the provision of services in Belgium, a CASP authorised under MiCA may provide regulated crypto asset services throughout the European Economic Area (EEA) by means of a single authorisation, subject to the applicable passporting procedures.

Entities requiring authorisation

Depending on the services provided, MiCA authorisation may be required for, among others:

- operators of crypto asset trading platforms;
- providers of exchange services between crypto assets and funds or between different crypto assets;
- custodians providing custody and administration of crypto assets on behalf of clients;
- providers of crypto asset transfer services;
- execution, reception and transmission of orders relating to crypto assets;
- providers of advice on crypto assets or portfolio management services;
- issuers of asset-referenced tokens and e-money tokens (subject to the specific MiCA regimes applicable to such tokens); and
- issuers making public offers of crypto assets, which may be required to prepare and publish a MiCA-compliant crypto asset white paper.

Whether decentralised finance ('DeFi') arrangements fall within the scope of MiCA depends on their specific structure. While genuinely decentralised services may fall outside MiCA's scope, arrangements involving identifiable intermediaries or centralised governance may constitute regulated crypto asset services and therefore require authorisation.

7. Anti-Money Laundering (AML) and the Travel Rule in Crypto Asset Transactions: Has your jurisdiction adopted a legal or regulatory framework to impose anti-money laundering (AML) obligations on VASPs, specifically with respect to the implementation of a Travel Rule? Please describe the applicable legal regime, including the scope of obligations imposed on VASPs to collect, verify, and transmit originator and beneficiary information in virtual asset transfers, whether such obligations apply to both domestic and cross-border transactions, and the current status of implementation (eg, enforceable regulation, non-binding guidance, or pending legislation). Additionally, indicate which regulatory or supervisory authority is responsible for overseeing compliance with these obligations.

Belgium has established a legal framework imposing AML and counter-terrorist financing (CFT) obligations on VASPs, which has since been complemented by the EU-wide regime applicable to CASPs under MiCA.

The Belgian AML framework is primarily set out in the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash, as amended (the 'Belgian AML Law') and its implementing Royal Decrees, which implement the EU

Anti-Money Laundering Directives. The Belgian AML Law imposes, among other things, customer due diligence (KYC), ongoing transaction monitoring, suspicious transaction reporting, record-keeping, governance and internal control requirements on Belgian CASPs.

On 24 December 2025, Belgium published a dedicated implementing law in the Belgian Official Gazette to further implement MiCA and the Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto assets (the 'Transfer of Funds Regulation' or TFR), and hence simultaneously amending the Belgian AML Law. With the entry into application of the TFR, CASPs established in Belgium must therefore also comply with the Travel Rule.

Under the Travel Rule, the CASP of the originator must collect, verify (where required), retain and transmit specified information relating to both the originator and the beneficiary of a crypto asset transfer to the beneficiary's CASP. The receiving CASP must have procedures in place to detect whether the required information accompanies the transfer and take appropriate follow-up measures where the information is missing or incomplete. The purpose of the Travel Rule is to enhance the traceability of crypto asset transfers and to strengthen the prevention and detection of money laundering, terrorist financing and sanctions evasion.

Belgium has not introduced additional national Travel Rule requirements beyond those contained in the TFR. Rather, compliance with the Travel Rule forms part of the broader AML/CFT obligations applicable to Belgian CASPs under the Belgian AML Law. The FSMA is responsible for supervising compliance with these requirements in relation to CASPs authorised under MiCA and may issue supervisory guidance regarding their practical implementation.

8. Enforcement and Cross-Border Recognition of Tokenisation and Structuring of Secured Transactions involving Crypto Assets: How are financial instruments structured in relation to tokenised assets (eg, tokenised real estate, digital bonds, DeFi instruments)? What types of collateral are typically used to secure obligations arising in such digital asset transactions? Please describe the procedures to create and perfect a security interest in these types of collateral, including any requirements for notarisation, registration, stamp duty, or other legal formalities. Will the courts in your jurisdiction recognise and enforce a foreign governing law clause in a crypto asset-related contract? In the case of a default, what enforcement procedures are available to secured lenders to realise their security interest and recover their claims? Is a public auction required for enforcement? Can a secured lender appropriate the collateral directly in certain cases?

Belgian law does not yet provide a standalone regime for tokenised assets. The applicable legal treatment depends on the classification of the underlying asset (eg, financial instrument, receivable, real estate interest or crypto asset). Security interests are therefore structured using existing Belgian property, securities and financial collateral law, interpreted in light of relevant EU frameworks (notably MiFID II and MiCA where applicable).

Structuring of security over tokenised assets

Tokenised securities/financial instruments (eg, tokenised bonds or shares)

Where tokens qualify as financial instruments under MiFID II, security is typically taken under the Belgian Financial Collateral Act. Collateral is taken over financial instruments or cash accounts via pledge or title transfer structures. Perfection is achieved through 'control' (custody with a regulated intermediary or contractual control arrangements). No notarisation or registration is generally required.

Tokenised receivables/cashflow assets

Security is commonly taken via pledge over receivables or assignment by way of security. Perfection generally requires notification to the underlying debtor or acknowledgment, unless a silent pledge structure is used (which is enforceable between parties but may have priority limitations against third parties). No general registration requirement applies.

Tokenised real estate (or real estate-linked tokens)

Where tokens represent economic rights to real estate (often via special purpose vehicles (SPVs)), security is taken over the underlying asset or SPV shares. Direct security over Belgian real estate requires a notarial mortgage deed and registration with the mortgage registry. Mortgage tax applies. Share pledges are used to avoid real estate formalities.

Native crypto assets (eg, Bitcoin and Ethereum)

Crypto assets are generally treated as intangible assets. Security is typically created via pledge under the Belgian Pledge Act, perfected through either a registration in the Belgian National Pledge Register and or via control of private keys (often via custodial arrangements, multi-sig structures or escrow with a regulated custodian). No notarisation or registration is required.⁴

Given the typical holding structure of crypto assets, the exercise of a pledgee's rights frequently depends contractually on the cooperation of third parties, such as issuers or custodians, in order to effectively enforce control over the assets. As a result, market practice has developed in Belgium whereby, instead of relying solely on registration in the National Pledge Register, crypto assets are placed in custody with the pledgee or a third-party custodian. The resulting claim, that is, the receivable of the pledgor against the pledgee or custodian for restitution of the assets, is then pledged in favour of the pledgee. This structure helps to mitigate certain issues related to perfection formalities and facilitates more effective enforcement of the security interest.

4 For intangible movable assets other than financial instruments or receivables, current Belgian law generally requires registration in the Belgian National Pledge Register in order to perfect a pledge. With respect to crypto assets, there is often debate regarding their legal qualification, in particular whether they should be characterised as receivables or as mere intangible movable property.

Cross-border recognition and governing law

Belgian courts generally uphold foreign governing law clauses under the Rome I Regulation for contractual obligations, including crypto-related agreements. However, proprietary aspects (eg, creation, perfection and priority of security rights over Belgian situs assets such as real estate or certain securities) remain subject to mandatory Belgian property/security law rules.

Enforcement

Enforcement mechanics depend on the asset class.

- Financial collateral (financial instruments/cash): Secured creditors may enforce via appropriation or private sale without court intervention if contractually agreed, subject to valuation safeguards.
- Pledged receivables: Enforcement typically involves collection directly from the debtor once default is triggered, or assignment/transfer of receivables to the secured party.
- Crypto assets: Enforcement is generally contractual and technical (transfer of control of private keys, liquidation via exchange or activation of smart contract-based enforcement logic). Judicial intervention is possible, but often unnecessary where control-based security is properly structured.
- Real estate: Enforcement requires judicial foreclosure and public auction through a notary. Private appropriation is not permitted for mortgage enforcement.
- Share pledges (SPVs): These may allow appropriation or private sale if contractually agreed and compliant with statutory safeguards; otherwise judicial sale may be required.

Conclusion

Belgium applies a functional, asset-based legal framework to tokenised secured transactions, relying on traditional security concepts (pledge, assignment and mortgage) adapted to digital asset structures. Enforcement flexibility is relatively high for financial collateral and crypto assets through control-based mechanisms, while real estate remains strictly formal and court-supervised.

Cross-border choice of law is generally respected for contractual matters, but does not override Belgian mandatory rules governing security creation and enforcement over Belgian-located assets.

9. Litigation & Jurisdiction on Crypto Assets: Legal implications of disputes involving Crypto Assets. Is a party's submission to a foreign jurisdiction legally binding and enforceable under the laws of your jurisdiction? Are exclusive jurisdiction clauses respected and enforceable?

Disputes involving crypto assets are not subject to a dedicated Belgian jurisdiction regime. They are assessed under general civil/commercial law principles and applicable EU private international law instruments, in particular:

- Brussels I Recast Regulation (EU civil and commercial jurisdiction rules);
- international level: 2007 Lugano Convention – applies where one party is domiciled in a non-EU EEA State (Iceland, Norway and Switzerland) and Brussels Ibis does not apply; and
- Belgian Code of Private International Law (for non-EU scenarios) ('CPIL').

Crypto assets do not alter the jurisdiction analysis; courts focus on the legal characterisation of the dispute (contract, tort, property-like claim, etc).

Submission to a foreign jurisdiction: legally binding?

Belgian courts generally uphold choice of court agreements, including foreign jurisdiction clauses.

Within the EU

Under Article 25(1) of Brussels Ibis, if the parties, regardless of their domicile, have agreed that a court or the courts of a Member State are to have jurisdiction to settle any disputes that have arisen or that may arise in connection with a particular legal relationship, that court or those courts shall have jurisdiction. Such jurisdiction shall be exclusive, unless the parties have agreed otherwise.

Non-EU

For submission to the jurisdiction of a court outside the EU and outside the Lugano Convention states, Article 7 of the CPIL provides that, where the parties, in a matter in which they are free to dispose of their rights under Belgian law, have validly agreed to confer jurisdiction on the courts of a foreign state to hear disputes arising from a legal relationship, and the case is brought before a Belgian court, the Belgian court must defer judgment unless:

- it is foreseeable that the foreign judgment cannot be recognised or enforced in Belgium; or
- the matter has such close links to Belgium that proceedings abroad would be impossible or unreasonable (Article 11 of the CPIL).

Exclusive jurisdiction clauses

For business-to-business (B2B) crypto asset transactions (between professional counterparties), both Brussels Ibis and the CPIL broadly respect exclusive jurisdiction clauses.

Exclusive jurisdiction limits

Irrespective of any choice-of-court agreement, certain matters carry mandatory exclusive jurisdiction in Belgian courts that cannot be overridden.

Under Article 24 of Brussels Ibis, the following matters have exclusive jurisdiction regardless of the domicile of the parties: (1) proceedings concerning rights *in rem* in immovable property – the courts of the Member State where the property is situated; (2) proceedings concerning the validity of the constitution, nullity or dissolution of companies or other legal persons – the courts of the Member State of the seat; (3) proceedings concerning the validity of entries in public registers – the courts of the Member State where the register is kept; (4) proceedings concerning the registration or validity of patents, trademarks, designs or similar rights – the courts of the Member State of deposit or registration; and (5) proceedings concerning enforcement of judgments – the courts of the Member State of enforcement.

Consumer protection

If the crypto user is a consumer, EU and Belgian law gives them protection:

- consumers often can sue in their home country; and
- jurisdiction clauses may be limited or overridden.

Mandatory Belgian law/overriding rules

Belgian courts may still hear the case if:

- Belgian public policy is involved;
- mandatory insolvency rules apply; and
- enforcement of certain rights must occur in Belgium.

Enforcement of foreign judgments

EU Member State judgments

If a foreign court renders a judgment within the EU, the decision is automatically enforceable under Brussels I Recast.

Under Article 45(1) of Brussels Ibis, on the application of any interested party, recognition of a judgment shall be refused: (a) if such recognition is manifestly contrary to public policy (*ordre public*) in the Member State addressed; (b) where the judgment was given in default of appearance and the defendant was not served in sufficient time; (c) if the judgment is irreconcilable with a judgment given between the same parties in the Member State addressed; (d) if the judgment is irreconcilable with an earlier judgment given in another Member State or in a third State between the same parties involving the same cause of action; or (e) if the judgment conflicts with the protective jurisdiction provisions for insurance, consumer or employment contracts, or with Article 24 exclusive jurisdiction.

Non-EU foreign judgments

A decision by a foreign court outside the EU requires prior Belgian exequatur procedure.

Under Article 25(1) of the CPIL, a foreign judicial decision shall not be recognised or declared enforceable if: (1) the effect of recognition or enforcement would be manifestly incompatible with Belgian public order (*ordre public*); (2) the rights of the defence were violated; (3) the decision was obtained solely to evade the application of a law designated by the CPIL in a matter where the parties cannot freely dispose of their rights; (4) the decision is still susceptible of an ordinary remedy; (5) the decision is incompatible with a decision rendered in Belgium or with a prior foreign decision recognisable in Belgium; (6) the claim was brought abroad after Belgian proceedings between the same parties on the same subject matter had already been instituted; (7) the Belgian courts had exclusive jurisdiction over the claim; (8) the jurisdiction of the foreign court was based solely on the presence of the defendant or of assets having no direct connection with the dispute; or (9) recognition or enforcement would conflict with any specific grounds of refusal in Articles 39, 57, 72, 95, 115 and 121.

Overview

Scenario	Governing framework	Exclusive jurisdiction clause enforced?
Both parties domiciled in EU Member States	Brussels Ibis (Regulation 1215/2012)	Yes – Art 25, subject to Art 24 mandatory rules and consumer/employee protections
One party domiciled in Switzerland, Norway and Iceland	2007 Lugano Convention	Yes – equivalent rules to Brussels Ibis
B2B crypto contract, one party outside EU/Lugano	Belgian CPIL (Art 7)	Yes – Belgian court must stay proceedings in favour of foreign court unless judgment cannot be recognised
Consumer crypto contract (retail CASP)	Brussels Ibis Arts 17–19	No – pre-dispute jurisdiction clause derogating from consumer protection is invalid
Dispute concerns Belgian immovable property	Brussels Ibis Art 24(1)	No – Belgian courts have mandatory exclusive jurisdiction
Arbitration clause	New York Convention + Belgian Judicial Code	Yes – enforced separately; Belgian courts refer parties to arbitration
Recognition of EU Member State judgment	Brussels Ibis Arts 36–52	Automatic, no exequatur; refusal only on Art 45 grounds
Recognition of non-EU foreign judgment	CPIL Arts 22–25	Exequatur required

10. Intellectual Property & Crypto Assets: Legal protection, ownership, enforcement, and monetisation of IP rights related to digital and virtual assets. Please briefly describe how innovations and inventions are protected in your jurisdiction, how ownership is determined, and how such rights are enforced and defended against third-party claims. How do you assess whether to seek protection in foreign jurisdictions, and what criteria are used to choose those jurisdictions? Can IP over crypto assets be monetised locally, and are there any legal restrictions?

Legal Framework

Belgium provides protection for intellectual creations through a combination of national law and EU harmonised regimes, including:

- copyright law (automatic protection upon creation);
- patent law (registration required);
- trademark law (registration required);
- database rights (*sui generis* protection); and
- trade secrets protection.

The EU framework includes harmonised regimes such as:

- European Patent Convention;
- EU Trademark Regulation; and
- Directive (EU) 2016/943 on Trade Secrets.

Their applicability depends critically on the nature of the crypto asset and IP right concerned (eg patents may be granted for specific technical innovation using algorithms; copyright protection may be available for certain source/object code and design materials; databases may benefit from database rights; and CASP brand names, tokens or exchange names may be registered as trademarks).

Ownership

Ownership depends on the creation context:

- individual creator: initial ownership vests in the author/inventor;
- employment relationship: the employer often owns IP created in the scope of employment (subject to contract and statutory rules); and
- commissioned work: ownership depends on contractual allocation (no automatic transfer in many cases).

Enforcement

IP rights are enforced through civil and sometimes criminal proceedings.

Civil enforcement tools

The tools include:

- injunctions (cease and desist orders);
- damages claims (actual damages or, alternatively, infringer's profits or a lump-sum royalty as an approximation);

- seizure and destruction of infringing goods or materials; and
- publication of judgments.

Criminal enforcement:

Belgian criminal law provides for IP-specific offences under Book XI of the Code of Economic Law (Articles XI.332 *et seq*). Wilful copyright infringement carries criminal penalties. Trade secret misappropriation can give rise to criminal liability under the Trade Secret Act (Law of 30 July 2018) and under general criminal provisions on corporate espionage.

Digital enforcement mechanisms

The mechanisms are:

- takedown requests (platform-based enforcement);
- domain name disputes; and
- enforcement against intermediaries (hosting providers, exchanges and marketplaces).

Burden of proof

Rightsholders must generally prove:

- existence of IP right;
- infringement; and
- causation of damage.

Monetisation of IP rights in the crypto context

IP rights can be commercially exploited in Belgium through:

- licensing agreements (software, protocols and branding);
- software as a service (SaaS) and API monetisation;
- non-fungible token (NFT) licensing (digital art, media and collectibles);
- token-based access models (utility tokens linked to IP use); and
- franchising or white-label blockchain infrastructure.

Monetisation is generally permitted under Belgian law, subject to:

- contract law principles;
- consumer protection rules (where applicable);
- IP licensing rules; and
- anti-fraud and financial regulation constraints.

Foreign protection

IP protection is territorial. Protection must generally be obtained per jurisdiction or via regional systems, for example, EU-wide protection (EU trademarks and EU designs), European patent route via the European Patent Convention (EPC) system and United States protection for software/tech-heavy inventions.

Criteria for choosing jurisdictions include:

- market relevance (where users/customers are located);
- enforcement strength (court efficiency and injunction availability);
- level of IP protection (patentability thresholds and copyright enforcement);
- piracy or infringement risk;
- commercialisation strategy (licensing or distribution markets);
- investor expectations (venture capital (VC)-backed global filings); and
- regulatory environment for digital assets.



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