

Poland

Krzysztof Wojdyło

Wardyński i Wspólnicy, Warsaw
krzysztof.wojdylo@wardynski.com.pl

Joanna Werner

Wardyński i Wspólnicy, Warsaw
joanna.werner@wardynski.com.pl

Konrad Werner

Wardyński i Wspólnicy, Warsaw
konrad.werner@wardynski.com.pl

Monika Górską

Wardyński i Wspólnicy, Warsaw
monika.gorska@wardynski.com.pl

Julia Padlewska-Oleksy

Wardyński i Wspólnicy, Warsaw
julia.padlewska-oleksy@wardynski.com.pl

Bartosz Troczyński

Wardyński i Wspólnicy, Warsaw
bartosz.troczynski@wardynski.com.pl

Jędrzej Figurski

Wardyński i Wspólnicy, Warsaw
jedrzej.figurski@wardynski.com.pl

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

There is no single comprehensive piece of legislation that governs the fintech sector in Poland. Regulations in this respect are scattered over various legal acts adopted on both the national and European Union levels. Below, we present the most important laws and regulations (both in force and foreseen to be adopted in the future) that relate to fintech.

Payment services providers

Payment services are mainly regulated in the second Payment Services Directive ('PSD2')¹ adopted at EU level and implemented in the Polish legal system in the Payment Services Act (PSA).² The PSA regulates the way traditional payment services providers (eg, banks and payment institutions) provide payment services to their customers, and introduces new types of payment services providers along with innovative types of payment services. The former includes account information service providers (AISPs), whereas the latter covers such services as account information services, payment initiation services (PIS) and services relating to confirmation of the availability of funds (CAF) connected with card-based payment instruments. The PSA also regulates e-money institutions and the issuance of e-money; as such, it implements yet another EU-level legislation (the E-Money Directive). See section 3 for more details.

At EU level, work is currently underway on the third Payment Services Directive ('PSD3')³ and Payment Services Regulation (PSR)⁴ package, which is intended to replace the current PSD2 framework. See section 3 for more details.

Open banking

The legal framework for the operation of open banking in Poland is mainly the PSD2, the PSA and Regulation 2018/389.⁵ Under PSD2, the philosophy of access to payment accounts has changed significantly, as authorised third parties (TPPs) can, on behalf of and with the consent of the customer, access account information or order the execution of payments. According to Regulation 2018/389, each account servicing payment service provider (ASPSP) should offer at least one application programming interface (API) allowing secure communication with the TPP. See section 5 for more details.

At the EU level, work is currently underway on the PSD3/PSR package, which is intended to replace the current PSD2 framework. See section 3 for more details.

1 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

2 Act of 19 August 2011 on payment services.

3 Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC.

4 Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010.

5 Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

Crowdfunding

Crowdfunding is regulated on the EU level by the European Crowdfunding Service Providers Regulation (the 'ECSP Regulation'),⁶ which sets out harmonised framework for investment-based (or share-based) and lending-based crowdfunding services providers in the EU. The ECSP Regulation requires such providers to obtain a licence to pursue crowdfunding business in the EU. Such providers are supervised by the Polish Financial Services Authority (the 'Polish FSA').

Artificial intelligence (AI)

The primary legal source that regulates the development and use of AI systems across the EU is the EU AI Act.⁷ The AI Act came into force on 1 August 2024, with certain provisions already applicable; others, particularly those concerning high-risk AI systems, applicable only following a transitional period. Early voluntary implementation of the AI Act's requirements is, however, promoted at the EU level through the EU AI Pact.

The regulation prohibits certain high-risk AI practices such as manipulative systems, social scoring and unauthorised biometric identification, with significant penalties for non-compliance. Companies must identify whether they are providers (developing AI) or deployers (using AI), as each role carries different compliance obligations including quality management, documentation, human oversight and registration requirements. Fintech firms using AI for credit assessment, pricing or customer interaction must ensure transparency by informing users when they interact with AI systems and marking AI-generated content appropriately. The regulation establishes a risk-based framework with stricter requirements for high-risk systems.

Cloud computing

There is no single piece of legislation that regulates cloud computing at present. Various legal acts come into play, in particular outsourcing regulations, data protection regulations, the Digital Operational Resilience Act (DORA)⁸ and the Data Act⁹ (which, in particular, addresses vendor lock-in issues).

Notwithstanding the above, please note that the European Commission is currently working on an EU-wide proposal for a Cloud and AI Development Act. The proposal will focus on three main objectives:

- supporting research and innovation that will accelerate the development of sustainable data centres and cloud solutions;

6 Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937.

7 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828.

8 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

9 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828.

- encouraging private investment in cloud and AI technologies;
- raising the level of data processing security by European cloud service providers.

The Act is expected to work alongside a proposed single EU-wide cloud policy for public administrations and public procurement, aiming to strengthen Europe's digital sovereignty and foster growth of European cloud providers.

Digital ID

The basis for electronic identification, authentication and certification is set out in the eIDAS Regulation,¹⁰ which has been recently amended by Regulation (EU) 2024/1183¹¹ (which entered into force on 20 May 2024) establishing a European Digital Identity Framework (the 'eIDAS 2.0 Regulation'). The primary objective is to implement European digital identity wallets (EDIW), ensuring citizens' right to securely participate in the digital society through digital access to public and private services across EU Member States.

The use of EDIW is voluntary, with open-source architecture giving users full control over data sharing, while alternative identification methods must remain available for those who choose not to use them. Member States must accept EDIW for online public services and provide at least one wallet by 2026, while private sector entities (excluding micro and small enterprises) obliged to use strong customer authentication must accept EDIW within 36 months of implementing acts entering into force. A draft bill adapting Polish regulations to the eIDAS 2.0 Regulation is currently being worked on by the Polish government, with parliamentary legislative process to follow afterwards.

Crypto assets

Crypto assets in Poland are currently governed by the Markets in Crypto-Assets Regulation (MiCAR),¹² which applies directly as an EU regulation. To date, no specific implementing legislation has been enacted at the national level in Poland. Accordingly, the regulatory framework is derived entirely from MiCAR's provisions, which have direct effect across all EU Member States, including Poland. For further details, see section 2.

Capital markets

There is no single comprehensive legislation that governs the operations of fintechs on the capital markets. The most used innovative solutions are algorithmic trading governed by the Regulation 2017/589¹³

10 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

11 Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

12 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.

13 Commission Delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organisational requirements of investment firms engaged in algorithmic trading.

issued under the second Markets in Financial Instruments Directive ('MiFID II')¹⁴ as well as robo-advisory services. Robo-advisory, being a specific and automated method of providing investment advice, is not subject to separate regulations on the provision of brokerage services. In November 2020, the Polish FSA issued a position paper on robo-advisory where it clarified the rules of deployment of this service by investment firms. Please also see our comments concerning the DLT Pilot Regime in Section 2.

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

Legal nature of crypto assets

Currently, the main legislative act dedicated to crypto assets is MiCAR, which defines crypto assets as a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology (DLT) or similar technology. The definition of crypto assets included in MiCAR is very broad, but the scope of MiCAR does not cover all crypto assets that could potentially meet this definition. Article 2 of MiCAR excludes from its scope the following types of crypto assets (in particular): non-fungible tokens (NFTs), financial instruments, funds (except where they qualify as e-money tokens (EMTs)) and deposits (including structured deposits), as well as instruments issued by the European Central Bank (ECB) or central banks of Member States – an exclusion designed to cover those central bank digital currencies (CBDCs) that are designed with the use of DLT technology or other similar technology. To the extent that a particular crypto asset is not directly excluded from MiCAR's scope, it may qualify as:

- An asset-referenced token (ART): that is, a type of crypto asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies.
- An EMT: that is, a type of crypto asset that purports to maintain a stable value by referencing the value of one official currency (eg, USDC). EMTs, while being crypto assets subject to MiCAR, are at the same time e-money subject to PSD2. This creates multiple legal and regulatory challenges (dual licensing, TPP access to custodial wallets being payment accounts, SCA requirements etc) which were initially identified and discussed at the EU level in the European Banking Authority (EBA)'s no-action letter on the interplay between MiCAR and PSD2.¹⁵ Further regulatory clarity around EMTs' dual classification may, nevertheless, require legislative intervention either through the PSD3/PSR package or amendments to MiCAR. ARTs and EMTs are commonly referred to as stablecoins.
- A utility token: that is, a type of crypto asset that is only intended to provide access to a good or a service supplied by its issuer.
- Other crypto asset: for example, bitcoin.

¹⁴ Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast).

¹⁵ Opinion of the European Banking Authority on the interplay between Directive EU 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCAR) in relation to crypto asset service providers that transact electronic money tokens.

Crypto assets to which MiCAR does not apply may be classified in various ways from a regulatory perspective. Such regulatory classification, in turn, will determine the applicable legal framework. For example, to the extent that a particular crypto asset qualifies as a financial instrument, it will generally be subject to MiFID as implemented in Poland in the Act on Trading in Financial Instruments.

Note that the DLT Pilot Regime, established by EU Regulation 2022/858,¹⁶ has been directly applicable in Poland since 23 March 2023. The DLT Pilot Regime is designed to allow for certain DLT market infrastructures to be temporarily exempted from some of the specific requirements of EU financial services legislation that could otherwise prevent operators from developing solutions for the trading and settlement of transactions in crypto assets that qualify as financial instruments, without weakening any existing requirements or safeguards applied to traditional market infrastructures (see motive 6 of the DLT Pilot Regime). The idea is to accelerate and facilitate the development of a digital securities (either tokenised or native) market in the EU.

Despite Poland having the legal framework in place, the regime has seen virtually no practical usage. The limited uptake is attributed to several challenges, including the absence of CBDCs for cash settlement, interoperability issues between DLT and traditional infrastructure, regulatory burdens for technology-driven applicants and restrictive thresholds limiting eligible financial instruments. The European Securities and Markets Authority (ESMA) has identified these low thresholds (shares below €500m market capitalisation, bonds below €1bn issuance and undertakings for collective investment in transferable securities (UCITS) below €500m assets under management) as requiring adjustment to attract more applicants. While the regime represents a significant regulatory innovation allowing capital market functions to be performed on DLT-based infrastructure with derogations from MiFID, the Markets in Financial Instruments Regulation (MiFIR)¹⁷ and the Central Securities Depository Regulation (CSDR),¹⁸ its practical implementation remains an EU-wide challenge rather than a Poland-specific issue.

Tax treatment of crypto assets

Polish tax law applies a specific regime to crypto assets, where the core principle is tax deferral. This deferral ends, and a tax obligation arises, at the moment of a disposal of a virtual currency for consideration. According to the law, this is defined as the exchange of a virtual currency for legal tender (fiat), goods, a service or a property right other than another virtual currency, as well as the settlement of other liabilities with a virtual currency. Consequently, transactions such as a swap between traditional cryptocurrencies, like bitcoin for Ethereum, are considered tax-neutral. The resulting net gain from a taxable disposal is subject to a flat 19 per cent capital gains tax (both for individuals and legal entities). For high-income individuals whose total annual income from all sources exceeds PLN 1m, an additional four per cent solidarity surcharge is levied on the surplus.

16 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU.

17 Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012.

18 Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012.

A significant area of legal uncertainty concerns EMTs or stablecoins. While the current administrative practice of the Polish tax authorities is to treat swaps involving EMTs as tax-neutral, the EU's MiCAR regulation introduces a significant legal consideration. MiCAR classifies EMTs as e-money. Because the Polish law's definition of virtual currency, which is used for tax purposes, explicitly excludes e-money from its scope, the MiCAR framework effectively carves stablecoins out of the established tax-neutral category. This currently creates a legal ambiguity and a risk that swaps involving EMTs could be deemed an immediate taxable event, specifically as an exchange for a 'property right other than another virtual currency'.

Sale and exchange of virtual currencies is exempt from tax on civil law transactions and from VAT.

CBDCs

While work on the digital euro are progressing at the EU level, there are currently no plans to introduce a CBDC (digital PLN) into circulation in Poland. The National Bank of Poland (NBP) has been studying and analysing the introduction of a CBDC. It is also constantly monitoring global trends in this respect. According to an official statement by NBP, it so far has not identified any systemic objective for issuing a Polish CBDC, nor any specific needs of consumers or economic entities that could not be met by traditional payment service providers in Poland but could only be met by the central bank through the introduction of a CBDC. NBP states that the process of supplying banks with PLN is stable and that there are no problems with the issuance and management of currency. The value of cash in circulation is constantly growing, and the Polish payment system and payment instruments are highly innovative. In addition, many diverse and effective digital payment methods are available. Therefore, NBP believes that there is currently no need to introduce a Polish CBDC.

Investor protection in relation to crypto asset transactions

Investors investing in crypto assets may benefit from different investor protection rules depending on the legal classification of crypto assets. For example, to the extent that a particular crypto asset is regulated by MiCAR, licensing and regulatory requirements governing the provision of crypto asset services come into play (and, to a certain extent, requirements stemming from PSD2 legislation with regard to EMTs due to their dual regulatory classification).

For those crypto assets that are financial instruments, the MiFID regulatory framework will apply, in turn. General rules on consumer protection may also come into play if the investor is a consumer (with oversight from the President of the Office for Competition and Consumer Protection). Such consumer-like protection also applies, to a limited extent, to investors being sole traders (mainly in the area of unfair contract terms).

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

Payment services providers (PSPs) are regulated in Poland by the PSA, which implements PSD2 and the E-Money Directive¹⁹ into the Polish legal system.

The PSA specifies which entities may be PSPs and e-money issuers under Polish law. The former group is quite broad and covers both traditional financial institutions (eg, banks) as well as those PSPs which are specifically regulated by the PSA. The latter category includes the following entities.

Payment institutions

These entities are authorised to perform the broadest scope of payment services for their customers (including innovative payment services such as the account information service (AIS) or payment initiation service (PIS) and may also act cross-border. Moreover, provided that certain additional requirements are met, payment institutions may also issue e-money (although certain territorial and quota limitations apply). In order for an entity to become a payment institution, it needs to obtain a licence from the Polish FSA. The process is rather complicated and burdensome, and may take up to 18–24 months to complete.

Small payment institutions (SMIs)

In order to provide payment services as an SMI in Poland, an entity needs to obtain an entry in the register of SMIs maintained by the Polish FSA. The licensing (or, rather, registration) route is less burdensome compared to the one applicable to payment institutions; however, the scope of services that SMIs may render is also limited. Namely, an SMI is not authorised to provide AIS and PIS –to do that, it needs to upgrade its licence and become a payment institution. Moreover, SMIs may only pursue their payment business in the territory of Poland (a limitation that is quite conservatively interpreted by the Polish FSA). In addition, they need to observe quota limits for payment transactions effected by them, as well as certain limits on the amount of funds held for one user on their payment account.

Account information service providers

Please see section 5 for further details.

Payment bureaux

This is another simplified form of providing payment services in Poland: to be exact, of money remittance services, as payment bureaux are not authorised to perform any other payment services. Like SMIs, payment bureaux can only act in the territory of Poland and need to observe quota limits on money remittance transactions that they execute. Payment bureaux are

¹⁹ Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

supervised by the Polish FSA; commencement of activities as a payment bureau needs to be preceded by an entry in the relevant register maintained by the regulator.

Apart from the above PSPs, the PSA regulates the terms and conditions of issuing e-money by e-money institutions. E-money institutions are regulated entities licensed and overseen by the Polish FSA. Apart from issuing e-money, e-money institutions may also provide other payment services (to the extent that these are covered by their licence). For the time being, there has only been one e-money institution licence issued in Poland: in 2019, to a company named Billon Solutions (currently Stabillon).

Custodial wallets of crypto assets and custodial wallet providers may also be subject to PSD2 regulation to the extent that those wallets are dedicated to EMT custody and administration (this is because of EMTs' dual regulatory status – see section 2).

At the EU level, work is currently underway on the PSD3/PSR package, which is intended to replace the current PSD2 framework. The legislative process is still ongoing, with an 18-month national transposition period to follow. PSD3 will:

- unify the regulatory framework for payment service providers and e-money institutions (currently split between PSD2 and the E-Money Directive);
- introduce new requirements including mandatory winding-up plans for all new or renewed authorisations;
- update capital requirements adjusted for inflation; and
- enhance client fund protection mechanisms such as the possibility of holding funds in central bank accounts and mandatory diversification across financial institutions.

The PSR regulation, which will apply directly across the EU, will establish uniform standards for open banking, consumer protection and supervisory coordination, including easier fraud information sharing between providers, mandatory International Bank Account Number (IBAN) and account holder verification systems, improved automated teller machine (ATM) fee transparency, and expanded access to EU payment systems for non-bank payment 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.

Fintech support programmes: Polish FSA

The following programmes which support the development of the fintech ecosystem are currently deployed by the Polish FSA.

- *Innovation Hub*: this legal support programme is dedicated to entities who operate or plan to launch their business in the fintech area, provided that the solution that those entities are planning to implement does not easily fit the existing legal and regulatory framework.

In such cases, eligible participants may run their innovative ideas past Polish FSA officers in order to obtain the regulator's assessment of the innovative business model or product.

- *Virtual Sandbox*: this is a technology testing environment allowing to simulate selected functionalities and services offered on the financial market. Participants gain access to an IT infrastructure that allows them to verify their business assumptions in controlled conditions. For the time being, the Virtual Sandbox is limited to testing basic PSD2 services: that is, PIS, AIS and CAF. Virtual Sandbox is an extension of the Innovation Hub programme and is available to participants of the Innovation Hub.

Apart from the above programmes, there are also the following tools and initiatives of the Polish FSA which have been introduced to support fintech.

- *Interpretations of the Polish FSA*: the interpretations that the Polish FSA may issue are intended to increase legal and regulatory certainty for entities supervised (or planning to become supervised) by the Polish FSA. Interpretations may be requested by entities planning to engage in activities relating to products and services that are intended to develop financial market innovation.
- *Fintech working group*: the purpose of the working group is to identify legal, regulatory and supervisory barriers to the development of financial innovation in Poland and to prepare proposals for solutions that could eliminate or reduce the identified barriers. The Polish FSA acts as a coordinator of this working group.
- *Fintech Interministerial Steering Committee*: the aim of the Committee is to coordinate the activities of various state institutions and bodies in order to support the development of the fintech sector in Poland, to develop common positions and to undertake joint inter-ministerial activities in the field of fintech.
- *#Supervision_Hack*: this is a series of hackathons organised by the Polish FSA, aimed at creating innovative technological solutions to support financial market supervision. During the hackathons, participants working individually or in teams develop innovative projects using advanced technologies such as AI, machine learning and data analysis. The best projects receive cash prizes and the opportunity to be implemented in the supervisory activities of the Polish FSA.

Notwithstanding the above initiatives, it is an expectation of the market to intensify efforts supporting the development of fintech ecosystem in Poland to, inter alia, further advance the migration to a paperless model of doing business by financial market entities and significantly shorten the duration of the licensing proceedings before the Polish FSA. More frequent publication of the Polish FSA's interpretations and positions pertaining to innovative business models would also positively contribute to legal and regulatory certainty on the Polish fintech market.

Institutional support for fintech in Poland beyond the Polish FSA

Several Polish institutions other than Polish FSA also provide support for fintech development.

- Polish Investment and Trade Agency (Polska Agencja Inwestycji i Handlu; or PAIH) facilitates foreign direct investment and internationalisation of Polish enterprises by offering access

to business information, assistance with administrative procedures, legal solutions, location scouting, partner identification and financial instruments through the Polish Development Fund Group.

- Polish Agency for Enterprise Development (Polska Agencja Rozwoju Przedsiębiorczości; or PARP) and the Association of Business and Innovation Centre Organisers in Poland (Stowarzyszenie Organizatorów Ośrodków Innowacji i Przedsiębiorczości w Polsce; or SOOIPP) support entrepreneurship, innovation and competitiveness through three types of centres:
 - entrepreneurship centres (promoting business incubation and supporting small firms);
 - innovation centres (facilitating technology transfer, academic entrepreneurship and science-business collaboration); and
 - para-banking financial institutions (providing tailored financial services to new ventures without credit history).
- Polish Development Fund (Polski Fundusz Rozwoju; or PFR) supports innovative startups and entrepreneurs through its Innovation Development Department, focusing on education (developing innovator competencies), networking (connecting ideas, capital and expertise) and thematic programmes (sector-specific comprehensive services). All programmes are accessible via startup.pfr.pl.
- Technology Transfer Centre (Centrum Transferu Technologii; or CTT) bridges academia and business by facilitating technology commercialisation, managing intellectual property (IP) from research institutions, promoting scientific achievements, providing advisory and training services, conducting technology audits, collaborating with venture capital investors, and securing funding for research and innovative projects.

These institutions collectively create an ecosystem supporting fintech ventures from concept through to commercialisation and scaling.

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

As already indicated, the main display of open banking in Poland is the PSD2 and its implementing legislation, which allows TPPs to access account information or order the execution of payments on behalf of and with the consent of the customer through APIs made available by the ASPSPs. A key element of the open banking ecosystem is a requirement for the ASPSPs to provide open APIs through which TPPs can offer innovative products and services. Detailed requirements relating to such APIs are set out in the Regulation 2018/389 issued under the PSD2. In response to the requirements for open APIs set out both in the PSD2 and in the Regulation 2018/389, the Polish financial sector under the leadership of the Polish Bank Association (Związek Banków Polskich) has developed an interface standard through which banks operating on the Polish market may offer access to their systems to TPPs – the so-called Polish API.

The two main payment services related to open banking are PIS and AIS, both introduced by the PSD2. In this context, services relating to CAF should also be mentioned, although these are

not formally considered to constitute a separate category of payment services under Polish law (although they are intrinsically connected with payment services relating to card-based instruments and, as such, may only be rendered by authorised PSPs).

Payment initiation services are widely used in e-commerce, where payment initiation services providers (PISPs) assist the users in the online payment process without taking possession of user funds. PIS is treated as a regulated payment service and its provision to customers is connected with a necessity to obtain an authorisation from the Polish FSA to operate as a national payment institution. At the same time, the scope of activities of a national payment institution may be much broader than the provision of PIS alone.

Account information services, on the other hand, consist of the provision of consolidated information relating to the user's online payment account or accounts held with one or more other PSPs – for example, an aggregated information concerning balances and turnover on such individual accounts. AIS often forms the basis for building many different business models and offering additional services to customers not always regulated by the PSA: for example, user identity confirmation services. AIS is a regulated payment service and its provision to customers requires an entry in the relevant register maintained by the Polish FSA. Those providers who limit their payment services to AIS are referred to as account information service providers (AISPs). If the AISP intends to provide other payment services on top of AIS, then such provider must obtain a license from the Polish FSA to operate as a national payment institution.

Confirmation on availability of funds services consist of enabling the user to make payments with a card-based payment instrument (eg, a debit card) issued by a third party other than the one that maintains the user's online payment account (ASPSP). In practice, the user enters into a contract with the CAF service provider who, at the same time, is the issuer of the payment instrument to the user. CAF services allow the provider to issue such payment instrument without having to open an account for the user, as the payment instrument is linked to the payment account the user has already set up with a third party ASPSP. CAF services may be provided as part of a service of issuing payment instruments and, as such, requires a licence from the Polish FSA to operate as a national payment institution.

At the EU level, work is currently underway on the PSD3/PSR package which is intended to replace the current PSD2 framework. See section 3 for more details.

6. Regulation of virtual asset service providers.

MiCA – as a directly applicable EU regulation – constitutes the primary legal framework governing the taking up and pursuit of activities relating to cryptoassets in Poland, including the activities of issuers of cryptoassets and cryptoasset service providers (CASPs). MiCA became fully applicable across all EU Member States, including Poland, on 30 December 2024 (with provisions on ARTs and ARTs issuers as well as EMTs and EMTs issuers having applied from 30 June 2024). The grandfathering period under Article 143(3) of MiCA, which allowed entities that were already providing virtual currency services under pre-MiCA national rules to continue operating on a transitional basis, has now lapsed. This development, coupled with Poland's failure to adopt the domestic implementing legislation required to designate a competent authority for the purposes

of granting MiCA CASP licences, has created a serious regulatory impasse for those VASPs that operated in Poland under the pre-MiCA regime – please see our further comments below.

Pre-MiCA ‘VASP’ regime and the end of grandfathering

Prior to MiCA’s full application, the provision of services in the area of virtual currencies in Poland was regulated under the Polish Act of 1 March 2018 on anti-money laundering and counter-terrorism financing (the ‘Polish AML Act’). Under that regime, entities known as virtual asset service providers (VASPs) were required to register in the VASP register maintained by the competent authority and comply with anti-money laundering (AML) obligations. The regulated activities covered: (1) exchanges between virtual currencies and fiat currencies; (2) exchanges between virtual currencies; (3) intermediation in such exchanges; and (4) maintaining custodial accounts of virtual currencies. Following MiCA’s full entry into force on 30 December 2024, and with the lapse of the transitional (grandfathering) period under Article 143 of MiCA, the VASP register regime has effectively ceased to operate. Existing registered VASPs that benefited from grandfathering are no longer authorised to continue operations and are required to wind down, as Polish law does not yet provide them with a pathway to obtain a MiCA CASP licence.

Poland’s failure to designate a competent authority – practical consequences

A key consequence of Poland’s delayed domestic implementation of MiCA is that no competent authority has been formally designated in accordance with Article 93 of MiCA to accept and review applications for CASP licences (or for authorisations concerning the offering to the public or admission to trading of ARTs or other cryptoassets (different from EMTs and ARTs)). This means that, in practice, entities wishing to provide cryptoasset services in Poland under a MiCA licence currently have no authority to apply to. Entities seeking a CASP licence must therefore explore applying in another EU Member State and, if authorised, passport their services into Poland. Under MiCA, the following categories of cryptoasset services are subject to licensing as a CASP:

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

CASPs are subject to ongoing regulatory requirements including capital requirements, governance and conflict of interest rules, conduct of business obligations and prudential supervision.

Special position of EMT issuers

One important exception to the general regulatory impasse concerns issuers of EMTs. Because EMT issuers must be either authorised e-money institutions or credit institutions under MiCA, and because the Polish FSA is already the designated supervisory authority for those entities under existing Polish law, the absence of specific MiCA-implementing legislation in Poland does not prevent EMT issuers from notifying their white papers to the Polish FSA as required under Article 48 and 51 of MiCA. In practice, the company Stabillon sp z oo has already submitted its EMT whitepaper and is listed as an EMT issuer supervised by the Polish FSA in the ESMA register maintained pursuant to Article 109 of MiCA.

Enforcement authority

The Polish FSA is expected to become the primary supervisory and enforcement authority for cryptoasset markets in Poland once the relevant implementing legislation is enacted. Until that occurs, enforcement of MiCA obligations in Poland remains limited in practical terms, as the full supervisory infrastructure – including the ability to grant CASP licences and take formal enforcement action against non-compliant CASPs – is not yet in place.

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

‘The Travel Rule’ in the EU is governed by the Transfer of Funds Regulation (TFR)²⁰ which applies to transfers of both traditional fiat money as well as to transfers of crypto assets by CASPs regulated under MiCAR.

While Poland has not yet implemented TFR-driven changes to the Anti-Money Laundering Directive (AMLD) (dedicated to AML treatment of self-hosted addresses and correspondent relationships concerning crypto assets) or executive provisions concerning TFR itself (eg, concerning penalties for non-compliance), TFR is directly applicable in Poland and, as such, should be complied with by market players.

At the same time, due to the above lack of implementation of executive provisions concerning TFR itself as well as the designation of the Polish competent authority under MiCAR, enforcement of compliance with those obligations is currently challenging. Once these implementing regulations are in force, we will also gain clarity about the authority(ies) that will oversee compliance with these obligations. This group will most likely comprise the Polish FIU – that is, the General Inspector for Financial Information – as well as the authority supervising the crypto assets market in Poland (the Polish FSA or another designated competent authority – see section 6).

20 Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto assets and amending Directive (EU) 2015/849.

Under TFR, the regulatory requirements target CASPs in accordance with their MiCAR definition, leading to ambiguity about whether VASPs benefiting from the transitional regime (grandfathering) and therefore lacking CASP licences fall within scope. Nevertheless, the EBA, ESMA and various national AML/counter-financing of terrorism (CFT) supervisory bodies throughout the EU, including Poland, have articulated the position that TFR provisions apply equally to such VASPs.

TFR applies where at least one of the CASPs involved in the transfer of crypto assets is established or has its registered office in the EU. It applies to both domestic and cross-border transfers. As explained in point 27 of the TFR's preamble:

'Due to the inherent borderless nature and global reach of transfers of crypto assets and of the provision of crypto asset services, there are no objective reasons to distinguish the treatment of money laundering and terrorist financing risks of national transfers from that of cross-border transfers, and no exemption from the scope of the TFR is granted to domestic low-value transfers of crypto assets, in line with the FATF requirement to treat all transfers of crypto assets as cross-border'.

The main obligations include the following.

Information requirements

CASPs of the originator must ensure transfers are accompanied by:

- originator's name;
- distributed ledger address and crypto asset account number (where applicable);
- originator's address, official document number and customer identifier (ID), or alternatively date and place of birth; and
- legal entity identifier (LEI) where provided.

Similar information is required for the beneficiary, including name, distributed ledger address, account number (where applicable) and LEI where provided. Information must be submitted in advance of, simultaneously or concurrently with the transfer, in a secure manner. The information need not be attached directly to the transfer itself.

Verification requirements

Before transferring crypto assets, the CASP of the originator must verify the accuracy of originator information based on documents, data or information from a reliable and independent source. The CASP of the beneficiary must verify beneficiary information before making crypto assets available. Verification is deemed complete where customer due diligence has been conducted under the AMLD.

Self-hosted addresses

For transfers to self-hosted addresses, CASPs must obtain and hold both originator and beneficiary information and ensure individual identification; for amounts exceeding €1,000, CASPs must assess whether the address is owned or controlled by the originator or beneficiary, as the case may be.

The above general requirements stem from TFR. Further details concerning compliance with these are included in EBA's Travel Rule Guidelines.²¹

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

Tokenisation of assets

Tokenisation projects in Poland commonly encounter two fundamental challenges that have substantially limited their adoption.

- First, legal obstacles to the direct tokenisation of ownership rights create significant uncertainty. Polish civil and property law frameworks were not designed to accommodate blockchain-based representations of ownership, making it difficult to structure tokens as direct ownership interests in assets such as real estate.
- Second, there is financial instrument classification risk. To circumvent ownership tokenisation obstacles, project owners often consider granting tokenholders alternative contractual rights – such as profit participation, debt-like claims or economic benefits. However, tokens structured in this manner typically risk classification as financial instruments, triggering substantial regulatory burdens.

Hence, the popularity of tokenisation projects in Poland is limited, with most activity remaining at the pilot stage rather than achieving meaningful market scale.

Types of collateral, creation and perfection requirements, and enforcement

Two scenarios need to be distinguished – one in which security is to be provided in order to secure obligations under transactions involving crypto assets, and the other in which security is to be established over the crypto assets themselves.

In the first scenario, the parties to a transaction have a wide choice of personal and *in rem* security to choose from, depending on the desired type and value of the security, and the scope and types of assets available to be presented as collateral.

The most common types of security interests used to secure various types of obligations in Poland are as follows.

²¹ Guidelines dated 4 July 2024 EBA/GL/2024/11 on information requirements in relation to transfers of funds and certain crypto assets transfers under Regulation (EU) 2023/1113.

Registered pledges

Register pledges can be established over movable assets (vehicles, machinery etc) or transferable property rights (such as shares in companies, claims under bank account agreements and IP rights). To create a registered pledge, the pledgee and pledgor should sign an agreement in simple written form and have the pledge registered in the register of pledges maintained by registry courts. The register is public; therefore, third parties generally cannot legally rely on the lack of knowledge about the existence of the pledge when entering into transactions relating to pledged assets, meaning that registered pledges offer a high level of protection and legal certainty to secured creditors.

Another advantage of registered pledges is that the parties to registered pledge agreements can agree on a prohibition on disposals and further encumbrances of the pledged assets or rights. This prohibition is also subject to registration in the public pledge register and is effective against third parties: this, in principle, makes it impossible for the pledgor to validly encumber the pledged assets in favour of a third party, or to transfer ownership of the pledged assets to a third party.

Another feature of registered pledges worth noting is that they can be established over organised collections of assets or rights (ie, not only on single assets or rights) and that the composition of such collections may be variable, much like in the case of a floating charge.

Finally, unlike most other types of security interests under Polish law, registered pledges may be enforced out-of-court, including by seizure of title to the pledged asset(s) or right(s) by the pledgee, effected on the basis of a written statement served by the pledgee on the pledgor.

Mortgages

Mortgages can be established over real estate. To establish a mortgage, the owner of a real property must issue a statement on the establishment of the mortgage in favour of the secured creditor in the form of a notarial deed. The notary submits such notarial deed to the registry court, which then registers the mortgage in the land and mortgage book maintained electronically for that real property, whereby the mortgage is legally created. The land and mortgage register is public. While mortgages are considered a strong form of security, their drawback is that they can only be enforced in formal court enforcement proceedings, which typically take from a few months up to about two years to complete.

Assignments of claims and security transfers of ownership.

These are not a regulated type of security and are based on the principle of freedom of contracting. In this form of security, the ownership of a movable asset, or a claim or other property right, is transferred/assigned to the secured creditor as security for a receivable. If the secured claim is satisfied, the creditor is obliged to transfer the asset or right back to the transferor (security provider). If there is a default on the secured claim, the transferee may enforce the security by disposing of the transferred asset (and satisfying the secured claim from the proceeds of such disposal) or, in the case of a security assignment of claims, collecting payments from debtors of the assigned claims and applying those collections towards the satisfaction of the secured claim.

Guarantees and suretyships

These are personal forms of security, in which one entity guarantees the performance of an obligation by another entity.

The second scenario, that is, when security is to be established over a crypto asset, is not currently common in Poland. From a formal civil law perspective, it appears possible to establish registered pledges over transferable crypto assets, as they would generally fall into the category of transferable property rights that may be subject to a pledge. However, in practical terms, it remains unclear how enforcement of such security would work against an uncooperative debtor/security provider. At present, given the lack of specific regulation in that regard, the most practical and effective way to establish security over crypto assets might be a security transfer of ownership, as this form of security eliminates the necessity for the secured creditor or court enforcement officer to forcibly effect the dispossession of the security provider from the crypto asset.

It is expected that future Polish legislation ‘implementing’ MiCAR will regulate the establishment of security interests over certain types of crypto assets. However, it is not yet clear whether, and in what precise form, those regulations will come into force.

Choice of law clauses

Polish private law allows the parties to select governing law in a contract. The choice of law does not affect applicability of mandatory regulations enforced in Poland, such as AML regulations. Further statutory provisions of law different than selected may apply depending on nationality of the parties and other elements and characteristics of the contractual relationship: for example, in business-to-consumer contracts subject to EU Regulation Rome I,²² choice of law is allowed but it may not deprive the consumer of protections afforded by statutory provisions that may not be contractually derogated.

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

Polish private law allows forum selection clauses. Poland has not enforced any statutes altering general principles of jurisdiction selection in disputes involving crypto assets. Varying formal requirements and limitations may nevertheless apply depending on the nationalities of contracting parties and other characteristics of their contractual relationship: these may trigger applicability of different international conventions on choice of law (Lugano Convention and Hague Convention), EU law (Brussels I Regulation²³) or Polish Code of Civil Proceedings.²⁴

22 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).

23 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast).

24 Act of 17 November 1964 – Code of Civil Procedure.

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

Protection of innovations and inventions

Innovations and inventions are primarily protected through the patent system governed by the Industrial Property Law.²⁵ Patents are granted by the Polish Patent Office for inventions that are novel, involve an inventive step and are capable of industrial application. Patent protection lasts for 20 years from the filing date. For inventions that do not meet the full patent criteria, utility models offer an alternative form of protection for up to ten years, requiring novelty and industrial applicability but not an inventive step.

Trademarks protecting designations, logos and distinctive signs can be registered with the Polish Patent Office, providing ten-year renewable protection. Industrial designs protecting the aesthetic appearance of products are protected for up to 25 years in five-year renewable periods.

Copyright protection arises automatically upon creation of original works, including software, databases and creative content, which is particularly relevant for crypto-related software and blockchain applications. Protection generally lasts for the lifetime of the author plus 70 years.

Confidential business information, including algorithms, technical processes and business methods related to crypto assets, can be protected as trade secrets under the Act on Combating Unfair Competition,²⁶ provided reasonable steps are taken to maintain confidentiality.

Ownership determination

For patents and utility models, the inventor is the initial owner unless the invention was created within an employment relationship, where the employer typically acquires rights under the employee inventions regime. Inventions made by an employee outside the scope of the individual's employment duties remain the property of the employee-inventor. Parties may agree different ownership arrangements, though such agreements must comply with mandatory provisions protecting employee rights. For jointly created inventions, co-inventors hold ownership in equal shares unless otherwise agreed.

For trademarks, ownership is determined by the first-to-file principle, with the party who first files a valid application with the Polish Patent Office or obtains an EU trademark registration acquiring ownership. Where a mark is developed by an employee in the course of employment, ownership generally vests in the employer, though this is typically governed by the employment contract rather than specific statutory provisions. Ownership of designs works similarly.

For copyright works, the author or creator is the initial owner. However, for works created by employees within the scope of their employment, economic rights typically transfer to the employer while moral rights remain with the author.

²⁵ Act of 30 June 2000, Industrial Property Law.

²⁶ Act of 16 April 1993, on Combating Unfair Competition.

In the context of commissioned works, ownership depends entirely on contractual arrangements: drafting clear IP assignment clauses is essential in development agreements for crypto-related projects. For blockchain and crypto projects, ownership can be particularly complex due to decentralised development models, open-source contributions, questions of smart contract authorship and NFT-related IP rights.

Enforcement and defence

IP rights holders can pursue civil enforcement through several remedies, including injunctions to cease infringement, damages or an account of profits, destruction of infringing materials, and publication of judgments. Since July 2020 there have been separate IP courts in Poland; however crypto-specific cases remain relatively novel.

IP infringements – for example, counterfeiting and piracy – can also result in criminal prosecution under the Industrial Property Law and Copyright Act,²⁷ with penalties including imprisonment. Customs authorities can also seize suspected counterfeit goods at borders following applications for action by rightsholders.

In parallel, there are administrative proceedings available before the Polish Patent Office and if necessary, in administrative courts. These concern oppositions, invalidities and revocations of IP rights.

Mediation and arbitration are rarely used for IP disputes but hopefully will become increasingly popular in commercial contexts involving crypto and technology sectors, offering faster and more confidential resolution than court proceedings.

Choosing foreign jurisdictions

When evaluating whether to seek IP protection in foreign jurisdictions for crypto-related innovations, Polish entities typically start from assessing market relevance. Consideration would include where target users and customers are located, which markets generate or will generate revenue, and where competitors are operating. The decentralised and global nature of crypto assets means that market analysis often points towards multiple jurisdictions.

Manufacturing and development locations are also crucial, including where the technology is developed or deployed, the location of servers or infrastructure, and where potential infringers are located.

Another factor is strategic importance of the territory. Key technology hubs such as the United States, the EU and Singapore are often prioritised, along with jurisdictions with favourable crypto regulation and markets with high crypto adoption rates. The cost-benefit analysis must account for filing and maintenance costs, translation requirements, local representation fees and the potential return on investment – which can be substantial given the global nature of crypto markets.

²⁷ Act of 4 February 1994, on copyright and related rights.

Polish crypto and technology companies commonly seek protection in the EU via the European Patent Office for patents and the EU Intellectual Property Office for trademarks and designs, which allow single application with protection in the whole EU.

International protection is widely pursued through several popular treaty-based mechanisms. The Patent Cooperation Treaty permits a single international application with up to 30 months to enter national phases in designated countries, while the European Patent Convention enables centralised prosecution for multiple European jurisdictions. For trademarks, the Madrid System provides international registration across Member States, and for designs, the Hague System offers equivalent multijurisdictional protection. These mechanisms are increasingly favoured as they substantially reduce administrative burden and initial costs when seeking protection across multiple territories.

Monetisation of IP over crypto assets

IP rights related to crypto assets can be monetised through various methods. Licensing arrangements, whether exclusive or non-exclusive, remain the most common approach, including technology transfer agreements, white-label solutions and franchise arrangements for crypto platforms. Assignment or outright sale of IP rights is also possible, including in the context of asset sales in M&A transactions or treating IP portfolios as investment assets in their own right.

Tokenisation represents a newer and more innovative monetisation method, including fractional ownership through tokens, NFTs representing IP rights and royalty-bearing tokens that distribute income to holders. Direct commercialisation through products and services, including software-as-a-service models for blockchain solutions and subscription-based access to proprietary technology provides another avenue for monetisation. The choice of method depends on the nature of the IP, the business model and the target market.

Tokenisation of IP rights, while legally possible in Poland, raises several specific issues and uncertainties. The legal characterisation of tokens, whether they represent securities, financial instruments or other assets, is not always clear and depends on the specific structure. Questions arise about whether traditional IP assignment formalities apply to tokenised transfers and how token holders can enforce underlying IP rights. The regulatory status of such arrangements continues to develop.



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