EU payments: What's in the regulatory pipeline for 2025?

Hogan Lovells

Contents

In this publication, we take a look at key topics that should be on the regulatory "to do" list for payments industry players in 2025. As well as highlighting upcoming compliance deadlines (for example under the European Accessibility Act and the Instant Payments Regulation), we also provide a snapshot of some existing areas of focus to be aware of – and some that are still taking shape (notably PSD3/PSR, the FiDA proposal and the digital euro project). If you're keen for more detail, you can click through to our selection of related publications and digital client solutions.

There is a timeline of the key dates towards the end of the publication. However, please note that timing for the entry into effect of proposed new legislation is dependent on the EU legislative process so any related timing information is only an estimate and is subject to change.

Click the title to navigate to each section

Directive on Security of Network and Information Systems (NIS2 Directive)

Impacts

The NIS2 Directive forms part of a "package" of European cyber security legislation to increase the level of digital resilience within the EU. It applies to a broader range of firms than the first NIS directive and introduces stronger enforcement powers and penalties for non-compliance.

The NIS2 Directive provides legal measures to strengthen the overall level of cybersecurity in the EU.

The national picture

Germany: Rules set out in the NIS Directive are implemented by the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit und Informationstechnik*; BSI Act) and the corresponding BSI Ordinance Determining Critical Infrastructures (*Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz; KritisV*). Due to political developments in Germany, NIS2 implementation has been delayed. Note, in order to apply, the current German law implementing the NIS Directive requires that the technical infrastructure must be operated in Germany.

Netherlands: In the Netherlands, NIS2 will be implemented into the Cybersecurity Act (*Cyberbeveiligingswet*), which will replace the current Dutch Network and Information Systems Security Act (*Wet beveiliging netwerk- en informatiesystemen*). The Netherlands did not meet the implementation deadline of 17 October 2024.

The Dutch government published a tool on its website, allowing organisations to determine whether NIS2 applies to their organisation, if their organisation is an ''essential'' or ''important'' entity, and whether their organisation falls under Dutch supervision. See: NIS2 Zelfevaluatie NL

Italy: Implemented by Legislative Decree 4 September 2024, n. 138 (accessible here, in Italian only). Secondary implementing acts are envisaged in the Italian decree (here is an up to date list of implementing measures already adopted and to be adopted, in Italian only).

Spain: The Spanish authorities have pushed forward a draft bill on Cybersecurity Coordination and Governance to implement the NIS2 Directive in Spain (the draft bill is not yet available, however). With that being said, the implementation process in Spain has been delayed due to legislative complexities and the need to adapt current structures and regulations.

Belgium: The NIS2 Directive was transposed in Belgium by the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security.

Ireland: The Irish Government published the General Scheme for the National Cyber Security Bill on 30 August 2024, which will transpose NIS2 Directive into Irish law. The Bill will pass through the Irish legislative process, with it being a high priority for the new government.

What to be thinking about

NIS2 requires a higher level of security across sectors that are providing critical infrastructure that is essential for the European economy and society and that heavily rely on ICT providers, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

The NIS2 requirements must be seen together with the Cyber Resilience Act, which applies to hardware, and also the Digital Operational Resilience Act (DORA) which is a more targeted piece of legislation for financial services entities and the third party firms that provide their information and communication technology (ICT) services, as it addresses specific risks relevant to the financial services sector.

Key dates

The Directive must be transposed into national law in EU Member States. Transposition deadline was 17 October 2024.

The new regime applicable since 18 October 2024.

Our insights and tools

The NIS2 Directive in Germany: Looking Ahead

The Data Chronicles: Navigating NIS2 | Cybersecurity in the EU

- Oct. '24
- Jan. '25
- April '25
- June '25
- Aug. '25 to Aug. '27
- Oct '25
- Oct. '25 to July '27
- Nov. '25
- Dec. '25
- Dec. '25
- July '26
- H2 '26 to Q1 '27
- July '27
- Dec. '27
- H2. '27

Digital Operational Resilience Act (DORA)

Impacts

DORA creates a harmonised and comprehensive set of rules for managing information and communication technology (ICT) risk. It applies to all financial entities in the EU/EEA.

The main obligations on financial entities are in the following areas:

- ICT risk management;
- Incident management and reporting;
- Digital operational resilience testing; and
- ICT third-party risk management (including subcontracting).

The scope and depth of DORA go beyond other existing guidelines and legislation on ICT risk management. In addition to the main DORA text, there is a body of secondary legislation comprising 14 additional documents detailing the requirements and together running to several hundred pages.

DORA further establishes a framework that imposes a specific set of obligations for ICT service providers that are considered critical to the stability of the financial ecosystem, and grants supervisory authorities certain powers over such ICT service providers.

National supervisory materials

Netherlands: Relevant information from the supervisors regarding DORA supervision and notifications are available here:

- AFM: Digital Operational Resilience Act (DORA)
- DNB: DORA | De Nederlandsche Bank

Italy: The Italian legislator is currently discussing a draft legislative decree adapting Italian law to DORA. As envisaged in this draft decree, the Bank of Italy, CONSOB (i.e. the financial market authority), IVASS (i.e. the insurance sector authority) and COVIP (i.e. the pension funds authority) would be the DORA competent authorities according to their respective supervisory powers.

Germany: BaFin has created a focus website where it publishes and regularly updates all materials in relation to DORA which is available here: BaFin: DORA – Digital Operational Resilience Act.

Belgium: The Belgian FSMA has published a dedicated portal in relation to DORA (available here Règlement DORA | FSMA). The National Bank of Belgium is very active on the subject. It is strongly committed to the successful implementation of DORA through increasing awareness in the sector by means of various seminars, communications and surveys; facilitating the integration of DORA into the Belgian legal order; developing the necessary ICT tools and processes for data collection and dissemination; adapting existing supervisory methodologies; and anticipating, insofar as possible, the impact that the oversight of critical third parties will have on its activities.

Ireland: The Central Bank of Ireland has a dedicated page where it publishes and updates all materials in relation to DORA here.

What to be thinking about

Becoming DORA compliant is a process, not a switch. There is no "one size fits all" approach and organisations will need to assess and implement DORA requirements in the context of their own business and operational structure.

The current priority for financial entities is to take a proactive approach to achieving compliance in the most significant risk areas in as timely a manner as possible. This includes the resilience of their critical or important functions.

Financial entities should, in particular, focus on:

- completing their registers of information on ICT third-party providers' contractual arrangements. According to a recent joint statement from the ESAs, these will need to be available for competent authorities "early in 2025";
- ensuring they are prepared to classify and report major ICT-related incidents; and
- remediation of contractual arrangements with ICT service providers, prioritising the ICT services that support their critical or important functions.

Key dates

Applicable since 17 January 2025.

Our insights and tools

Hogan Lovells | Operational Resilience Hub

DORA – One week to go

- Oct. '24
- Jan. '25
- April '25
- June '25
- Aug. '25 to Aug. '27
- Oct '25
- Oct. '25 to July '27
- Nov. '25
- Dec. '25
- Dec. '25
- July '26
- H2 '26 to Q1 '27
- July '27
- Dec. '27
- H2. '27

Safeguarding in Germany

Impacts

On 27 November 2024, the German Federal Ministry of Finance published a draft of the Future Financing Act II (*Zukunftsfinanzierungsgesetz* II), a second law on the financing of future-oriented investments. Due to discontinuity of the German federal government, current legislative proposals cannot be finalised and therefore have to be re-drafted and re-submitted by the ministries, which means that all procedural steps have to be taken again.

In response, Alliance 90/The Greens and the Social Democrats parliamentary group published a draft law on 17 December 2024 for urgent changes in the financial market and tax areas. The draft law takes up selected proposals from the ZuFinG II, including the measures for payment/e-money institutions.

One of the most important measures for payment/e-money institutions is the safeguarding of client funds in a separate account at a credit institution or in an account at the Deutsche Bundesbank or another central bank of a member state of the European Union. Hence, it is therefore no longer necessary to maintain an open trust account with a credit institution.

Funds deposited on a trust account must be protected by law: funds received in the course of providing payment services and operating the e-money business are not accessible to the institution's general creditors; Right of segregation (*Aussonderungsrecht*) within the meaning of Section 47 of the German Insolvency Code (*Insolvenzordnung*) in insolvency proceedings for PSUs.

What to be thinking about

The proposed changes consider the needs of the industry by facilitating more flexible business operations while enhancing customer protection.

Firms will need to assess and, if required, modify their internal processes and systems to comply with the new legal standards. This may involve investments in IT infrastructure and staff training.

Key dates

The draft bill has been passed by the German legislator and new rules on safeguarding shall apply from 9 April 2025.

- Oct. '24
- Jan. '25
- **April '25**
- June '25
- Aug. '25 to Aug. '27
- Oct '25
- Oct. '25 to July '27
- Nov. '25
- Dec. '25
- Dec. '25
- July '26
- H2 '26 to Q1 '27
- July '27
- Dec. '27
- H2. '27

Directive on the accessibility requirements for products and services (European Accessibility Act - EAA)

Impacts

The EAA:

- Promotes the equal and non-discriminatory participation of people with disabilities, limitations and older people.
- Covers “consumer banking services“ (including credit agreements, payment services and investment services) and “e-commerce services”. However, pure deposit business is not in scope of “consumer banking services” (only payment accounts and electronic money are covered).
- Also covers payment terminals and ATMs.
- Requires “economic operators” of in-scope products and services to provide certain information in an accessible manner (the two-senses principle), making websites and mobile applications accessible (by making them perceivable, operable, understandable and robust).

“Economic operators” includes financial services providers, including banks, payment service providers and e-money providers. In relation to physical products, “economic operators” includes the manufacturers, authorised representatives, importers and distributors of ATMs and payment terminals.

Where available, support services (help desks, call centres, technical support, relay services and training services) must provide information on the accessibility of the service and its compatibility with assistive technologies, in accessible modes of communication. “Relay services” are not defined in the EAA but are services that allow people with disabilities (e.g. those with hearing and/or speech impairments) to communicate with others through a relay assistant that, for example, converts speech to text.

Additional obligations for consumer banking services are:

- identification methods, electronic signatures, security, and payment services must be perceivable, operable, understandable and robust; and
- information provided must be understandable, without exceeding a level of complexity superior to level B2 (upper intermediate) of the Council of Europe’s Common European Framework of Reference for Languages.

The national picture

Ireland: The EAA has been implemented in Irish Law via S.I. No. 636/2023 - European Union (Accessibility Requirements of Products and Services) Regulations 2023.

Netherlands: In the Netherlands, the Dutch Implementation Act was approved by the Dutch Parliament in April 2024. This act aligns Dutch legislation with the EAA. As from 28 June 2025 the EEA will therefore apply in the Netherlands. See Staatsblad 2024, 87 | Overheid.nl > Officiële bekendmakingen

The accessibility requirements for products and services will be incorporated into various existing Dutch laws and regulations. As far as the financial sector is concerned, the following are in scope:

1. Providers of credit, banks, investment firms, payment service providers, and electronic money institutions, which provide “consumer banking services”;
2. Self-service terminals, which should include payment terminals and ATMs;
3. E-commerce services: services provided at a distance, through websites and mobile device-based services by electronic means and at the individual request of a consumer with a view to concluding a consumer contract.

The legislator has included the rules for banking services in a new Section 4:22.0a of the Dutch Financial Supervision Act (DFSA) and Sections 32ac and 49.0c of the Decree on Conduct Supervision Financial Undertakings DFSA (Decree on Conduct). For self-service terminals and e-commerce services the new Sections 6:230fa to 6:230fd of the Dutch Civil Code (DCC) and 190aa of the Transitional Act New DCC are relevant.

For the financial sector (including financial e-commerce services), the AFM is charged with supervision and enforcement under the DFSA/Decree on Conduct and the Dutch Consumer Protection Enforcement Act (Wet handhaving consumentenbescherming).

Italy: The EAA has been implemented in Italy through Legislative Decree 27 May 2022, no. 82 (accessible here, in Italian only). Secondary implementing acts are envisaged in the Italian decree, but have not been issued yet.

Directive on the accessibility requirements for products and services (European Accessibility Act - EAA) cont.

Impacts cont.

Germany: The EAA has been implemented by the Accessibility Strengthening Act (Barrierefreiheitsstärkungsgesetz; BFSG) and its corresponding regulation. The BFSG Regulation specifies the accessibility requirements in relation to products and services in scope of the BFSG.

Spain: The EAA has been implemented in Spain through Title I of Law 11/2023, of 8 May (accessible here, in Spanish only). Secondary developing regulations are envisaged in the near future.

Belgium: The EAA has been implemented in Belgium through the Belgian Accessibility Law of 5 November 2023, amending several books of the Belgian Code of Economic Law and the law of 2 August 2002 on the supervision of the financial sector and financial services. Further implementing measures are expected.

What to be thinking about

Firms with retail banking products and services will need to ensure that they design their websites, mobile apps and certain communications with consumers, including call centre services as well as devices such as payment terminals and ATMs in a way that is accessible to persons with disabilities.

Firms are required to meet certain information obligations on their services in an accessible manner. This includes an explanation of how the services meet the accessibility requirements, this information must be made available to the public in a written and oral format.

ATMs and payment terminals (card machines) placed on the market on or after 28 June 2025 will need to be designed in accordance with certain international standards (although note that there is a transitional period for payment terminals and ATMs which were lawfully in use before 20 June 2025, which applies either until the end of their life or for 20 years from first use, whichever is sooner).

Firms should consider whether they may be able to avail of an exemption, i.e. where compliance with the EAA requires a significant change in a product or service that would "fundamentally alter its basic nature" or would impose a disproportionate burden. Any firm seeking to rely on an exemption should take advice as any such decision needs to be carefully documented and improper reliance on exemptions could lead to regulatory enforcement action.

Microenterprises providing services or products are exempt from certain accessibility requirements with the aim of preventing undue burdens on them. Microenterprises are defined as businesses with fewer than ten employees and an annual turnover or balance sheet total not exceeding €2 million euros.

Firms providing banking services within the meaning of the regulation or e-commerce services need to ensure that identification methods are accessible. In order to meet these requirements firms can use the Web Content Accessibility Guidelines as a standard for implementation.

Key dates

Applicable from 28 June 2025.

Our insights and tools

Ireland's June 2025 deadline for making consumer banking services more accessible to persons with disabilities

Digital Accessibility

- Oct. '24
- Jan. '25
- April '25
- **June '25**
- Aug. '25 to Aug. '27
- Oct '25
- Oct. '25 to July '27
- Nov. '25
- Dec. '25
- Dec. '25
- July '26
- H2 '26 to Q1 '27
- July '27
- Dec. '27
- H2. '27

Regulation laying down harmonised rules on artificial intelligence (EU AI Act)

Impacts

The EU AI Act lays down harmonised rules on artificial intelligence.

It requires the classification of AI systems, for example:

- Unacceptable risk = prohibition (e.g., social scoring).
- High-risk = comprehensive requirements (e.g., remote biometric identification systems, credit assessment, HR).
- Interaction characteristics = transparency requirements (e.g., Robo advice).

It applies, among others, to deployers using the AI system, except in relation to personal use.

To the extent that an AI system processes personal data, the obligations (e.g. Art. 28 sub-processing terms) and principles (e.g. lawfulness, fairness and transparency) under the GDPR also need to be considered.

In relation to credit scoring, the GDPR rules on automated decision making (Art. 22 GDPR) must be considered. Provisions on high-risk AI systems (Annex II no. 5 lit. b AI Act) must also be considered.

The national picture

Italy: The Italian government presented (and is still working on) an Italian draft AI Bill, containing, among other things, tougher penalties for using AI in money laundering and financial crimes. The draft AI Bill has been analysed by the European Commission (opinion (C(2024) 7814)), which raised some issues on the interplay of the Italian draft AI Bill with the AI Act.

What to be thinking about

Financial entities will need to pay particular attention when using AI in the context of use cases that may fall within scope of the "high-risk AI systems" as defined in the AI Act, such as AI systems used for evaluating creditworthiness or establishing credit scores, risk assessment and pricing in the case of life and health insurance, recruitment, and use of biometrics.

Additionally, while the AI Act predominantly focusses on high-risk use cases, with supplementary rules for general purpose AI, it would be wrong to focus solely on these types of systems. Companies should generally evaluate the use of any AI within their company, such as the use of AI-powered chatbots for customer service as well as fraud detection tools, and compliance needs to be considered also from the perspective of the existing legal framework, with privacy, IP, consumer protection and anti-discrimination laws applying to a broader range of systems.

Equally, the rapid development of AI technologies and their use in every organisation underlines the need for robust governance structures in any company.

Key dates

Most provisions apply from 2 August 2026.

However, some key provisions apply earlier:

- Prohibited AI practices are banned outright from 2 February 2025.
- Obligations on providers and deployers regarding AI literacy apply from 2 February 2025.
- Penalties apply from 2 August 2025 (except penalties applicable to providers of general-purpose AI (GPAI) models which apply from 2 August 2026.
- Rules on GPAI models apply from 2 August 2025.

Rules on high-risk AI systems incorporated within products covered by certain product safety legislation apply from 2 August 2027.

There are also complex rules covering products already on the EU market when the AI Act entered into force on 1 August 2024 (although the rules do not apply to prohibited AI practices which, as mentioned above, are banned outright from 2 February 2025).

Our insights and tools

Hogan Lovells | AI Act Applicability and Compliance Tools

Hogan Lovells AI Hub

2024-2025 Global AI Trends Guide

The AI Investment Summit 2024

The EU AI Act: an impact analysis (part 1)

The EU AI Act: an impact analysis (part 2)

- Oct. '24
- Jan. '25
- April '25
- June '25
- **Aug. '25 to Aug. '27**
- Oct '25
- Oct. '25 to July '27
- Nov. '25
- Dec. '25
- Dec. '25
- July '26
- H2 '26 to Q1 '27
- July '27
- Dec. '27
- H2. '27

Digital euro

Impacts

The European Central Bank (ECB) is working with the national central banks of the euro area to explore the possible issuance of a digital euro. It would be a central bank digital currency, an electronic equivalent to cash, which would complement banknotes and coins, giving people an additional choice about how to pay. As a form of public money, it would be available free of charge to everyone in the euro area, for any digital payments.

The ECB's vision for the digital euro is that it would:

- be issued by the ECB;
- be used for digital payments;
- be universally accepted in the euro area;
- be free of charge;
- be available offline;
- be secure and private (the ECB would not be able to determine the identity or payment habits of people using digital euro);
- be guaranteed value (i.e. the digital euro would always be worth the same as a €1 coin); and
- "not be a crypto-asset" but rather would have immutable value and be backed by the ECB.

A key aspect is a high level of data protection and privacy. An offline functionality (payment without an internet connection after pre-funding the digital euro account) will have a standard that is close to that for cash transactions, i.e. personal transaction data is not shared with payment service providers (PSPs) or the Eurosystem. Online digital euro transaction details will only be accessible to the PSP to the extent necessary to comply with legal requirements, such as AML rules.

Other key points include that individuals' digital euro holdings will be subject to holding limits, and a digital euro rulebook for a single set of rules and standards is being developed by the Rulebook Development Group.

The national picture

Germany: Bundesbank survey from June 2024 shows digital euro is widely accepted in Germany. However, there are gaps in public's' knowledge about the new means of payment (e.g., some people believe it will replace cash payments). One of the concerns is privacy and data protection.

Ireland: The Central Bank of Ireland (CBI) delivered a keynote address outlining the importance of adopting the digital euro and sees the benefits of a retail digital payment solution that is available and accepted free of charge throughout Europe, both online and offline.

Italy: The Bank of Italy recently set up a working table on the digital euro project, inviting trade associations representing both payment service providers (PSPs) and users, as well as some representative banks and technology service providers, to present their concerns on the project and actively contribute to its discussion.

Spain: The Bank of Spain is actively monitoring the implementation of the digital euro in Spain. In fact, in late 2024 the Spanish banking supervisor's experts carried out a 'tentative' analysis to assess the impact that the new digital currency would have on the financing plans and liability structures of 65 entities doing business in Spain.

Belgium: The National Bank of Belgium is actively monitoring the implementation of the digital euro in Belgium. The National Bank is generally favorable to the digital euro, which it sees as a viable option to meeting central bank objectives and as an attractive payment instrument.

China's e-CNY v Digital euro: We have written an article that compares a number of key features of the digital yuan (e-CNY) distributed by the Chinese central bank the People's Bank of China (PBOC) with the proposed digital euro and as well as exploring the implications of the e-CNY's current and planned use cases. In particular, it includes a side-by-side comparison of technological infrastructure, distribution mechanisms, the regulatory framework, financial inclusion considerations, peer-to-peer transfers, international implications, and privacy and security. This last point highlights a notable area of difference between the PBOC and ECB approaches. In China, obtaining access to e-CNY requires using some form of ID that will allow the Chinese government to identify the user and PBOC's policy of "managed anonymity" means that in practice PBOC retains a record of all transactions that can be accessed by the distributing banks or other authorities in China

Digital euro cont.

Impacts

subject to certain safeguards and guard rails. While no doubt helpful for AML/CTF compliance purposes, commentators have pointed out that this does raise concerns about privacy. In contrast in the EU, the debate on the digital euro has centered around protection of personal data and privacy rights of users when transacting using the digital euro.

UK: In January 2025, the Bank of England (BoE) published a design note outlining its current thinking relating to the design of a digital pound for retail use and a progress update summarising its digital pound work in 2024. With the launch of a new Digital Pound Lab technology sandbox due in 2025, interested firms should be ready for more experimentation around potential use cases and business models for the proposed digital pound. It is important to note that the BoE's current proposal is for a retail CBDC, and that the design note does not apply to, or refer to, a digital pound for wholesale use (although the BoE is also exploring the wholesale aspect).

What to be thinking about

The ECB is exploring a broad range of use cases for the digital euro, including an ability for banks and other payment service providers to integrate the digital euro services as a new feature within their existing applications.

The digital euro is likely to enhance innovation in the payments industry at a pan-European level and there are potential opportunities, including public-private partnerships with the ECB and other national regulators.

Key dates

The project is currently in the Preparation phase – Part 1 (lasting until October 2025), during which the Eurosystem is focusing on technical features and tools for the digital euro.

Our insights and tools

Hogan Lovells | Digital Assets and Blockchain Hub

A Tale of Two CBDCs: e-CNY v. Digital Euro

Bank of England outlines path to digital pound

- Oct. '24
- Jan. '25
- April '25
- June '25
- Aug. '25 to Aug. '27
- **Oct '25**
- Oct. '25 to July '27
- Nov. '25
- Dec. '25
- Dec. '25
- July '26
- H2 '26 to Q1 '27
- July '27
- Dec. '27
- H2. '27

Regulation on instant credit transfers in euro (Instant Payments Regulation - IPR)

Impacts

The IPR amends the SEPA Regulation ((EU) 260/2012) to introduce uniform rules on instant credit transfers in euro in respect of both national and cross-border payments. All payment service providers (PSPs) that offer a credit transfer service must also offer an instant credit transfer service.

The IPR provides that an instant credit transfer must be executed within ten seconds, 24 hours a day and on any calendar day (which also includes holidays and Sundays).

PSPs are required to:

- comply with the AML/CFT rules to the same extent as for normal transactions;
- implement account-based sanctions screening for EU sanctions with many remaining practical and legal questions, e.g. concerning treatment of third countries;
- introduce IBAN-verification services (verification of payee) to mitigate the risk of authorised push payment (APP) fraud; and
- install proper fraud detection and prevention measures to avoid erroneous or fraudulent transactions.

Member states who do not have the euro as currency will also have to apply the rules if accounts already offer regular transactions in euros.

What to be thinking about

Significant investment in technological enhancements is required to ensure instant processing and settlement of credit transfers in euro.

In scope firms will need to ensure they can comply with the stringent security and anti-fraud requirements, including verification of payee.

Firms will also need to ensure they can screen customers against EU sanctions changes in real time and will need to consider how to perform non-EU sanctions screening, and other financial crime related screening and transaction monitoring within the permitted 10 seconds for completing the payment.

Cross-border operational aspects to consider include the fact that the UK and Switzerland, while SEPA members, are not subject to the IPR. This means that payments sent from UK accounts will not be subject to the 10 second rule under the IPR or the limitations on sanctions screening – potentially compromising consistency of service and financial crime controls across PSPs' European operations.

Key dates

The IPR entered into force on 8 April 2024.

There are phased implementation deadlines, modified for different components of the initiative and to allow for euro area and non-euro area member states.

For example:

- Eurozone based PSPs other than PIs/EMIs had until **9 January 2025** to implement a service for receiving instant credit transfers. They have until **9 October 2025** to implement a service for sending them, which is also the deadline for all eurozone based PSPs including PIs/EMIs to implement the verification of payee service;
- Eurozone based PIs/EMIs have until **9 April 2027** to implement services for receiving and sending instant credit transfers;
- Non-eurozone based PSPs other than PIs/EMIs have until **9 January 2027** to implement a service for receiving instant credit transfers. Broadly, they have until **9 July 2027** to implement a service for sending them, which is also the deadline for all non-eurozone based PSPs including PIs/EMIs to implement the verification of payee service; and
- Non-eurozone PIs/EMIs have until **9 April 2027** to implement a service for receiving instant credit transfers. They have until **9 July 2027** to implement a service for sending them.

Our insights and tools

The Payments Newsletter including Digital Assets & Blockchain, April 2024

The Instant Payment Regulation and EU restricted party screening

- Oct. '24
- Jan. '25
- April '25
- June '25
- Aug. '25 to Aug. '27
- Oct '25
- **Oct. '25 to July '27**
- Nov. '25
- Dec. '25
- Dec. '25
- July '26
- H2 '26 to Q1 '27
- July '27
- Dec. '27
- H2. '27

Directive on credit agreements for consumers (Second Consumer Credit Directive - CCD2)

Impacts

As well as some completely new requirements, CCD2 also introduces a number of technical changes which could have a potentially significant impact on the current consumer credit practices of firms who are already subject to national implementing measures under Directive 2008/48/EC (CCD1).

Among the other changes introduced by CCD2 is an expansion of the scope of the current consumer credit regime under CCD1. The aim is to increase transparency and improve consumer protection where certain credit products involve high costs or high fees for missed payments. 'Buy now, pay later' (BNPL) products involving third party BNPL providers are now caught within the expanded scope.

The national picture

Ireland: The Department of Finance conducted a consultation to obtain submissions on the transposition of CCD2. It posed a number of questions which set out the discretions contained in CCD2 and the Department invited comments on whether these discretions should be availed of, how they should be availed of and clear reasoning for such a position. Comments were also welcomed where the transposition will have an impact on certain other national legislation.

Italy: The Italian implementation of CCD2 recently started, with parliamentary work on a draft delegated law which mandates the Italian Government to implement the European directive in Italy.

Germany: The German legislator has not yet published a draft bill for transposing CCD2 requirements into national law.

Belgium: The Belgian legislator and regulators have not yet published a draft law nor any guidance in relation to CCD2.

What to be thinking about

Impact on buy now pay later (BNPL) lenders

Deferred payment schemes in which consumers are able to pay suppliers directly for goods or services in instalments and free of interest are outside the scope of CCD2. However, this narrower exemption has the effect of bringing many BNPL products that use third party BNPL providers within the regulatory perimeter for the first time.

Newly in-scope firms will have to get to grips with the detailed requirements of CCD2, including in relation to:

- licensing and supervision;
- advertising;
- pre-contractual information;
- creditworthiness assessments;
- form and content of the credit agreement; and
- various other ongoing information requirements.

CCD2 also introduces a number of new conduct of business obligations for creditors and credit intermediaries, as well as new provisions on arrears and forbearance.

This will involve a major regulatory compliance project. Affected firms may also want to consider the feasibility of adapting their current or planned business models to ensure they remain outside the regulatory perimeter.

- Oct. '24
- Jan. '25
- April '25
- June '25
- Aug. '25 to Aug. '27
- Oct '25
- Oct. '25 to July '27
- Nov. '25
- Dec. '25
- Dec. '25
- July '26
- H2 '26 to Q1 '27
- July '27
- Dec. '27
- H2. '27

Directive on credit agreements for consumers (Second Consumer Credit Directive - CCD2) cont.

What to be thinking about cont.

Impact on existing consumer credit providers

There are some completely new requirements that existing creditors and credit intermediaries need to be aware of in terms of potential impact on their current processes, including:

- There is a new requirement for non-discriminatory treatment of applicants for consumer loans. Creditors cannot differentiate on the basis of a consumer's nationality or place of residence. However, objectively justified reasons for different credit conditions remain possible.
- Restrictions on bundling consumer credit with insurance and other financial products are introduced.
- For consumers in financial difficulties, creditors will be required, where appropriate, to exercise reasonable forbearance before enforcement proceedings are initiated, including taking into account the consumer's individual circumstances.
- Creditors must have processes and policies for early detection of consumers in financial difficulties to facilitate referral to independent debt advisory services (which must be easily accessible to the consumer).
- There are a number of new conduct of business obligations for creditors and credit intermediaries.

However, the devil is also in the detail of CCD2, with a number of technical changes that could require significant lead times for necessary system and process updates. For example:

- While the information required for the prescribed form of pre-contractual information (Standard European Consumer Credit Information form – SECCI) is very similar to CCD1, a new layout means that significant systems changes are likely to be required.
- The CCD2 requirements for creditworthiness assessments are more detailed than under CCD1. Among the new provisions is a requirement for creditors to establish procedures for the creditworthiness assessment and to document and maintain those procedures as well as the information on the consumer's income and expenses and other financial and economic circumstances used to carry out the assessment. In addition, where the assessment involves the use of automated processing of personal data, consumers must be informed of their right to request and obtain human intervention from the creditor.

Those firms with UK businesses should note that the work to bring BNPL products within the UK regulatory perimeter continues. Updated proposals and a draft statutory instrument were published for consultation in October 2024. However, whilst BNPL regulation is clearly a priority for the government, realistically it's unlikely that BNPL products will be regulated until 2026 at the earliest. Under the UK proposals only BNPL agreements offered by third-party lenders will be regulated, meaning that the government has opted not to follow the EU position under CCD2 where third party BNPL lending is now caught within the expanded scope.

Regarding wider UK consumer credit reform, in July 2023 the UK government published its response to a first-stage consultation on the strategic approach to reforming the Consumer Credit Act 1974 (CCA), described in the response as 'an ambitious overhaul' of the regime. The previous government had been working on policy development to produce more detailed proposals. The aim was to publish a second stage consultation in 2024, but we are now awaiting next steps under the new government. For more on the consultation response, take a look at this article.

Key dates

National implementation deadline is 20 November 2025.

National implementing measures will have to be applied by 20 November 2026.

Our insights and tools

EU Second Consumer Credit Directive: Scope and impact for buy-now pay-later (BNPL) providers

EU Second Consumer Credit Directive: Impact for existing consumer credit providers

EU Second Consumer Credit Directive: changes ahead for credit providers

Buy-Now Pay-Later reform: UK government publishes updated proposals – now over to the FCA

UK Consumer Credit Act 1974: HM Treasury responds to first stage consultation on reform

Directive on financial services contracts concluded at a distance (Amended Consumer Rights Directive)

Impacts

Directive (EU) 2023/2673 amending Directive 2011/83/EU (Consumer Rights Directive) as regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC (Distance Marketing of Financial Services Directive).

Directive (EU) 2023/2673 is aiming at sharpening the focus on consumer protection and simplifying the existing legal framework by repealing the Distance Marketing of Financial Services Directive as of 19 June 2026 and including a new Chapter IIIa (Articles 16a-16e) on rules concerning financial services contracts into the Consumer Rights Directive.

The amended Consumer Rights Directive contains an amended scope and covers contracts between consumers and traders where the consumer pays a price or agrees to pay a price. Various articles of the Consumer Rights Directive are declared applicable to financial services concluded at a distance.

The new Chapter IIIa in particular includes the following rules:

- For distance contracts concluded by means of an online interface, firms shall ensure that the consumer can also withdraw from the contract by using a withdrawal function. The withdrawal function shall be labelled with the words "withdraw from contract here" or an unambiguous corresponding formulation in an easily legible way.
- Additional pre-contractual information obligation requirements, e.g. information on the consequences of late or missed payments; where applicable, that the price was personalised on the basis of automated decision-making.
- Providing adequate explanation that enables consumers to assess whether the proposed contract /ancillary services are adapted to their needs / financial situation.
- Additional protection regarding online interfaces for prevention of dark patterns.

The national picture

Germany: On 9 December 2024, the German legislator published a discussion draft on the new rules. According to the discussion draft, new rules will be included in/will amend current rules of the German Civil Code (*Bürgerliches Gesetzbuch*, BGB).

Ireland: No discussions have taken place by the Irish authorities on the transposition of this Directive into Irish law.

What to be thinking about

Firms need to build technical solutions in order to implement the online withdrawal button. Technical solutions must also observe exceptions to the withdrawal right.

New requirements in relation to the pre-contractual information obligation and adequate explanation prior to conclusion of contracts require a re-papering exercise.

Firms should assess whether online interfaces require adaptation in order to comply with additional protection requirements.

Key dates

Member States need to transpose rules into local law by 19 December 2025.

New rules will then apply from 19 June 2026.

Our insights and tools

EU distance marketing of financial services contracts: New Directive finalised

- Oct. '24
- Jan. '25
- April '25
- June '25
- Aug. '25 to Aug. '27
- Oct '25
- Oct. '25 to July '27
- Nov. '25
- **Dec. '25**
- Dec. '25
- July '26
- H2 '26 to Q1 '27
- July '27
- Dec. '27
- H2. '27

Regulation on information accompanying transfers of funds and certain crypto-assets (Funds Transfer Regulation - FTR)

Impacts

Legal change

The FTR, the EU's new payment transparency law, makes two key changes:

- The Legal Entity Identifier (LEI) or equivalent unique identifier is a new mandatory field for payments to and from corporate customers. Although in principle this requirement only bites if the payment service provider (PSP) has an LEI or equivalent for its corporate customer, it is noted that the EU's 5th Money Laundering Directive expects unique tax identifiers be obtained as part of customer due diligence.
- Equivalent payment transparency requirements to those already in place for wire transfers are extended to transfers of crypto-assets.

EBA Guidelines changes

Material changes have been made to the EBA Guidelines. The EBA Guidelines guide the enforcement approach of supervisory authorities and help firms to understand how the law is intended to apply. Material changes include:

- Detailed expectations for firms using the payer address to meet the mandatory information requirements.
- Requirements for risk-based decisions to be mapped against a list of risks set out in the Guidelines (in addition to any other risks identified by the firm).

UK and Swiss PSPs

Divergence may occur between the expectations of supervisory authorities in the UK and Switzerland and those in the EU.

What to be thinking about

Firms engaged in crypto transactions will need to consider how and when they are collecting, recording and updating relevant data points throughout the customer lifecycle.

PSPs should review their existing payment transparency control frameworks against the EBA Guidelines.

Non-EU PSPs should consider how to identify additional data contained within payment messages from the EU, and how to build this into financial crime control frameworks. Non-EU PSPs may also see a higher rejection rate for transactions that don't meet the EU's new requirements. As some EU PSPs may not be able to apply different controls to different payment sources.

Key dates

The original implementation deadline of 24 December 2024 was extended by the EBA to 24 December 2025.

- Oct. '24
- Jan. '25
- April '25
- June '25
- Aug. '25 to Aug. '27
- Oct '25
- Oct. '25 to July '27
- Nov. '25
- Dec. '25
- **Dec. '25**
- July '26
- H2 '26 to Q1 '27
- July '27
- Dec. '27
- H2. '27

Markets in Crypto-assets Regulation (MiCAR)

Impacts

The Markets in Crypto-assets Regulation (MiCAR) seeks to harmonise the regulatory framework for crypto-assets which are not otherwise regulated under existing financial services legislation across the EU.

It sets out provisions for those issuing and providing services relating to crypto-assets, including so-called "stablecoins"—MiCAR categorises these as asset-referenced tokens (ARTs) (i.e. crypto-assets which aim to stabilise their value by referencing another value or right, or combination thereof, including one or several official currencies) and e-money tokens (EMTs) (i.e. crypto-assets that aim to stabilise their value by referencing only one official currency).

For example, firms issuing (or otherwise making a public offering of) ARTs and EMTs will need to be appropriately authorised, and comply with the relevant requirements such as disclosing information via MiCAR-compliant whitepapers (including sustainability-related information).

MiCAR and PSD2

Potential issues arising from the overlap between MiCAR and PSD2 remain an open question. It is worth noting that in December 2024, John Berrigan of the European Commission wrote a letter to the EBA and ESMA highlighting the interplay between the two regimes (e.g. where transfers of EMTs by crypto-asset service providers may be considered as a payment service under PSD2 and therefore trigger a requirement for dual authorisation), and requesting a possible "no action letter" by the EBA in light of the ongoing revision of PSD2. In response, the EBA published a short letter agreeing with the Commission's concerns and stating that the EBA (in coordination with ESMA) will assess the matter and aim to publish a response by April 2025.

What to be thinking about

Impact on stablecoin issuers and related service providers

The requirements under MiCAR on the activities of issuing, offering to the public or seeking admission to trading of, ARTs and EMTs have been applicable since 30 June 2024. Firms seeking to issue or otherwise make an offering of ARTs and EMTs in the EU will need to ensure that they are MiCAR-compliant.

Additionally, crypto-asset service providers (CASPs) have since been expected to assess compliance with MiCAR of ARTs/EMTs for which they offer related services and to refrain from carrying out services that constitute offering to the public, seeking admission to trading or placing non-compliant ARTs/EMTs. More recently, ESMA has further clarified its expectations in a Statement on 17 January 2025, stating that CASPs such as those operating a trading platform are expected to stop making non-compliant ARTs and EMTs available for trading as soon as possible and by no later than Q1 2025. Accordingly, firms who have not already done so should set up procedures as soon as possible to assess the MiCAR compliance of stablecoins and other crypto-assets in relation to which they offer services, and to restrict services for such crypto-assets (e.g. by delisting tokens from the exchange platform).

Impact on crypto-asset service providers

More broadly, since 30 December 2024 (i.e. when all provisions of MiCAR became fully applicable) firms are not permitted to provide crypto-asset services within the EU without obtaining the appropriate MiCAR authorisation, unless they are able to avail of national transition regimes which typically requires such firms to already have been registered with the relevant Member State authority. (Note however that being able to offer services under national transition regimes does not mean that firms will be able to passport their services across the EU.) Importantly, firms should note that CASPs will face different transitional periods depending on the Member State(s) in which they are active.

Unregistered firms which cannot benefit from national transition regimes, but seek to provide crypto-asset services within the EU, will need to engage with national competent authorities (depending on the Member State) and obtain the appropriate authorisation as a CASP under MiCAR.

Key dates

Entered into force on 29 June 2023.

Provisions relating to issuance of ARTs and EMTs became applicable from 30 June 2024.

All other provisions became fully applicable on 30 December 2024.

National transition periods for CASPs are subject to the approach taken by each Member State; all transition periods should come to an end by 1 July 2026 (i.e. 18 months after MiCAR became fully applicable).

Our insights and tools

Implementation of MiCAR: A Jurisdictional Comparison

Italian Legislative Decree implementing MiCAR

Sustainability Disclosures under MiCAR

- Oct. '24
- Jan. '25
- April '25
- June '25
- Aug. '25 to Aug. '27
- Oct '25
- Oct. '25 to July '27
- Nov. '25
- Dec. '25
- Dec. '25
- **July '26**
- H2 '26 to Q1 '27
- July '27
- Dec. '27
- H2. '27

Proposed Directive on payment services and electronic money services (PSD3) and proposed Regulation on payment services in the EU (PSR)

Impacts

The legislative proposals for a Directive on payment services and electronic money services (PSD3) and a Regulation on payment services in the EU (PSR) encompass changes in a number of areas including:

Licensing

There are no proposed significant changes concerning the procedures of application for authorisation, control of shareholding and prudential requirements under PSD3; however:

- additional information is required to be submitted to address ICT, data sharing, passporting and wind-down arrangements;
- changes required to the way authorised payment institutions (APIs) and e-money institutions (EMIs) safeguard to mitigate concentration risk will need to be notified to the regulator; and
- EMIs will need to register their distributors (like APIs do agents).

Current APIs and EMIs will have two years to demonstrate compliance with the incoming prudential requirements.

Enhanced fraud prevention

Payment service providers (PSPs) will be required to provide a verification of payee service free of charge to customers that notifies the customer of any discrepancy, and the degree of such discrepancy, between a unique identifier and the payee name provided by the customer (verification of payee). The requirement will not apply to transactions where the payer did not input the unique identifier and the name of the payee themselves or to instant credit transfers under SEPA.

Impersonation fraud

The proposed PSR would introduce a new obligation on PSPs to refund a consumer within 10 business days where the consumer is tricked into authorising a payment by a fraudster impersonating the PSP. The European Parliament's proposed amendments go significantly further in extending this liability to payments that result from any other relevant entity of a public or private nature.

Strong Customer Authentication (SCA)

Proposed changes include that:

- account information service provider (AISP) access would be permitted for 180 days following the initial SCA without requiring further SCA to be performed (unless there are fraud concerns);
- SCA elements would no longer need to be from different categories (i.e., it could rely on two knowledge elements); and
- accessibility requirements would require PSPs to develop "a diversity of means" for the application of SCA to cater for the specific situations of all their customers. This requirement applies in addition to and independent of EAA requirements.

Open banking

Account servicing payment service providers (ASPSPs) would be required to provide at least one dedicated interface for third party provider (TPP) data access.

In the event the dedicated interface is unavailable, ASPSPs would have to offer an alternative interface without delay, with TPPs able to lobby regulators that they should have use of the customer interface if this takes too long.

Oct. '24
Jan. '25
April '25
June '25
Aug. '25 to Aug. '27
Oct '25
Oct. '25 to July '27
Nov. '25
Dec. '25
Dec. '25
July '26
H2 '26 to Q1 '27
July '27
Dec. '27
H2. '27

Proposed Directive on payment services and electronic money services (PSD3) and proposed Regulation on payment services in the EU (PSR) cont.

What to be thinking about

Our PSD3 Impacts Report summarises the impact of the PSD3 and PSR legislative proposals thematically, highlighting the areas where the EU trialogue process might shift the dial further before the texts are finalised, and flagging where changes might need to be reflected in PSPs' businesses.

For those in need of a very quick overview, the Report also includes an "at a glance" table mapping the changes, and a synopsis of the legislative process to date and expected timing.

Those firms with UK businesses should note that the recently published UK National Payments Vision sets out (among other things) the government's intention of replacing the prescriptive SCA requirements with regulatory rules by committing to revoke the SCA regulations in the Payment Services Regulations 2017 and allow the FCA to incorporate them into its rules – enabling a more flexible, outcomes-based approach to SCA. The FCA has also consulted on two-stage reforms to the UK safeguarding regime. It plans to publish final interim rules with an accompanying policy statement within the first six months of 2025.

Key dates

The PSD3 legislative process is ongoing. Subject to a number of factors within the legislative process which could cause delays, PSD3 may not come into effect until Q1 2027 (and the PSR could take effect in H2 2026).

However, affected firms should monitor the evolution of the PSD3 and PSR texts. We've already started working with firms to assist them in analysing changes they might need to make within their businesses in anticipation of the final position.

Our insights and tools

Hogan Lovells PSD3 Impacts Report: Getting ahead of the evolving EU payments regulatory landscape

PSD3: European Parliament adopts amended PSD3 and PSR texts at first reading

PSD3: European Parliament's ECON Committee adopts draft reports on PSR and PSD3

PSD3: Putting citizens at the heart of EU payments

Evolution not revolution: European Commission publishes financial data access and payments package

UK National Payments Vision: Key takeaways

Payments and e-money: UK FCA consults on two-stage reforms to safeguarding regime

- Oct. '24
- Jan. '25
- April '25
- June '25
- Aug. '25 to Aug. '27
- Oct '25
- Oct. '25 to July '27
- Nov. '25
- Dec. '25
- Dec. '25
- July '26
- **H2 '26 to Q1 '27**
- July '27
- Dec. '27
- H2. '27

6th AML package

Impacts

The 6th AML package replaces the 5th money laundering directive with a suite of new laws, the most significant of which are:

AML Regulation

The operational requirements for firms in respect of anti-money laundering and combatting terrorist financing are now set out in EU Regulations. This means the requirements will be directly applicable on an EU level and do not require transposition into member states' national laws. The aim is to harmonise the legal framework within the European Union and thus avoid discrepancies between member states. However, this approach affects the ability of member states to tailor the requirements to deliver pragmatic outcomes in the context of financial service delivery within their domestic markets.

AMLD6

The sixth Anti-Money Laundering Directive (AMLD6) sets out the infrastructure arrangements that members states, national supervisors and FIUs will need establish or adjust to meet the new requirements.

These will include requirements for verification of information on EU company and trust registers and the establishment of an overseas entities and trusts register.

AMLA

The new EU Anti-Money Laundering Authority (AMLA) will be based in Frankfurt am Main.

AMLA will have supervisory and sanctioning powers in relation to so-called "selected obliged entities". The relevant selected obliged entities will be determined based on a risk assessment of those credit institutions, financial institutions and groups of credit institutions and financial institutions that operate (through establishments or under the freedom to provide services) in at least six Member States (including the home Member State), regardless of whether the activities are carried out through infrastructure on the territory concerned or remotely. AMLA will also cooperate and coordinate with supervisory authorities and national Financial Intelligence Units (FIUs).

AMLA will issue guidance to support the understanding of the Regulations and the Directive by supervisory authorities and firms. Engagement with AMLA will be critical to ensuring that the practical challenges of implementing the Regulations or the Directive are understood by AMLA and addressed in AMLA's guidance.

80 Regulatory Technical Standards (RTS) are expected in relation to AMLA.

What to be thinking about

Firms should identify the practical challenges of implementing these legal changes within their EU operations. Firms can then use these to support their discussions with supervisory authorities and AMLA. Elements of the 6th AML package containing the most material changes include:

- The changes to when a business relationship is considered to commence.
- The changes to the test for beneficial ownership.
- The new requirements for sanctions evasion and circumvention risk assessments.
- The new prescribed enhanced due diligence requirements for high net worth individuals.

Firms should identify entities and trusts within their groups that are established outside the EU but fall within the new registration requirements. For entities established within the EU, firms should prepare for updating their existing register entries in company and trust registers to meet the new requirements.

Key dates

AML Regulation: The majority of the provisions will apply from 10 July 2027.

AMLD6: Must be transposed into national law by 10 July 2027.

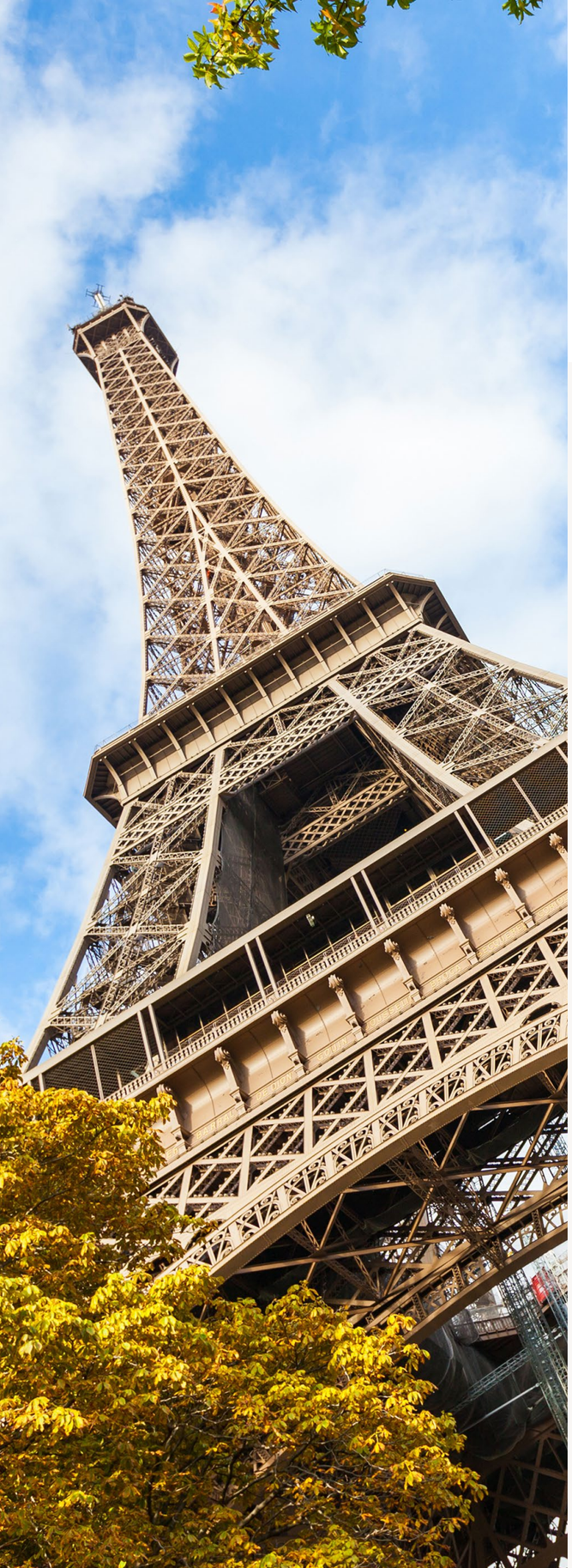
AMLA is expected to start issuing draft guidance in 2025, but won't be fully operational until 2028. See:

- About AMLA
- Questions and Answers: The new EU Anti-Money Laundering Authority (AMLA)

Our insights and tools

Football agents and professional football clubs subject to the new EU Anti-Money Laundering Regulation

Oct. '24
Jan. '25
April '25
June '25
Aug. '25 to Aug. '27
Oct '25
Oct. '25 to July '27
Nov. '25
Dec. '25
Dec. '25
July '26
H2 '26 to Q1 '27
July '27
Dec. '27
H2. '27



Regulation on establishing the European Digital Identity Framework (eIDAS 2.0)

Impacts

eIDAS 2.0 is legislation that builds on and amends the original eIDAS Regulation to address interoperability, enhance security, and promote the use of digital identities across the EU.

eIDAS 2.0 facilitates the introduction of European Digital Identity (EUDI) wallets, allowing citizens to store their identity and payment credentials securely on their smartphones or devices. This can improve the efficiency of payment processes, especially in the context of online payments, as customers can authenticate transactions using these digital wallets. The use of the EUDI wallets by consumers will be voluntary, but each Member State will be required to issue at least one EUDI wallet.

Where payment service providers or financial institutions that provide services are required by EU or national law to use strong user authentication for online identification or where strong user authentication for online identification is required by contractual obligation, the entities will be required to accept the EUDI wallets upon the voluntary request of a user (for instance, to authenticate payment transactions) by December 2027 (Art. 5f(2) of eIDAS 2.0).

What to be thinking about

Firms will need to assess the applicability of eIDAS 2.0, in particular their role and corresponding obligations under the Regulation.

Payment service providers or financial institutions will be required to establish an appropriate governance framework, and if they are qualified as a 'relying party' (where relying upon the EUDI wallet for the provision of services), they will need to register in the Member State where they are established.

Key dates

eIDAS 2.0 entered into force on 20 May 2024.

The European Commission adopted technical and operational specifications and reference standards of the EUDI wallets by means of implementing acts in December 2024.

As set out under "Impacts", relevant firms need to accept the EUDI wallets where required by EU or national law to use strong user authentication for online identification or where strong user authentication for online identification is required by contractual obligation by December 2027.

- Oct. '24
- Jan. '25
- April '25
- June '25
- Aug. '25 to Aug. '27
- Oct '25
- Oct. '25 to July '27
- Nov. '25
- Dec. '25
- Dec. '25
- July '26
- H2 '26 to Q1 '27
- July '27
- **Dec. '27**
- H2. '27

Proposed Regulation on a framework for Financial Data Access (FiDA)

Impacts

The proposed FiDA Regulation seeks to establish a framework to govern the access and use of consumer data in finance. The proposed Regulation would bring into scope an exhaustive set of data and lists firms that fall within the scope of the legislation. As the Commission's proposal for open finance, the scope covers a range of data from energy right the way through to savings.

The proposed Regulation would introduce a legal obligation on data holders to make available to customers the data that is within the scope of the Regulation. The customer would have the right to request that the data holder shares its data with the data user through a data sharing scheme. The proposed Regulation sets out the requirements for the creation and governance of financial data sharing schemes which brings together data holders and data users. It would require firms within the scheme to establish standards for data and technical interfaces. As part of this, there is also the requirement to have a financial data access permissions dashboard to ensure that customers can monitor their data permissions by being able to access an overview of their data permissions, grant new ones and withdraw permissions if necessary. Data holders would be entitled to reasonable compensation for making the data available to the data users. This would reflect the costs incurred for making available the technical interface.

What to be thinking about

FiDA looks to set out the European Commission's plan for open finance. In doing so it is quite a substantial proposal that will disrupt existing business models and open up this data to new market entrants and create new value chains. Whilst taking a slightly different approach, the disruption will be akin to that of the payments industry through PSD2. With data holders having to open up their data to data users, firms will need to consider where they position themselves and how they can capitalise on this. For example, a data holder may use this as an opportunity to be a data user as well and provide a range of new services.

There are some significant requirements under FiDA that clients will need to consider. First of all, how to establish a data sharing scheme. The proposal has left it to industry to determine what these schemes look like and whether it crosses industry. The Commission noted that the best use cases of Open Banking are not the ones envisaged whilst drafting the proposal and want to ensure that these schemes are market driven. As such, clients will need to consider where the opportunity is themselves. The schemes themselves will be complicated. Those within the scheme will need to develop standardised data and technical interfaces and put in place coordination mechanisms for the operation of a financial data access permission dashboard, which will require early coordination. In addition to this, there will also have to be joint standardised contractual frameworks to govern access to specific datasets as well as the rules on governance of these schemes, transparency requirements, compensation rules, liability, and dispute resolution.

Key dates

The European Parliament has voted through its text and the Council of the EU has adopted a General Approach. Trilogues have yet to commence. The proposal has caused quite some controversy and we expect quite lengthy trilogues, so timing on application of the proposed Regulation is currently uncertain but could be around H2 2027. One point of compromise could be extending the implementation period, which could see FiDA take effect after this date.

Our insights and tools

Fintech Fundamentals – PSD3
Webinar Series – The FiDA Proposal

- Oct. '24
- Jan. '25
- April '25
- June '25
- Aug. '25 to Aug. '27
- Oct '25
- Oct. '25 to July '27
- Nov. '25
- Dec. '25
- Dec. '25
- July '26
- H2 '26 to Q1 '27
- July '27
- Dec. '27
- H2. '27

Key dates

2023

Jan. | Feb. | March | April | May | June | July | Aug. | Sept. | Oct. | Nov. | Dec.

MiCAR ((EU) 2023/1114): entered into force on 29 June 2023.

2024

Jan. | Feb. | March | April | May | June | July | Aug. | Sept. | Oct. | Nov. | Dec.

Instant Payments Regulation ((EU) 2024/886): entered into force on 8 April 2024.

eIDAS 2.0 ((EU) 2024/1183): entered into force on 20 May 2024.

NIS2 Directive ((EU) 2022/2555): transposition deadline for EU member states was 17 October 2024; new regime applicable since 18 October 2024.

MiCAR ((EU) 2023/1114): all other provisions other than those relating to issuance of ARTs and EMTs applicable on 30 December 2024.

MiCAR ((EU) 2023/1114): provisions relating to issuance of ARTs and EMTs applicable from 30 June 2024.

eIDAS 2.0 ((EU) 2024/1183): European Commission adopted technical and operational specifications and reference standards of the EUDI wallets by means of implementing acts in December 2024.

2025

Jan. | Feb. | March | April | May | June | July | Aug. | Sept. | Oct. | Nov. | Dec.

Instant Payments Regulation ((EU) 2024/886): eurozone based PSPs other than PIs/EMIs had until 9 January 2025 to implement a service for receiving instant credit transfers.

DORA (Regulation (EU) 2022/2554): applicable since 17 January 2025.

Safeguarding in Germany: draft bill passed and new rules on safeguarding apply from 9 April 2025.

Instant Payments Regulation ((EU) 2024/886): eurozone based PSPs other than PIs/EMIs have until 9 October 2025 to implement a service for sending instant credit transfers. This is also the deadline for all eurozone based PSPs including PIs/EMIs to implement the verification of payee service.

European Accessibility Act ((EU) 2019/882): applicable from 28 June 2025.

Second Consumer Credit Directive ((EU) 2023/2225): national implementation deadline is 20 November 2025.

Funds Transfer Regulation ((EU) 2023/1113): implementation deadline is 24 December 2025.

EU AI Act ((EU) 2024/1689): prohibited AI practices banned outright and obligations on providers/deployers regarding AI literacy apply from 2 February 2025.

EU AI Act ((EU) 2024/1689): penalties apply from 2 August 2025 (except penalties applicable to providers of general-purpose AI (GPAI) models which apply from 2 August 2026). Rules on GPAI models apply from 2 August 2025.

Digital euro: project currently in Preparation Phase – Part 1, lasting until October 2025. During this phase the Eurosystem is focusing on technical features and tools for the digital euro.

Amended Consumer Rights Directive ((EU) 2023/2673): member states to transpose rules into local law by 19 December 2025.

Key dates

2026

MiCAR ((EU) 2023/1114): national transition periods for CASPs are subject to approach taken by each member state; all transition periods should come to an end by 1 July 2026 (i.e. 18 months after MiCAR became fully applicable).

Second Consumer Credit Directive ((EU) 2023/2225): national implementing measures to be applied by 20 November 2026.

Jan. | Feb. | March | April | May | June | July | Aug. | Sept. | Oct. | Nov. | Dec.

Amended Consumer Rights Directive ((EU) 2023/2673): new rules will apply from 19 June 2026.

EU AI Act ((EU) 2024/1689): most provisions apply from 2 August 2026, including penalties applicable to providers of general-purpose AI (GPAI) models (other penalties apply from 2 August 2025).

2027

PSD3/PSR: legislative process is ongoing. Subject to a number of factors within the legislative process which could cause delays, PSD3 may not come into effect until Q1 2027 (and the PSR could take effect in H2 2026).

Instant Payments Regulation - IPR ((EU) 2024/886): eurozone based PIs/EMIs have until 9 April 2027 to implement services for receiving and sending instant credit transfers. This is also the deadline for non-eurozone PIs/EMIs to implement a service for receiving instant credit transfers.

FiDA: timing on application of the proposed Regulation is currently uncertain but could be around H2 2027. One point of compromise could be extending the implementation period, which could see FiDA take effect after this date.

European Accessibility Act ((EU) 2019/882): applicable from 28 June 2025.

eIDAS 2.0 ((EU) 2024/1183): relevant firms need to accept the EUDI wallets where required by EU or national law to use strong user authentication for online identification or where strong user authentication for online identification is required by contractual obligation by December 2027.

Jan. | Feb. | March | April | May | June | July | Aug. | Sept. | Oct. | Nov. | Dec.

Instant Payments Regulation ((EU) 2024/886): non-eurozone based PSPs other than PIs/EMIs have until 9 January 2027 to implement a service for receiving instant credit transfers.

Instant Payments Regulation - IPR ((EU) 2024/886): broadly, non-eurozone based PSPs other than PIs/EMIs have until 9 July 2027 to implement a service for sending instant credit transfers. This is also the deadline for non-eurozone PIs/EMIs to implement a service for sending instant credit transfers, and for all non-eurozone based PSPs including PIs/EMIs to implement the verification of payee service.

EU AI Act ((EU) 2024/1689): rules on high-risk AI systems incorporated within products covered by certain product safety legislation apply from 2 August 2027.

2028

6th AML package (AMLA): while AMLA is expected to start issuing draft guidance in 2025, it won't be fully operational until 2028.

Contacts

Eimear O’Brien

Partner | Dublin
eimear.obrien@hoganlovells.com

Roger Tym

Partner | London
roger.tym@hoganlovells.com

Charles-Henri Bernard

Counsel | Brussels
charles-henri.bernard@hoganlovells.com

Sebastien Gros

Partner | Paris
sebastien.gros@hoganlovells.com

Franck Dupret

Counsel | Paris
franck.dupret@hoganlovells.com

Richard Reimer

Partner | Frankfurt
richard.reimer@hoganlovells.com

Sarah Wrage

Partner | Frankfurt
sarah.wrage@hoganlovells.com

Andreas Doser

Counsel | Frankfurt
andreas.doser@hoganlovells.com

Eoin O Connor

Partner | Dublin
eoin.oconnor@hoganlovells.com

Jeffrey Greenbaum

Partner | Rome
jeffrey.greenbaum@hoganlovells.com

Elisabetta Zeppieri

Counsel | Rome
elisabetta.zeppieri@hoganlovells.com

Pierre Reuter

Partner | Luxembourg
pierre.reuter@hoganlovells.com

Victor de Vlaam

Partner | Amsterdam
victor.devlaam@hoganlovells.com

Carlos Carbajo Amigo

Associate | Madrid
carlos.carbajoamigo@hoganlovells.com

James Black

Partner | London
james.black@hoganlovells.com

Louise Crawford

Partner | London
louise.crawford@hoganlovells.com

John Salmon

Partner | London
john.salmon@hoganlovells.com

Andrew McGinty

Partner | Hong Kong
andrew.mcginty@hoganlovells.com

Americas

- **Boston**
- **Denver**
- **Greater Washington, D.C.**
  - Baltimore
  - Washington, D.C. and Northern Virginia
- **Houston**
- **Los Angeles**
- **Miami**
- **Minneapolis**
- **New York**
- **Philadelphia**
- **Northern California**
  - San Francisco
  - Silicon Valley
- **Latin America**
  - Brazil
  - Mexico

Europe, Middle East and Africa

- **Amsterdam**
- **Brussels**
- **Dublin**
- **Germany**
  - Berlin
  - Düsseldorf
  - Frankfurt
  - Hamburg
  - Munich
- **London**
- **Luxembourg**
- **Madrid**
- **Milan**
- **Rome**
- **Paris**
- **Middle East**
  - Dubai
  - Riyadh

Asia Pacific

- **Greater China**
  - Beijing
  - Hong Kong
  - Shanghai
- **South East Asia**
  - Ho Chi Minh City
  - Jakarta
  - Singapore
- **Tokyo**

www.hoganlovells.com