

Prompt Attention: The Treatment of AI Assistants at Banks, Investment Firms and CASPs under EU Laws

A CahillNXT Article on the Regulatory Treatment of Client-Facing AI Chatbots under the AI Act, MiFID II, MiCA, PSD II, and DORA

October 27, 2026

EXECUTIVE SUMMARY

The days of long phone calls with ubiquitous hold music and nail-biting frustration when trying to get to the bottom of a declined card payment are seemingly coming to an end, with one considerable caveat: the human at the other end of the line may now be getting replaced by an AI assistant. The European Banking Authority (EBA) reported in September 2025 that more than half of the banks it surveyed were using general-purpose or agentic AI in processes facing consumers. Most of the securities firms using generative AI that responded to the survey of the European Securities and Markets Authority (ESMA) relied on commercial models, and few of the third-party AI providers named in the survey were actually established in the Union.¹

Typically, behind most client assistants (interchangeably also called “chatbots” here) sits a general-purpose AI model that the bank, investment firm or crypto-asset service provider (CASP) offering the assistant did not build. To avoid unwieldy switching between banks, investment firms and CASPs, the regulated institution offering the assistant is referred to as the “firm” in this article unless stated otherwise. Usually, a firm pays the company that trained the model for access, gives the model standing instructions and the firm’s own documents, and presents the result to clients under its own name. The EU’s AI Act² describes a general-purpose AI model as one capable of competently performing a wide range of distinct tasks and treats the company that trains such a model and places it on the market under its own name as its provider (which we will also call the “model provider”). Relying on a model provider in this way resembles engaging a capable generalist through an agency, briefing them on the firm’s products and seating them at the front desk. One of the main differences is that different laws

¹ Estimates vary by source and methodology. See EBA, “Rising application of AI in EU banking and payments sector” (factsheet, 25 September 2025) (“EBA factsheet”), reporting 55 percent of surveyed banks; ESMA, “AI adoption and trends in securities markets: EU evidence”, ESMA50-481369926-30599 (20 February 2026) (“ESMA Survey”), reporting that 81 percent of firms using generative AI relied on commercial models and that about 8 percent of the third-party providers named were domiciled in the Union.

² Regulation (EU) 2024/1689

apply, and the question becomes which EU rules attach to an assistant built on a third-party model and in what capacity the firm answers for it.

The answer would appear more palatable than the volume of recent legislation suggests. Under the AI Act, a firm that *builds* a chatbot on a general-purpose AI model and offers it under its own name is likely to be the *provider* of the chatbot as an AI system. A provider of such a chatbot has a short list of obligations, centered on informing clients they are interacting with an AI system and marking what the chatbot writes. The list of obligations does become considerably longer where the chatbot is put to a use that the Act treats as high-risk, such as assessing a client's creditworthiness. A firm that licenses a finished chatbot from a third party that offers it under its own name would appear to be only the chatbot's *deployer*, the AI Act's term for a person using an AI system under its authority, so the transparency obligations stay with the third party as the chatbot's provider. Whichever role the firm plays, the heavier obligations that the AI Act attaches to general-purpose AI models with systemic risk, which are the most capable models, would ordinarily stay with their model providers. On the other hand, the more demanding rules for an assistant that discusses investments or crypto-assets are the familiar ones in the Markets in Financial Instruments Directive (MiFID II) and the Markets in Crypto-Assets Regulation (MiCA), which regulate what is done for a client whoever, or whatever, does it. For instance, a common design issue arises where an assistant designed to explain products drifts, one answer at a time, into recommending them, which may result in the giving of advice that MiFID II or MiCA regulates.

The article first describes how firms are using client assistants and which EU rules apply to them, and then considers the AI Act, followed by MiFID II and MiCA and by the Payment Services Directive (PSD II) for assistants that deal with payments and agents that effect them. The later sections deal with the firm's contract with the model provider, the client's right to speak to a human and the firm's liability for a wrong answer. Much of the guidance is recent or still in draft, so the conclusions are qualified throughout.³

1. HOW ARE BANKS, INVESTMENT FIRMS AND CASPS USING AI CHATBOTS?

The assistants in use range from the narrow to the open-ended. At the narrow end, a support assistant can answer questions about fees, cards, transfers and withdrawals, retrieve the client's balance or transaction history, and hand the conversation to a member of staff when it is unable to resolve a query. Support assistants feature prominently among the uses of AI that the EBA, in its factsheet on AI in banking, and ESMA, in its statement on AI in investment services, describe as already adopted or being explored. Further along the range, an assistant may explain products, statements and market movements by reference to the client's own holdings, and may comment on the client's portfolio, for instance on its concentration in a single asset. Assistants that turn an instruction given in ordinary language into an order, such as "sell half my position" or "convert 500 euros into a stablecoin", appear to be becoming more commonplace. At the more open-ended and advanced end of the range, agents, which take several steps toward a goal the client sets within limits fixed by the client or the firm, appear to be emerging as well. The

³ See European Commission, Guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of Regulation (EU) 2024/1689 (AI Act), C(2026) 5054 final (20 July 2026) ("Article 50 Guidelines"); European Commission, Draft guidelines on the classification of high-risk AI systems (19 May 2026) ("draft classification guidelines"); ESMA, Public Statement on the use of Artificial Intelligence (AI) in the provision of retail investment services, ESMA35-335435667-5924 (30 May 2024) ("ESMA AI Statement"), which describes itself as initial guidance (paragraph 26).

EBA's figure covers general-purpose and agentic AI together, however, and official sources do not yet describe order-taking assistants or agents as common practice in the Union.⁴

Most client assistants share a common design, in which each client message is sent to the model provider's servers through an application programming interface (API), the channel the firm's software uses to send requests to the model. Every message travels with the firm's standing instructions to the model, which are known as the "system prompt", together with passages retrieved from the firm's documents and, where the assistant can act, a description of the functions it may call, such as a balance lookup or an order ticket. The model's answer comes back to the firm's software, which can filter it before the client sees it and decides whether to run any action the model proposes. The firm therefore controls what the model is told, what data it sees, what it may do and what is shown to the client, while the model provider controls the model itself and can change or retire it.

The regulatory treatment of a deployment would appear to depend on:

- i) who built the assistant and under whose name it is offered;
- ii) whether its answers draw on the client's circumstances;
- iii) whether it can act on the client's account;
- iv) whether its users include consumers; and
- v) where client data goes when the firm sends it to the model provider.

A single support assistant built by the firm, serving consumers and sending their account data to a model provider outside the Union, may therefore still be subject to several sets of EU rules at once, even where it does not discuss investments at all.

2. WHICH EU RULES APPLY TO A CLIENT CHATBOT?

The AI Act **governs the assistant as a technology** and allocates its obligations according to the role the firm plays, so the question under it is whether the assistant is the firm's own, built by the firm or for it, or one that a third party offers under its own name. MiFID II and MiCA **govern what the assistant does for the client**, and since both are technology-neutral they apply to advice or an order given through a chatbot as they apply to advice or an order given by a human member of staff. PSD II **governs what a payment service provider's assistant tells clients about payments** and the **conditions on which any firm's agent may make payments from a client's account**. Moreover, the Digital Operational Resilience Act (DORA) governs the firm's arrangement with the model provider, since access to a general-purpose AI model through an API would appear to be an information and communication technology (ICT) service.

The outsourcing rules of MiFID II and MiCA apply alongside DORA where model access amounts to outsourcing. The Consumer Rights Directive, as amended in 2023 for financial services contracts concluded at a distance, requires Member States to give consumers a right to human intervention where a trader uses online tools, subject to the rules on adequate explanations in other Union acts. Last but not least, the General Data Protection Regulation (GDPR) governs the client data the firm sends to the model provider and gives clients rights in relation to automated decisions.⁵

⁴ ESMA AI Statement (n 2), paragraph 3(a); EBA factsheet (n 1); ESMA Survey (n 1).

⁵ Regulation (EU) 2024/1689 (OJ L, 2024/1689, 12.7.2024), as amended by Regulation (EU) 2026/1744 (OJ L, 2026/1744, 24.7.2026) (the "Digital Omnibus on AI") (the "AI Act"); Directive 2014/65/EU (OJ L 173, 12.6.2014, p. 349) ("MiFID II") and Commission Delegated Regulation (EU) 2017/565 (OJ L 87, 31.3.2017, p. 1) ("Delegated Regulation 2017/565"); Regulation (EU) 2023/1114 (OJ L 150, 9.6.2023, p. 40) ("MiCA"), recital 9; ESMA AI Statement (n 2), paragraphs 2 and 7; Regulation (EU) 2022/2554 (OJ L 333, 27.12.2022, p. 1) ("DORA"); Directive (EU) 2015/2366 (OJ L 337, 23.12.2015, p. 35) ("PSD II"); Directive 2008/48/EC (OJ L

Perhaps interestingly, the Digital Services Act (DSA) would not appear to apply to most of what a firm's chatbot does. The DSA regulates intermediary services, which transmit, cache or host information provided by the recipients of the service, while a chatbot answering the firm's clients tends to generate the firm's content. The Commission's designation of a consumer chatbot service under the DSA, made in August 2026, treated that service as a very large online search engine because it can search the web, and does not address a regulated firm that calls a model through an API to answer its clients.⁶

3. WHAT DOES THE AI ACT ASK OF A FIRM WHOSE CHATBOT RUNS ON A GENERAL-PURPOSE AI MODEL?

The AI Act is an EU regulation adopted in 2024 that sets rules for AI across all sectors of the economy and applies directly in every Member State. It regulates AI according to the risk it presents, prohibiting a limited set of practices outright and imposing its most extensive requirements on high-risk AI systems, such as those used to assess a person's creditworthiness. AI systems that interact with people or generate content are also subject to transparency obligations, and providers of general-purpose AI models have obligations of their own, which are heavier for the most capable models. Providers established outside the Union are also within the Act's scope where they place AI systems or general-purpose AI models on the EU market, as are providers and deployers outside the Union where the output of their AI systems is used in the Union. A US company that offers its model to firms in the Union would therefore appear to be subject to the Act as the model's provider.

Following the Act's entry into force on 1 August 2024, its provisions have applied in stages, with most of the prohibitions applying since 2 February 2025 and the obligations on providers of general-purpose AI models since 2 August 2025. Most other provisions, including the transparency obligations, have applied since 2 August 2026, while the rules on high-risk AI systems are due to apply from 2 December 2027 or 2 August 2028, depending on the category of system.⁷

ROLES AND CLASSIFICATION UNDER THE AI ACT

An AI model and an AI system are distinct concepts under the AI Act, since a model needs further components, "such as for example a user interface", to become a system. The relationship resembles that between an engine and a car, with the model provider building the engine and the firm that adds the body, the controls and its own badge building the car. Obligations under the Act attach to the role a person plays in relation to an AI system or model, so the Act regulates the technology through obligations on the persons who develop and use it. The Act treats as a "provider" whoever develops an AI system or a general-purpose AI model, or has one developed, and places it on the market or puts the system into service under its own name or trademark. Placing on the market means making a system or model available on the Union market for the first time, while a system is put into service when it is supplied for first use directly to a deployer or for the provider's own use. The Act's recitals count offering a model through an API, the channel a firm's chatbot usually uses, among the ways of placing it on the market, so a firm connecting to the model through the API would not appear to become the model's provider. A firm that builds a client chatbot on the model and puts it into service in its own channels under its own name would appear to be the provider of the chatbot as an AI system and, since it also uses the chatbot itself, its deployer as well. The Act calls a

133, 22.5.2008, p. 66) and Directive (EU) 2023/2225 (OJ L, 2023/2225, 30.10.2023) (the "new Consumer Credit Directive"); Directive 2014/17/EU (OJ L 60, 28.2.2014, p. 34) (the "Mortgage Credit Directive"); Directive 2005/29/EC (OJ L 149, 11.6.2005, p. 22) (the "Unfair Commercial Practices Directive"); Directive (EU) 2024/2853 (OJ L, 2024/2853, 18.11.2024) (the "Product Liability Directive"); Directive 2011/83/EU (OJ L 304, 22.11.2011, p. 64), as amended by Directive (EU) 2023/2673 (OJ L, 2023/2673, 28.11.2023) (the "Consumer Rights Directive"), Article 16d(3) and (5); Regulation (EU) 2016/679 (OJ L 119, 4.5.2016, p. 1) ("GDPR"), Article 22.

⁶ Regulation (EU) 2022/2065 (OJ L 277, 27.10.2022, p. 1), Article 3(g) and recital 29; European Commission, press release IP/26/1772 (31 August 2026).

⁷ AI Act (n 4), Articles 2(1)(a) and (c), 5, 6, 50, 53, 55 and 113 and Annex III, point 5(b).

provider of an AI system that integrates an AI model, including one supplied by another under a contract, a “downstream provider”.⁸

Chatbots built by third parties are harder to classify than those the firm builds itself, since the firm may stand in either role depending on who specified the chatbot and whose name it is offered under. Licensing a finished chatbot from a third party that offers it under its own name and using it unmodified would appear to make the firm a deployer only, so the obligation to inform clients that they are interacting with an AI system falls on the third party as the chatbot’s provider. The firm’s own obligations under the Act would then be largely limited to supporting the AI literacy of its staff and avoiding the prohibited AI practices, which bind deployers as well as providers. The firm may, however, be the provider of a chatbot built by a third party to the firm’s specification and presented as the firm’s own, since the Act treats as a provider a person that “has an AI system ... developed” and puts it into service “under its own name or trademark”. Merely putting the firm’s own name on a third party’s off-the-shelf chatbot is a less certain case, since the Act’s rule that rebranding a system makes a person its provider is written for high-risk AI systems.⁹

Many client chatbots are likely to be built on the most capable models, which the AI Act classifies as general-purpose AI models with systemic risk. The obligations attached to the systemic-risk classification, such as model evaluation, adversarial testing and serious incident reporting, would ordinarily remain with the model provider unless the firm’s own work on the model makes the firm the provider of a modified model. System prompts, retrieval from the firm’s documents and the use of tools typically leave the model itself unchanged, much as a firm that configures licensed trading or banking software with its own products, fees and limits leaves the software supplier’s code untouched. Prompts, retrieval and tools are also the kind of further components that turn a model into a system, so on the better reading they leave the firm a downstream provider of an AI system, although the Commission’s guidelines do not address prompts, retrieval or tools as such. Fine-tuning would appear to make the firm the provider of the modified model only where it significantly changes the model’s generality, capabilities or systemic risk. The Commission’s indicative test for a significant change looks at the computation the modification uses, and fine-tuning one of the most capable models would not ordinarily approach its threshold. A firm that fine-tunes a smaller open-weight model could still, however, meet the threshold, since it is measured against the computation used to train the *original* model, and would then need to consider whether it has itself become the provider of a general-purpose AI model, with obligations limited to its modification.¹⁰

INFORMING CLIENTS THAT THEY ARE INTERACTING WITH AN AI SYSTEM

The primary obligation that applies to every client chatbot of which the firm is the provider, and has applied since 2 August 2026, is the transparency obligation in Article 50(1) of the AI Act. Clients must be informed that they are interacting with an AI system unless this is obvious to a reasonably well-informed, observant and circumspect person. The information has to be given in a “clear and distinguishable manner” by the time of the first interaction and in a form that meets the applicable accessibility requirements. The Commission’s guidelines on Article 50 list chatbots in helpdesks among the cases to which the exception for obvious cases does not apply, and treat a disclosure solely placed in terms and conditions, or a generic reference to an “assistant”, as insufficient on its own.¹¹ The Commission also considers periodic reminders likely to be necessary in contexts such as financial advice, insurance and complaints handling, and expects disclosure for the specific replies that are AI-generated where a

⁸ AI Act (n 4), Article 3(3), (4), (9), (11), (63) and (68) and recital 97; Article 50 Guidelines (n 2), paragraphs 11 and 15; European Commission, Guidelines on the scope of the obligations for general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act), C(2025) 5045 final (18 July 2025) (“GPAI Guidelines”), paragraphs 53 and 57.

⁹ AI Act (n 4), Articles 3(3) and (4), 4(1), 5(1), 25(1)(a) and 50(1); Article 50 Guidelines (n 2), paragraph 11.

¹⁰ AI Act (n 4), Articles 51 and 55, Annex XIII and recital 97. Under Article 51(2), a model is presumed to have high-impact capabilities, and so to be classified as a model with systemic risk under Article 51(1)(a), where the cumulative amount of computation used for its training, measured in floating-point operations, is greater than 10^{25} , and under Article 51(1)(b) the Commission may designate a model with equivalent capabilities or impact. GPAI Guidelines (n 7), paragraphs 60 to 71, under which the indicative test for a significant modification is whether it uses more than a third of the computation used to train the original model.

¹¹ AI Act (n 4), Articles 50(1) and (5) and 113; Article 50 Guidelines (n 2), paragraphs 38 and 45.

conversation passes between the assistant and a member of staff, other than replies that a member of staff has properly reviewed and sent.¹²

MARKING AI-GENERATED TEXT

Article 50 also requires providers of AI systems that generate synthetic text to ensure that the output is marked in a machine-readable format and detectable as artificially generated, through technical solutions that are “effective, interoperable, robust and reliable” as far as technically feasible. The Commission’s guidelines on Article 50 exclude output that merely reproduces existing content, which would appear to cover the firm’s pre-approved wording returned word for word. The guidelines list logging and fingerprinting among the marking techniques, under which the provider keeps a record of the text the system has produced, or a compact digital signature of it, so that a piece of text can later be checked against the record. The provider is also expected to make a means of detection available to the people who receive the content, and may rely on a marking solution offered by the model provider while remaining responsible for compliance. Logging would appear to be the most workable of the listed techniques for a text chatbot; a firm could build it on the conversation records it is obliged to keep under MiFID II or MiCA, extended to every reply the chatbot gives.¹³

Under the Digital Omnibus on AI, the regulation that amended the AI Act in July 2026, providers of AI systems that generate synthetic content and were placed on the market before 2 August 2026 have until 2 December 2026 to comply with the marking obligation. The Commission describes this extension as available “only for AI systems placed on the market before 2 August 2026”, so a firm’s chatbot would benefit from it only if the chatbot was placed on the market. A firm that builds a chatbot for its own channels would appear to put it into service for its own use, since its clients use the firm’s service without acquiring the system. The chatbot would therefore appear to fall outside the Digital Omnibus on AI extension and already be subject to the marking obligation even where the firm launched it before 2 August 2026.¹⁴

AI LITERACY AND PROHIBITED AI PRACTICES

The AI Act also requires providers and deployers to take measures to support the development of AI literacy among their staff, and the prohibited AI practices listed in Article 5 apply to client chatbots as to any other AI system. The prohibitions include the use of purposefully manipulative or deceptive techniques with the objective, or the effect, of materially distorting a person’s behavior by appreciably impairing the ability to make an informed decision. Article 5 also prohibits the exploitation of vulnerabilities due to age, disability or a specific social or economic situation, and both prohibitions apply where significant harm is reasonably likely. The Commission counts financial loss among the relevant harms and accepts that intent may be unnecessary where a system capable of distorting behavior in a significantly harmful way is deployed without preventive measures.

An assistant that uses false urgency, or pressure tailored to a client’s known vulnerabilities such as over-indebtedness, to prompt transactions reasonably likely to cause the client significant harm could therefore fall within Article 5, breaches of which may attract fines of up to €35 million or 7 percent of worldwide annual turnover. The false urgency need not have been designed by the firm, since a model may adopt urgent or persuasive language of its own accord, so it is thought that testing for such language before launch would be among the preventive measures the Commission has in mind. Lawful commercial practices are not prohibited

¹² Article 50 Guidelines (n 2), paragraphs 30 and 40.

¹³ AI Act (n 4), Article 50(2); Article 50 Guidelines (n 2), paragraphs 65, 73 to 75, 80 and 81.

¹⁴ AI Act (n 4), Articles 3(9) to (11) and 111(4); Article 50 Guidelines (n 2), paragraph 11; European Commission, “Transparency obligations under Article 50 of the AI Act” (FAQs, last updated 24 July 2026).

manipulation in themselves, and most persuasive design is more likely to be measured against the Unfair Commercial Practices Directive and the conduct rules of MiFID II and MiCA than against Article 5 of the AI Act.¹⁵

HIGH-RISK USES

High-risk status arguably seldom attaches to a firm's client chatbot. The financial uses that the AI Act classifies as high-risk are the evaluation of the creditworthiness of natural persons or their credit scoring, other than to detect fraud, and risk assessment and pricing in life and health insurance. A provider may treat an AI system listed in Annex III as not being high-risk where the system does not pose a significant risk of harm, for instance because it performs only a narrow procedural task. On the other hand, an AI system listed in Annex III "shall always be considered to be high-risk" where it profiles natural persons, as an assistant assessing a client's creditworthiness from the client's own data would appear to do (which is one of the specifically listed high-risk activities in Annex III). Beyond the financial uses listed in Annex III, a voice assistant that infers a caller's emotions from the voice would also appear to be high-risk as an emotion recognition system, although inferring emotions from the content of typed text would appear to fall outside the emotion recognition category.¹⁶

A firm that extends its own chatbot, or one supplied by a third party, to assess creditworthiness would appear to become the provider of a high-risk AI system, with the provider obligations applying from 2 December 2027. The AI Act lightens part of the regulatory obligations for financial institutions, since a financial institution that complies with the internal governance rules of financial services law is deemed to meet most of the Act's requirements for a quality management system and, as deployer, its obligation to monitor the system. Financial institutions in this sense would appear to include banks and investment firms and may also include CASPs, which MiCA subjects to governance requirements.

The AI Act's other requirements for high-risk AI systems apply in full, including those on data governance, technical documentation, transparency, human oversight and accuracy, together with the conformity assessment before the system is placed on the market or put into service and its registration in the EU database. As deployer, a firm using a high-risk AI system to assess creditworthiness would also need to perform a fundamental rights impact assessment before first use. The firm's contract with the model provider or, for a chatbot supplied by a third party, with that supplier would then need to secure the information and access the firm needs in order to comply, which a model provider whose acceptable use policy excludes creditworthiness assessment may decline to give.¹⁷

INFORMATION FROM THE MODEL PROVIDER AND ENFORCEMENT

The AI Act requires the model provider to make available to the firm, as a downstream provider, information and documentation on matters such as the tasks the model is intended to perform, its acceptable use policies and the format of its inputs and outputs. The information and documentation are meant to let the firm understand the model's capabilities and limitations, although they may still fall short of what the firm needs to show its competent authority, meaning the authority that supervises it under MiFID II, MiCA or banking law, how the chatbot behaves. Any shortfall would then need to be made up through the firm's own testing of the chatbot and through information rights negotiated in its contract with the model provider.¹⁸

Enforcement of the AI Act would appear to rest with the market surveillance authority, the body each Member State designates to supervise AI systems on its market, and the Act contemplates that for regulated financial institutions this may be the firm's competent authority, as Germany has provided by designating the Federal

¹⁵ AI Act (n 4), Articles 4(1), 5(1)(a) and (b) and 99(3) and recital 29; European Commission, Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 5052 final (29 July 2025), paragraphs 78 to 84, 89 and 109; Unfair Commercial Practices Directive (n 4).

¹⁶ AI Act (n 4), Articles 3(39) and 6(3) and Annex III, points 1(c), 5(b) and 5(c); draft classification guidelines (n 2), paragraphs 123, 124 and 171 to 177.

¹⁷ AI Act (n 4), Articles 8 to 16, 17(4), 25(1)(c), (2) and (4), 26(5), 27(1), 43, 49(1) and 113 and recital 158; MiCA (n 4), Article 68.

¹⁸ AI Act (n 4), Article 53(1)(b) and Annex XII.

Financial Supervisory Authority (BaFin). Each Member State lays down the penalties for breaches of the AI Act, and fines for breaches of its transparency obligations can be as much as €15 million or 3 percent of worldwide annual turnover, whichever is higher.¹⁹

4. WHAT DO MIFID II AND MICA ASK OF A FIRM WHOSE CHATBOT DEALS WITH INVESTMENTS OR CRYPTO-ASSETS?

MiFID II and MiCA would appear to apply to an assistant according to the service the assistant performs for the client, such as advice or the reception and transmission of orders. For investment and crypto-asset services, MiFID II and MiCA run in parallel, with the classification of the asset deciding which of them applies, since MiCA does not apply to crypto-assets that qualify as financial instruments under MiFID II. A bank or an investment firm may also provide crypto-asset services without authorization as a CASP, after notifying the competent authority of its home Member State, although an investment firm may provide only the crypto-asset services equivalent to its authorized investment services and activities. MiCA's conduct rules then apply accordingly to the crypto-asset service whichever kind of institution provides it.²⁰

An assistant that deals only with a bank's payment, card and lending services would appear to fall outside MiFID II and MiCA, since a bank falls within MiFID II only where it provides investment services or performs investment activities, or sells or advises clients on structured deposits.²¹

WHEN AN ASSISTANT'S ANSWERS MAY BECOME ADVICE

Advice is the service a firm may be most likely to provide unintentionally through an assistant. MiFID II treats a recommendation as investment advice where it is made to a person as an investor or potential investor and is presented as suitable for that person or based on the person's circumstances. The recommendation should concern buying, selling, holding or another listed step in respect of a particular financial instrument, and is excluded where it is issued exclusively to the public. ESMA's briefing on the definition of advice reads its references to an adviser as including an automated system used as a client-facing tool, and accepts that a recommendation may be implicit, as where a firm lets its information become subjective so that it steers the client to one product over others.²²

An assistant that retrieves the client's holdings or account data and draws on them in its reply would appear to consider the client's circumstances on the facts, and ESMA also treats a recommendation as based on those circumstances where the client can reasonably expect information the firm holds to be used. ESMA considers that a recommendation addressed to a particular person by email or private message does not benefit from the exception for recommendations issued to the public, so a reply generated for one client in a private conversation is unlikely to fall within that exception. The reply could therefore be treated as investment advice where the other conditions are met.²³ A firm that is only authorized for the reception and transmission of orders and their execution on behalf of clients would then appear to be providing advice outside its authorization.²⁴

MiCA casts its net wider, since its definition of advice extends beyond recommendations on transactions in crypto-assets to personalized recommendations on "the use of crypto-asset services". ESMA has stated that the scope of

¹⁹ AI Act (n 4), Articles 70(1), 74(6) and 99(1) and (4)(g) and recital 158; KI-Marktüberwachungs-und-Innovationsförderungs-Gesetz of 22 July 2026 (BGBl. 2026 I Nr. 223), § 2(3).

²⁰ MiCA (n 4), Articles 2(4)(a), 3(1)(15), 59(1)(b) and 60(1), (3) and (10).

²¹ MiFID II (n 4), Article 1(3) and (4).

²² MiFID II (n 4), Article 4(1)(4); Delegated Regulation 2017/565 (n 4), Article 9; Case C-604/11, *Genil* 48, judgment of 30 May 2013, EU:C:2013:344, paragraphs 52 to 55; ESMA, Supervisory briefing on understanding the definition of advice under MiFID II, ESMA35-43-3861 (11 July 2023) ("Advice Briefing"), paragraphs 24 and 29.

²³ Advice Briefing (n 21), paragraphs 69 to 74 and 79.

²⁴ MiFID II (n 4), Article 6(1).

advice under MiCA should be regarded as broader than under MiFID II because of the reference to crypto-asset services, and the tests it lists do not require the recommendation to concern a particular instrument;²⁵ moreover, MiCA does not repeat MiFID II's exclusion of generic advice about a type of instrument. For instance, a personalized suggestion that a client move part of its savings into stablecoins, without naming a stablecoin, may constitute advice on crypto-assets, although the point remains open to debate. A CASP authorized only for custody and administration of crypto-assets and their exchange for funds may likewise be advising without the necessary authorization where its assistant recommends another of the CASP's services by reference to the client's holdings.²⁶

The dividing line runs between information and recommendation, much as a shop assistant explaining how electric and stovetop kettles differ provides information, while one telling a customer which kettle suits the customer's kitchen is giving a recommendation (you may treat this as a cue to brew a cup of tea as we are halfway through). ESMA describes information as statements of fact or figures without comment, value judgment or suggestion on their relevance to a decision, which would appear to cover:

- i) explaining a product's terms, costs and risks;
- ii) comparing types of instrument without comparing specific products;
- iii) retrieving prices; and
- iv) reporting the client's holdings as facts.

Observations on a client's portfolio, such as its concentration in one asset, are harder to place, since they are value judgments on the client's own position and may be taken as implicit recommendations to sell or to hold. A generative model can move from information to recommendation within a single reply, often depending on how the client frames the question.²⁷

For a firm that does not intend to advise, the controls should therefore sit in the assistant's design, since ESMA considers that describing a service as non-advised in the firm's documentation is not sufficient on its own. A system prompt that confines the model to factual answers works like a standing instruction to staff, which shapes behavior without stopping a persistent client from coaxing out an opinion. The firm's competent authority would be likely to expect the firm to test the assistant before launch with questions designed to draw out recommendations and to have its compliance function review samples of conversations. The firm would also be expected to screen the assistant's replies for suggestions to buy, sell or hold a particular instrument by reference to the client and, for crypto-asset services, for personalized suggestions about types of crypto-asset or the use of crypto-asset services.²⁸

SUITABILITY ASSESSMENT OBLIGATIONS WHERE A FIRM ADVISES

For a firm authorized to advise, a recommendation its assistant makes can call for a suitability assessment, which under both MiFID II and MiCA tests whether the recommendation suits the client's knowledge and experience, financial situation and objectives. The firm may not recommend where it lacks the information the assessment requires, and remains fully responsible for the assessment where it is made through an automated system. ESMA's suitability guidelines expect a firm advising through an automated tool to tell clients the degree of human involvement and "if and how" they can ask for human interaction.²⁹ The guidelines also expect the firm to

²⁵ MiCA (n 4), Article 3(1)(24); ESMA, Questions and Answers on MiCA ("MiCA Q&A"), Q&A 2882 (18 June 2026).

²⁶ MiCA (n 4), Article 59(1) and (6); Delegated Regulation 2017/565 (n 4), recital 15.

²⁷ Advice Briefing (n 21), paragraphs 28 to 38, 61 and 62.

²⁸ Advice Briefing (n 21), paragraphs 19 and 20; ESMA AI Statement (n 2), paragraphs 16 and 21.

²⁹ MiFID II (n 4), Article 25(2); Delegated Regulation 2017/565 (n 4), Article 54(1) and (8); MiCA (n 4), Article 81(1), (8) and (11); ESMA, Guidelines on certain aspects of the MiFID II suitability requirements, ESMA35-43-3172 (23 September 2022) ("MiFID II Suitability Guidelines"), paragraph 17; ESMA, Guidelines on certain aspects of

document the purpose, scope and design of the algorithms behind its recommendations, including any decision trees or decision rules, and to test and monitor them. However, a general-purpose AI model does not produce its answers through decision rules that the firm can set out, and the firm would not ordinarily be able to inspect or change the model's design. A suitability assessment made by the model itself may therefore be difficult to document in the way the guidelines describe. Keeping the suitability assessment in rules the firm controls, and using the model to conduct the conversation, would appear easier to reconcile with the guidelines than leaving the assessment to the model.³⁰

ORDERS PLACED THROUGH AN ASSISTANT

An assistant that turns an instruction such as “sell half my position” into an order may give clients a new way of using an order service that the firm could historically have been offering through its app or website; in such instances, the firm's obligations would then depend on which of its order services the assistant is used for. The order services differ mainly in who completes the trade and in what capacity. The rules of MiFID II and MiCA on how the firm handles the client's order vary in part between them, which the assistant's design would need to reflect. Dealing on own account contrasts with passing the order on or executing it for the client, since the firm trades against its own capital as the client's counterparty, as is common for conversions of euros into a stablecoin, a service MiCA calls the exchange of crypto-assets for funds.³¹

The best execution rules of MiFID II and MiCA, under which a firm executing client orders has to seek the best possible result for the client, and their order-handling rules would appear to apply to an order taken through an assistant as they apply to one placed on the firm's order screen. The assistant would therefore need to pass each order to the firm's existing execution arrangements without altering it. Both regimes require a firm's execution arrangements to provide for the “prompt, fair and expeditious execution of client orders”, and an assistant that holds back an order the client has confirmed while the conversation continues could undermine those arrangements. A CASP exchanging crypto-assets for funds also has to execute the client's order at the price it displays when the order becomes final, so any price the assistant gives the client in conversation would need to be that displayed price.³²

Conversation with a chatbot can add a risk that a standard order screen largely avoids, since the assistant may misread the instruction and place an order the client did not mean, for instance by selling the wrong asset or converting the wrong amount. The firm would appear able to reduce the risk with a confirmation step, in which the assistant shows the client the asset, whether to buy or sell, the amount and any price limit as the assistant has understood them, before the order becomes final. Confirming each order in this way would also appear to support the firm's compliance with its duty to act in the client's best interests and to record executed orders accurately.³³

An order that the assistant has prompted may also call for an appropriateness assessment under MiFID II, which requires a firm providing an order service to assess whether the client has the knowledge and experience to understand the risks involved, an assessment known as the appropriateness test. The test may be dispensed with where, among other conditions, the order concerns a non-complex instrument and is given on the client's own initiative. An order ordinarily counts as given on the client's own initiative unless the client places it in response to a personalized communication from the firm that invites the client to buy or sell a specific instrument, or is meant to

the suitability requirements and format of the periodic statement for portfolio management activities under the Markets in Crypto Assets Regulation (MiCA), ESMA35-1872330276-2031 (26 March 2025) (“MiCA Suitability Guidelines”), paragraphs 18 and 86.

³⁰ MiFID II Suitability Guidelines (n 28), paragraph 90; MiCA Suitability Guidelines (n 28), paragraph 85.

³¹ MiFID II (n 4), Article 4(1)(5) and (6) and Annex I, Section A, points (1) to (3); MiCA (n 4), Article 3(1)(19), (21) and (23).

³² MiFID II (n 4), Articles 27(1) and 28(1); MiCA (n 4), Articles 77(3) and 78(1) and (2); European Commission, “Commission answers to CESR scope issues under MiFID and the implementing directive”, working document ESC-07-2007 annexed to its letter to CESR of 19 March 2007, paragraphs 6 to 9. Under the Commission's test, a firm dealing on own account may owe best execution where the client legitimately relies on the firm to protect its interests in the pricing, which the Commission considered likely to be presumed of a retail client in ordinary circumstances.

³³ MiFID II (n 4), Article 24(1); Delegated Regulation 2017/565 (n 4), Article 67(1)(a); MiCA (n 4), Articles 66(1) and 68(9).

influence the client's decision to do so; orders prompted by a general promotion addressed to the public can still count as given on the client's own initiative. An assistant's suggestion about a specific instrument is typically addressed to one client in a private conversation, so it would appear to be a personalized communication from the firm even where it falls short of a personal recommendation. Appropriateness would therefore need to be assessed before the firm acts on an order that the suggestion prompts. Lastly, while MiCA does not contain an equivalent test, the Commission appears to be considering one in its review of MiCA.³⁴

AGENTS THAT TRADE FOR A CLIENT

Agents would appear to stand differently from order-taking assistants where they act at their own discretion, since they may be seen as managing a client's portfolio under a discretionary mandate, which would qualify as portfolio management under both MiFID II and MiCA. Portfolio management services can extend to popular implementations such as copy trading; ESMA's supervisory briefing on copy trading treats a copy trading service as portfolio management where trades generated automatically execute unless the client modifies or rejects them within a set time, since the trades are then executed without any necessary intervention by the client. ESMA has said that the briefing applies, with the necessary changes, to identifying which crypto-asset service copy trading involves. It is reasonable to assume that limits set by the client, such as a maximum amount per trade or a list of permitted assets, would not by themselves remove the discretion that makes an agent's service portfolio management. An agent that executes a trade only on the client's positive confirmation of that trade would appear to provide an order service; however, where its proposals are personal recommendations, they would likely constitute advice. The difference resembles that between a broker who telephones for instructions before each trade and a portfolio manager who trades within a mandate.³⁵

COMMUNICATIONS, STAFF COMPETENCE AND RECORDS

The answers an assistant gives typically qualify as the firm's communications to its client, which MiFID II and MiCA both require to be fair, clear and not misleading, and require any marketing communications to be identified as such. MiFID II adds specific conditions for information that compares products or refers to past or future performance, such as stating the sources of a comparison and warning that past performance is not a reliable indicator of future results. MiCA requires a CASP not to mislead a client, deliberately or negligently, about the real or perceived advantages of a crypto-asset. A model that misquotes a fee, misstates a feature of a product or mischaracterizes a risk would likely therefore have given the client, on the firm's behalf, information that does not meet the requirement to be "fair, clear and not misleading". The fair, clear and not misleading standard applies under MiFID II and MiCA alike and, unlike MiCA's rule on the advantages of a crypto-asset, would not appear to depend on whether the firm was at fault. For distance financial services contracts with consumers, the Consumer Rights Directive also requires Member States to ensure that traders do not design their online interfaces in a way that deceives or manipulates consumers, which would appear to extend to a chatbot's conversational design. ESMA's statement on AI in investment services expects investment firms to disclose their use of chatbots during the conversation and to check the accuracy of information used by AI systems, and adds that "firms' decisions remain the responsibility of management bodies, irrespective of whether those decisions are taken by people or AI-based tools".³⁶

The knowledge and competence rules of MiFID II and MiCA apply to natural persons and would not appear to cover an assistant as such, although it should be noted that ESMA's guidelines under MiCA extend them, from July

³⁴ MiFID II (n 4), Article 25(3) and (4) and recital 85; Delegated Regulation 2017/565 (n 4), Article 56(1); MiCA (n 4), Article 140(2)(p); European Commission, Targeted consultation on the review of Regulation on the markets in crypto-assets (MiCA) (20 May 2026), question 47.

³⁵ MiFID II (n 4), Article 4(1)(8); MiCA (n 4), Article 3(1)(25);³⁵ ESMA, Supervisory briefing on supervisory expectations in relation to firms offering copy trading services, ESMA35-42-1428 (30 March 2023), paragraphs 27 to 29 and 33; MiCA Q&A (n 24), Q&A 2463 (7 April 2025).

³⁶ MiFID II (n 4), Article 24(3); Delegated Regulation 2017/565 (n 4), Article 44(3), (4) and (6); MiCA (n 4), Article 66(2); ESMA AI Statement (n 2), paragraphs 2, 9 and 16; Consumer Rights Directive (n 4), Article 16e(1).

2026, to the staff who determine the content of information or advice delivered in an automated manner. Conversations through an assistant are also records of the firm, which MiFID II requires to be kept for communications relating to, or intended to result in, transactions concluded when dealing on own account and the reception, transmission and execution of client orders. MiCA requires a CASP to keep records of all crypto-asset services, activities, orders and transactions. ESMA's expectation that records of AI use cover modifications made over time suggests that the firm should be able to identify which version of the model, and of its own instructions, produced each answer.³⁷

5. WHAT APPLIES WHEN AN ASSISTANT DEALS WITH PAYMENTS OR AN AGENT MAKES THEM FOR A CLIENT?

What a bank's assistant tells clients about payments, cards and loans may be subject to information duties that apply whether a member of staff or an assistant gives the information. Under PSD II, a bank has to give clients specified information on the charges and execution times of its payment services and on each payment. The Mortgage Credit Directive and the consumer credit directives in turn require a lender to give consumers pre-contractual information and adequate explanations of the credit on offer.³⁸

Beyond giving information, an agent may also move money for a client, for instance by paying a bill or sending funds to a third party. When this happens, PSD II likely comes into play, as it determines whether the firm needs a further authorization and who bears the loss of a payment the client did not intend. A firm whose agent instructs the client's bank to transfer money from the client's account may be providing a payment initiation service, which PSD II defines as initiating a payment order at the client's request from an account held with another payment service provider. A bank may provide that service under its existing authorization, while an investment firm or a CASP would appear to need authorization as a payment institution or an electronic money institution. Conversely, technical service providers that support payment services without ever holding the funds, such as providers of data processing or authentication, fall outside PSD II, although the exclusion does not extend to payment initiation.³⁹

Card payments may leave more room for the exclusion for technical service providers than transfers that the agent initiates. The card scheme, with the approval of the client's bank, can issue the agent a substitute for the client's card details, known as a card token, which the agent presents when it pays. The payment then remains a card payment that the client's bank approves as issuer of the card, and the firm offering the agent may be able to treat its own role as that of a technical service provider. An agent that sends e-money tokens held for the client directly to the payee, outside any card scheme, would appear to bring the firm back within PSD II. MiCA treats e-money tokens, the stablecoins that reference a single official currency, as electronic money, so a CASP whose agent transfers them to third parties for the client may be providing a payment service. In the EBA's view, a CASP that transfers e-money tokens for clients has needed authorization as a payment institution or an electronic money institution since March 2026, unless it works through an authorized payment service provider.⁴⁰

A payment that an agent makes beyond what the client intended may well be treated as unauthorized, since PSD II treats a payment as authorized only where the payer has consented to it. The client's bank would then have to refund the client by the end of the following business day, even where the payment was initiated through the firm's agent, and could recover the amount from the firm where the firm is liable for the unauthorized payment as a

³⁷ MiFID II (n 4), Articles 16(7) and 25(1); MiCA (n 4), Articles 68(9) and 81(7); ESMA, Guidelines for the criteria on the assessment of knowledge and competence under the Markets in Crypto Assets Regulation (MiCA), ESMA35-24871704-2922 (28 January 2026), paragraph 17; ESMA AI Statement (n 2), paragraph 24.

³⁸ PSD II (n 4), Title III; Directive 2008/48/EC (n 4), Article 5; new Consumer Credit Directive (n 4), Articles 10 and 12; the new Consumer Credit Directive replaces Directive 2008/48/EC from 20 November 2026 under its Articles 47 and 48(1); Mortgage Credit Directive (n 4), Articles 14 and 16.

³⁹ PSD II (n 4), Articles 1(1)(a) and (b), 3(j), 4(15) and 11(1) and Annex I, point (7).

⁴⁰ MiCA (n 4), Articles 3(1)(7) and 48(2); EBA, Opinion on the interplay between Directive (EU) 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCA) in relation to crypto-asset service providers that transact electronic money tokens, EBA/Op/2025/08 (10 June 2025), paragraphs 18 and 23.

payment initiation service provider. Most electronic payments also require strong customer authentication, which combines two or more independent elements, such as a password and the client's phone, to confirm that the client is the one paying. A client who hands an agent its own passwords and other personalized security credentials so that the agent can complete that authentication may breach the client's duty under PSD II to keep them safe and, if that amounts to gross negligence, bear the whole loss of an unauthorized payment. PSD II entitles clients to use authorized payment initiation service providers, however, so the risk would appear greatest where the firm offering the agent lacks that authorization. Requiring the client to confirm and authenticate each payment, as with orders, would appear to reduce both the risk of a disputed payment and any need for the client to share credentials.⁴¹

The Payment Services Regulation and a third Payment Services Directive, which the EU institutions agreed provisionally in November 2025 and have yet to adopt formally, are due to replace PSD II. The agreed texts would appear to keep the concepts of consent, payment initiation and strong customer authentication on which the rules for agents that make payments depend. An investment firm or a CASP that needs authorization for its agent's payments would then appear to need it as a payment institution, since electronic money institutions would become a category of payment institution.⁴²

6. WHAT SHOULD THE FIRM'S CONTRACT WITH THE MODEL PROVIDER CONTAIN?

Should a firm rely on a model provider for the model behind its chatbot, then such a contractual relationship would fall under DORA, which applies to banks, investment firms and CASPs alike. DORA defines ICT services broadly enough that access to the model through an API would appear to qualify as an ICT service, so the model provider would be an ICT third-party service provider to be recorded in the firm's register of information on its ICT arrangements. Every contractual arrangement on the use of ICT services should describe the services and address, among other things, the locations where data is processed and the firm's termination rights. A chatbot that answers clients about the firm's services or takes their orders may also support a "critical or important function", meaning broadly a function whose disruption or failure would materially impair the firm's financial performance, the soundness or continuity of its services, or its compliance with its authorization and other financial services law. In such cases, the firm's contractual arrangement with the model provider would then also need to include exit strategies and rights of access, inspection and audit. DORA's requirements also apply where the firm accesses the model through the platform of a cloud provider, as many firms may do, although the firm's ICT third-party service provider would then be the cloud provider and the model provider would appear to be the cloud provider's subcontractor.⁴³ The designation of several cloud providers in November 2025 as "critical ICT third-party service providers", subject to direct oversight at EU level, would leave the firm's own obligations under DORA unchanged.⁴⁴

Alongside DORA, the firm's arrangement with the model provider may also amount to outsourcing under MiFID II and MiCA. MiFID II imposes its detailed conditions where the outsourced function is "critical or important", meaning one whose defective performance would materially impair the firm's compliance, its financial performance or the soundness or continuity of its services. Interestingly, MiFID II's outsourcing rules do not treat the purchase of standardized services, such as market information services and price feeds, as the outsourcing of a "critical or important" function. This means that a firm might argue that access to a general-purpose AI model is also a standardized service, since the model provider offers the model on standard terms to many customers. The

⁴¹ PSD II (n 4), Articles 4(30), 64, 66(1) and (3)(b), 69(2), 73(1) and (2), 74(1) and 97(1) and (2) and recital 69.

⁴² Council of the EU, final compromise texts of the proposed Payment Services Regulation, ST 8221/26 (17 April 2026), recitals 54, 69b and 76a, and of the proposed third Payment Services Directive, ST 8222/26 (17 April 2026); European Parliament, "Payment services deal: More protection from online fraud and hidden fees" (press release, 27 November 2025); European Parliament, Legislative Observatory, procedures 2023/0209(COD) and 2023/0210(COD).

⁴³ DORA (n 4), Articles 2(1)(a), (e) and (f), 3(19), (21) and (22), 28(3) and 30(2)(a), (b) and (h) and (3)(e) and (f); European Supervisory Authorities, Q&A DORA030, answered by the European Commission.

⁴⁴ European Supervisory Authorities, list of designated "critical ICT third-party service providers" (18 November 2025); DORA (n 4), Articles 28(1)(a) and 31.

exclusion for standardized services may be harder to apply to a model that composes the answers given to clients, however, since market information and price feeds are inputs to the firm's own work, while such a model typically performs part of that work. A model that gives clients wrong answers could materially impair the firm's compliance, so the function it performs may be "critical or important" however standardized the terms on which the firm obtains the model.⁴⁵

Outsourcing calls for further contractual protections that a model provider's standard terms may not offer, and what is required differs for banks, investment firms and CASPs:

- A bank using the model for its banking services outside MiFID II and MiCA would appear to fall under the EBA's Guidelines on outsourcing arrangements, which require access and audit rights for the bank and its competent authority where the function is "critical or important". The EBA's new guidelines on third-party risk are to replace them from a date the EBA has yet to set, and since the new guidelines exclude ICT services, a bank's access to a general-purpose AI model would then appear to be governed by DORA alone.⁴⁶
- An investment firm outsourcing a "critical or important" function under MiFID II has to ensure, among other things, that the firm, its auditors and its competent authority have effective access to the model provider's data on the outsourced function and, where necessary, to its business premises. Any sub-outsourcing by the model provider would also need the firm's consent.⁴⁷
- A CASP is subject to MiCA's outsourcing rules whatever the importance of the function. MiCA does not define outsourcing, although a model that composes the answers a CASP's staff would give would appear to perform a process the CASP would otherwise undertake itself, which is how the Commission's delegated regulation under MiFID II defines outsourcing. The CASP would need to ensure that the model provider cooperates with the CASP's competent authority and that the CASP has direct access to the relevant information. Its written agreement with the model provider would also need to set out the Union data protection standards that the model provider has to meet and give the CASP a right to terminate the agreement.⁴⁸

The arrangement with the model provider also has to meet data protection rules, since client conversations will usually contain personal data. The GDPR allows a model provider acting as the firm's processor to use the personal data only on the firm's documented instructions, including instructions on transfers of the data to a third country or an international organization. The model provider would appear to become a controller in its own right if it uses the conversations to train its own models, so the firm's contract with the model provider would usually address whether the model provider may do so.⁴⁹

Beyond the information the AI Act requires the model provider to give, the firm's contract is the main means by which the firm can secure notice of changes to the model, access for testing and the information it needs to keep its disclosures, records and controls current. For a model obtained through a cloud platform, the firm would also need to secure the same commitments from the cloud provider, backed by the cloud provider's own arrangements with the model provider. The contract should also allocate the cost of a wrong answer between the firm and the model provider, for instance through indemnities and limits on the model provider's liability, although the allocation would leave the firm's own responsibility to its clients unchanged.

⁴⁵ MiFID II (n 4), Article 16(5); Delegated Regulation 2017/565 (n 4), Articles 2(3), 30 and 31; ESMA AI Statement (n 2), paragraph 14.

⁴⁶ EBA, Guidelines on outsourcing arrangements, EBA/GL/2019/02 (25 February 2019), Section 13.3, paragraph 87; EBA, Guidelines on the sound management of third-party risk, EBA/GL/2026/09 (18 September 2026), paragraphs 7, 18 and 22.

⁴⁷ Delegated Regulation 2017/565 (n 4), Article 31(2)(i) and (3).

⁴⁸ Delegated Regulation 2017/565 (n 4), Article 2(3); MiCA (n 4), Article 73(1) and (3).

⁴⁹ GDPR (n 4), Articles 28(3)(a) and (10) and 29.

7. DO CLIENTS HAVE A RIGHT TO SPEAK TO A HUMAN?

Under the Consumer Rights Directive, as amended in 2023, Member States have had to apply, from 19 June 2026, national measures giving consumers a right “to request and to obtain human intervention” where a trader uses online tools in connection with a financial services contract concluded at a distance. The right applies at the pre-contractual stage and, in justified cases, after the contract is concluded. The recitals to the 2023 amendments give chatbots, robo-advice and interactive tools as examples and describe a right to a human acting for the trader, free of charge, during business hours. For a contract comprising an initial service agreement followed by successive operations, most of the Consumer Rights Directive’s rules on distance financial services contracts only apply to the initial agreement; a support chatbot serving an existing account holder would therefore appear to engage the right only in the justified cases the recitals describe, such as renewal or a need for further explanation of the contractual terms.⁵⁰

The right to human intervention forms part of the Consumer Rights Directive’s rules on adequate explanations, which give way where another Union act governing a specific financial service contains its own rules on adequate explanations.⁵¹ MiFID II has its own rules on explanations for investment services, as do the consumer credit directives and the Mortgage Credit Directive for consumer loans and mortgages. For investment services the right would therefore appear to give way to MiFID II, although a court could treat human intervention as a distinct right that survives, and ESMA’s suitability guidelines ask robo-advice firms only to explain whether and how clients can ask for human interaction. For a bank, the right would appear to apply chiefly to deposits, payment accounts and payment services concluded at a distance.⁵² The new payment services rules agreed in November 2025 would also, once adopted, require payment service providers to give users access to human customer support in addition to any chatbot.⁵³

The Consumer Rights Directive does not address whether crypto-asset services are financial services “of a banking, credit, insurance, personal pension, investment or payment nature”, so its application to CASPs remains uncertain. MiCA amended the regulation establishing ESMA so that ESMA’s remit covers the relevant parts of the Distance Marketing Directive to the extent that it applies to CASPs, which suggests that the EU legislature contemplated its application to them. The Consumer Rights Directive’s rules on distance financial services contracts have since replaced the Distance Marketing Directive, which points toward their coverage of CASPs as well. On the view that the Consumer Rights Directive covers CASPs, MiCA’s suitability rules, which would appear to be the MiCA rules closest to rules on adequate explanations, may displace the right for advice and portfolio management. A CASP providing exchange, execution, custody or transfer services to consumers at a distance could then be subject to the right, since MiCA’s rules for those services would not appear to include rules on adequate explanations.⁵⁴

The GDPR already gives a client who is a natural person the right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects. The client may obtain human intervention, express a point of view and contest the decision where such a decision is nonetheless allowed because it is necessary for a contract or rests on the client’s explicit consent. Therefore, a chatbot that itself declines an application or blocks a payment could trigger the client’s right under the GDPR to obtain human intervention. The Court of Justice held in *SCHUFA* that even a credit score on which a lender draws strongly can itself be a decision

⁵⁰ Consumer Rights Directive (n 4), Articles 3(1b) and 16d(3); Directive (EU) 2023/2673 (n 4), Article 2(1) and recitals 15 and 40.

⁵¹ Consumer Rights Directive (n 4), Article 16d, headed “Adequate explanations”, and Article 16d(5); Directive (EU) 2023/2673 (n 4), recital 15, which presents the right as part of the rule on adequate explanations.

⁵² Directive (EU) 2023/2673 (n 4), recital 20; Mortgage Credit Directive (n 4), Article 16; Directive 2008/48/EC (n 4), Article 5(6); new Consumer Credit Directive (n 4), Article 12; MiFID II Suitability Guidelines (n 28), paragraph 17.

⁵³ European Parliament press release of 27 November 2025 (n 41).

⁵⁴ Consumer Rights Directive (n 4), Article 2(12); MiCA (n 4), Article 81, and Article 145, which amends Article 1(2) of Regulation (EU) No 1095/2010 and refers to Directive 2002/65/EC (OJ L 271, 9.10.2002, p. 16) (the “Distance Marketing Directive”), repealed with effect from 19 June 2026 by Directive (EU) 2023/2673 (n 4), Article 3.

based solely on automated processing, so a chatbot's assessment on which the firm's staff rely strongly could also engage the right.⁵⁵ From 20 November 2026, the new Consumer Credit Directive also gives consumers whose creditworthiness is assessed with automated processing a right to human intervention, an explanation and a review, which a chatbot gathering information for the assessment would appear to engage.⁵⁶

8. WHO ANSWERS FOR WHAT A CHATBOT TELLS A CLIENT?

Responsibility for the assistant's answers rests with the firm under whichever rules govern the service in question, which for investment and crypto-asset services are MiFID II and MiCA, since the assistant's answers typically qualify as the firm's own communications to its client. DORA also keeps the firm fully responsible for its obligations whatever ICT services it uses. MiFID II further requires Member States to ensure that compensation may be paid, or other remedial action taken, in accordance with national law for financial loss resulting from an infringement, a provision MiCA does not appear to match. A CASP providing custody is, however, liable under MiCA for the loss of a client's crypto-assets resulting from an incident attributable to it, which an agent acting on the client's account could cause. Beyond MiFID II's compensation rule and MiCA's custody liability, civil liability to a client is largely left to national law, subject to the principles of equivalence and effectiveness, and the claims available for a wrong answer, in contract, in tort or delict or for breach of conduct rules, vary between Member States.⁵⁷

The Higher Regional Court of Hamm has given an early indication of how national courts may treat a chatbot's wrong answers, in injunction proceedings that a consumer association brought under the German law implementing the Unfair Commercial Practices Directive. The chatbot of an aesthetic medicine practice had given the two doctors running the practice specialist titles that they did not hold, and the court held in May 2026 that the practice was responsible for the misleading statements. It rejected the argument that the chatbot was a third party, for whose statements the practice would answer only if it had breached a duty of care, and considered that the practice would remain responsible even if it had the chatbot programmed using only correct data. The court allowed an appeal to the Federal Court of Justice, so the judgment is not yet final, although its reasoning would appear to apply equally to a regulated firm whose chatbot misstates a fee or a feature of a product. For instance, a disclaimer by a firm telling clients to check the chatbot's answers elsewhere would arguably be unlikely to change the result under MiFID II or MiCA.⁵⁸

EU product liability law would appear to offer clients little by way of remedy, since the revised Product Liability Directive compensates only natural persons and only for death, personal injury and certain damage to property and data; the financial loss a client suffers by acting on a wrong answer would not appear to fall within those heads of damage. However, a client who loses money in that way may seek redress from the firm through the complaints procedures that MiFID II and MiCA require firms to maintain.⁵⁹

⁵⁵ GDPR (n 4), Article 22(1) to (3); Case C-634/21, *SCHUFA Holding (Scoring)*, judgment of 7 December 2023, EU:C:2023:957, paragraphs 50 and 73.

⁵⁶ New Consumer Credit Directive (n 4), Articles 18(8) and 48(1).

⁵⁷ MiFID II (n 4), Articles 24(3) and 69(2); MiCA (n 4), Articles 66(2) and 75(8); DORA (n 4), Article 28(1)(a); see, to that effect, *Genil* 48 (n 21), paragraph 57.

⁵⁸ Higher Regional Court of Hamm (Oberlandesgericht Hamm), judgment of 12 May 2026, 4 UKI 3/25, *Verbraucherzentrale Nordrhein-Westfalen e.V. v. Aesthetify GmbH*, and press release of 12 May 2026; Unfair Competition Act (Gesetz gegen den unlauteren Wettbewerb), § 5(1) and (2), point 3; Unfair Commercial Practices Directive (n 4), Article 6(1)(f).

⁵⁹ Product Liability Directive (n 4), Articles 5(1) and 6(1) and recital 24; Delegated Regulation 2017/565 (n 4), Article 26; MiCA (n 4), Article 71.

9. CONCLUSION

On balance, the AI Act is likely to be the comparatively lighter part of the work for a firm launching a client chatbot. The more challenging regulatory requirements lie in MiFID II and MiCA, depending on the latitude and capabilities of the AI model being deployed, since, for instance, an assistant built to explain can drift into advising, and one that takes orders in conversation may misread the instruction it is given. MiFID II and MiCA would appear to hold the firm responsible for what the assistant does as fully as for the work of its own staff, while the model behind the assistant remains under the model provider's control. A firm could therefore be answerable for a service whose central component it would not ordinarily be able to inspect or change.

A firm's contract, whether with the model provider or with a cloud provider, may be its main route to the information, access and exit rights it needs to account for the assistant to its competent authority. It can be said that one of the optimal situations for a firm operating a chatbot would be where the model conducts the conversation and the decisions for which the firm answers rest on rules the firm controls or on the client's confirmation of each order and payment. Furthermore, a suitability assessment made by rules, or an order the client has confirmed, can be documented and defended in a way that a model's own judgment may not. Recording and monitoring the assistant's conversations as the firm's own communications (in line with a firm's obligations under MiFID II and/or MiCA, and with the GDPR) would also give the firm a record of what the model told each client.

The configurations described in this article are stylized, and live deployments tend to combine them or even introduce other functionalities; the conclusions depend on the facts, on national transposition and on documentation, and would need to be tested against any particular deployment. The regulatory ground is also moving dynamically, since the Commission's guidelines on Article 50 date from July 2026, and ESMA has not issued a statement on AI under MiCA comparable to its 2024 statement on investment services. The pace of change should come as no surprise, given the novelty of the technology as well as the flexibility granted to the Commission under the AI Act to, *inter alia*, adjust the list of high-risk uses and the threshold for general-purpose AI models with systemic risk by delegated act as the technology develops.⁶⁰ The Retail Investment Strategy, a legislative package amending MiFID II and other Union acts on retail investment, will tighten MiFID II's rules on marketing communications, with particular attention to digital channels (and therefore including AI chatbots), while the Strategy and the Payment Services Regulation are still awaiting formal adoption and are likely to add further rules on how firms communicate with clients online.⁶¹

In the meantime, we would expect competent authorities to judge a client chatbot much as they would the agency hire at the front desk, by what it tells clients and does on their accounts and by how carefully the firm briefed and supervised it. The firm would then answer for the chatbot much as a principal answers for its agent, which gives the term "AI Agent" a meaning beyond the technical one. Any client-facing chatbots and assistants should therefore be carefully structured and calibrated in order to avoid any unintended regulatory breaches of the myriad applicable legal frameworks.

⁶⁰ AI Act (n 4), Articles 7(1) and (3), 51(3) and 97.

⁶¹ Article 50 Guidelines (n 2); ESMA AI Statement (n 2); Council of the EU, "Retail investment strategy: Council and Parliament agree on package to empower consumers while boosting markets" (press release, 18 December 2025); European Commission, request to ESMA for technical advice on the implementation of the amendments to MiFID II, the UCITS Directive and the AIFM Directive in the context of the Retail Investment Strategy, fisma.c.3(2026)6598499 (30 July 2026), section 3(e); European Parliament, Legislative Observatory, procedures 2023/0167(COD) and 2023/0210(COD).

CONTACT

The CahillNXT team advises banks, investment firms, crypto-asset service providers, technology providers, and institutional participants on the regulatory treatment of AI chatbots and agentic tools under the AI Act, MiFID II, MiCA, DORA and PSD II, and on the preparation of responses to regulatory consultations in this area, and would be glad to discuss how any of the matters addressed above may bear upon a particular structure. If you have any questions about the issues addressed in this article, or would like a copy of any of the materials mentioned in it, please do not hesitate to call or email author Jonathan Galea (partner) at +44.20.7947.9315 or jgalea@cahill.com, or email publicationscommittee@cahill.com.



Jonathan Galea

Partner

+44.20.7947.9315

jgalea@cahill.com