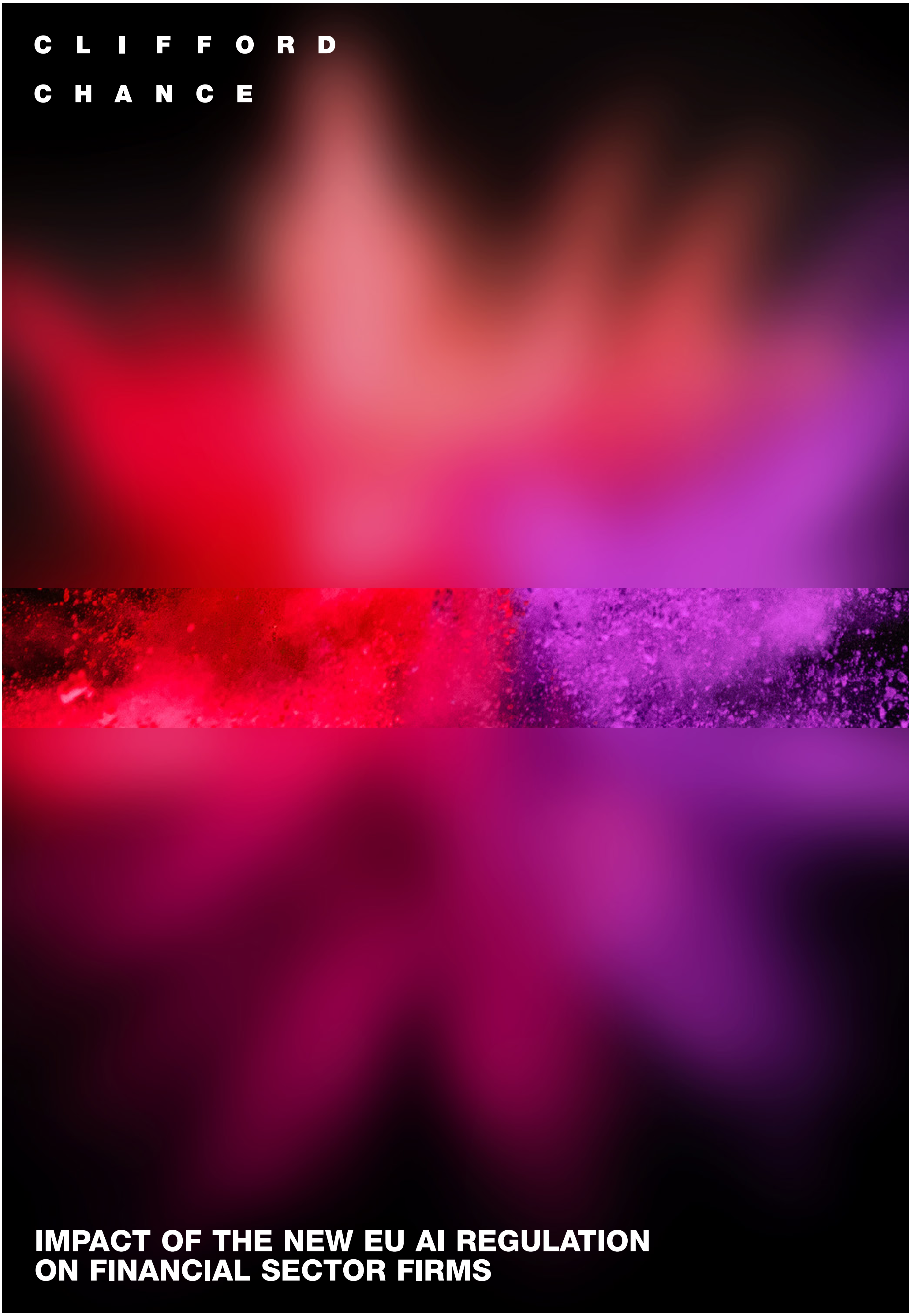
CLIFFORD
CHANCE



IMPACT OF THE NEW EU AI REGULATION ON FINANCIAL SECTOR FIRMS

IMPACT OF THE NEW EU AI REGULATION ON FINANCIAL SECTOR FIRMS

The recently proposed EU regulation on artificial intelligence (AI Act) will impose new regulatory requirements on firms across the financial sector when they use, provide, import or distribute computer software for biometric identification, human capital management or credit assessment of individuals. It will also prohibit the deployment of software exploiting subliminal techniques or vulnerabilities due to age or disability and impose transparency obligations on providers and users of other software. Firms' compliance with the new requirements will be challenging because of the difficulty of determining what software will be treated as an 'artificial intelligence system' subject to these requirements and which entities within a financial sector group will be subject to obligations under the AI Act, especially given its extraterritorial application.

Key issues

The AI Act is likely to have a significant impact on financial sector firms

Its definition of 'AI system' could capture almost any software

Some software is prohibited: exploitation of subliminal techniques, age or disability

High-risk software is subject to burdensome regulatory requirements

This includes software for biometric identification, human capital management or credit assessment of individuals

Transparency requirements apply to some other software

EU and non-EU firms may be regulated as users, providers, importers or distributors of software

Fines of up to 6% of global turnover will apply to contraventions

The AI Act is expected to become law in 2022: firms must comply 2 years later

Firms should begin to organise their response to the new requirements

The European Commission issued its **legislative proposal** for the AI Act in April 2021 as part of its wider plan to coordinate EU policy priorities on, and investment in, artificial intelligence (AI). The AI Act aims to address the risks associated with certain uses of this emerging technology by creating a harmonised EU legal framework to give users confidence in AI-based solutions, encourage businesses to develop those solutions and prevent fragmentation of the EU single market as a result of diverging national regulation of AI. The Commission's consultation on the text of the proposal has now closed.

The regulation is in the early stages of the legislative process and the European Parliament and the Council may amend the proposal before it is finally adopted (and there have already been calls for changes to extend the obligations of firms under the regulation). The legislation is expected to become law towards the end of 2022 and firms will have to comply with the new requirements two years later. However, firms will need to develop the procedures, systems and controls needed to ensure compliance well in advance of that date.

The AI Act is 'horizontal legislation' applying to all industry sectors and to public bodies but is likely to have a particular impact on financial sector firms. Financial sector firms are more likely to make use of some of the classes of software subject to the new requirements (such as software used for biometric identification and credit assessment of individuals). In addition, many financial sector firms are likely to be subject to the new obligations applicable to software providers, importers and distributors, as well as the obligations applicable to software users, because of their use of in-house software development teams, their extensive commissioning of bespoke software from third-party providers, and their complex, cross-border legal structures.

This briefing focuses on the obligations under the AI Act most likely to be relevant to financial sector firms. For a more general discussion of the AI Act and other international developments on the regulation of AI, see our briefing: **The Future of AI Regulation in Europe and its Global Impact** (May 2021).

'AI system' = any software?

The AI Act will prohibit the deployment of and regulate the use, provision, import and distribution of certain classes of 'artificial intelligence system (AI system)'. defined as any:

"software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."

The annexed list of techniques and approaches covers machine learning approaches, logic- and knowledge-based approaches, statistical approaches, Bayesian estimation and search and optimisation methods. The Commission will be given the power to amend the annexed list of techniques and approaches to reflect market and technological developments.

This definition could, on its face, capture almost any software used by firms, even if it does not involve any recognisable form of artificial intelligence. For example, almost any spreadsheet or database tool could be regarded as using a logic-based approach or search method to generate outputs which meet human-defined objectives and influence decisions taken by its users.

Even if the listed techniques and approaches are computer-science 'terms of art' which limit the scope of the definition, it may be difficult to determine their meaning with legal certainty in a rapidly evolving field — the Commission's own impact assessment acknowledges that definitions of AI are highly contested. Also, users, importers and distributors of third-party software, and firms that commission or modify third-party software, may not have sufficient information to determine whether the software was developed using the listed techniques or approaches. In any event, it seems likely that new software will increasingly use techniques and approaches that are associated with recognised AI technologies. Therefore, firms may have to assume that a very wide range of software potentially falls within the definition and look to other provisions of the AI Act to determine whether software is prohibited or subject to regulation.

> **"The definition of AI system could capture almost any software used by firms, even if it does not involve any recognisable form of artificial intelligence."**

What software will be prohibited or regulated under the AI Act?

The AI Act will impose obligations on firms with respect to three classes of 'AI system': prohibited AI systems, AI systems regulated as 'high-risk' and AI systems subject to transparency requirements (see Box 1).

What software will be prohibited?

The AI Act will prohibit firms placing on the market, putting into service or using 'AI systems' that exploit subliminal techniques or vulnerabilities due to age, physical or mental disabilities in a manner that causes or is likely to cause physical or psychological harm. These prohibitions are relatively narrow but there are already calls to extend some of the prohibitions that will apply to public authorities and law enforcement bodies so that they apply to private sector firms as well (eg, the prohibitions on certain uses of facial recognition techniques in public spaces).

Box 1: What classes of 'AI system' are subject to the AI Act?	
Prohibited AI systems	
Exploitation of subliminal techniques or age or disability	Software: • deploying subliminal techniques beyond a person's consciousness to materially distort a person's behaviour; or • exploiting any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, to materially distort the behaviour of a person pertaining to that group, in a manner that causes or is likely to cause that person or another person physical or psychological harm.
High-risk AI systems	
Biometric identification and categorisation	Software intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons.
Employment, workers management and access to self-employment	Software intended to be used for recruitment or selection of natural persons (including for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests). Software intended to be used for: • making decisions on promotion and termination of work-related contractual relationships, • task allocation and • monitoring and evaluating performance and behaviour of persons in such relationships.
Credit assessment of natural persons for essential private services	Software intended to be used to: • evaluate the creditworthiness of natural persons or • establish the credit score of natural persons (with the exception of software put into service by providers that are micro- or small enterprises for their own use).
AI systems subject to transparency requirements	
Individual users	Software intended to interact with natural persons.
Emotion recognition and biometric categorisation	Software identifying or inferring emotions or intentions of natural persons from their biometric data. Software assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data.
'Deep fake' software	Software generating or manipulating image, audio or video resembling persons, objects, places or other entities or events that would falsely appear to be authentic or truthful.

What software will be regulated as 'high-risk'?

The principal regulatory obligations of the AI Act will apply to the use, provision, import or distribution of 'high-risk AI systems'. The definition of this covers certain software used as safety components in physical products or by operators of critical infrastructure, educational or vocational training institutions, public authorities and law enforcement. However, the AI Act also treats as 'high-risk' some classes of AI system that that may be relevant to financial sector firms, in particular software used for biometric identification, human capital management and the credit assessment of individuals. The Commission will be given the power to extend the definitions of these classes to cover additional types of software.

The class of biometric identification software treated as 'high-risk' may be limited to software involving remote biometric identification, described as "the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified". It is not clear whether biometric authentication software, such as fingerprint or face recognition software used to establish customer identity and allow customer access to accounts or to allow staff access to firms' premises or computer systems, will be treated as falling within this class.

It may be difficult to determine when software used for human capital management or credit assessment of individuals is treated as 'high-risk', especially given the potential breadth of the definition of 'AI system'. For example, this class could cover almost any software (including spreadsheets or databases) used to manage recruitment, recording and retrieval of employee data, appraisals, salary, bonus or promotion reviews, holiday allocation, time recording or task allocation as part of work management. While the class of credit assessment software may be limited to software used in relation to evaluate access to 'essential private services' this includes software used to evaluate access to financial resources, which may cover banking, insurance or other financial services. It may also be difficult to delineate the scope of the software subject to regulation, for example, where software used for credit assessment of individuals is integrated with the firm's pricing or risk-management systems.

What software will be subject to transparency requirements?

Providers of an AI system intended to interact with natural persons will have to ensure that the system is designed or developed so that natural persons are aware that they are interacting with an 'AI system', unless this is already obvious. This will cover chatbots but may also cover a wide range of other software where natural persons interact with the software in any way (eg, by inputting data or accessing content).

Users of an AI system which is an emotion recognition or biometric categorisation system will have to inform natural persons exposed to the system of its operation. Users of AI systems generating or manipulating 'deep fakes' will have to disclose that the content has been artificially generated or manipulated.

These obligations will also apply to high-risk AI systems which have the described characteristics.

Other software

The AI Act will not impose any requirements on firms with respect to other AI systems or software. However, it does envisage that the Commission and Member

States will encourage and facilitate the drawing up of codes of conduct for the voluntary application of the requirements for high-risk AI systems to other AI systems and for the voluntary application of other requirements to AI systems generally (eg, requirements on environmental sustainable or accessibility for persons with a disability, stakeholder engagement and diversity). There have also been calls to impose further obligations on operators of AI systems including giving consumers additional rights to access information and explanations about algorithmic decisions.

Which financial sector firms will be subject to obligations under the AI Act?

Financial sector firms will be subject to obligations under the AI Act where they are users, providers, importers or distributors of relevant AI systems or when they place prohibited AI systems on the market or put that software into service (see Box 2).

Box 2: 'AI systems' – who is regulated?	
Prohibited AI systems	Anyone: • placing the software on the market • putting the software into service or • using the software.
High-risk AI systems	• Users • Providers • Importers • Distributors.
AI systems subject to transparency requirements	• Providers of software intended to interact with natural persons. • Users of emotion recognition, biometric categorisation or 'deep fake' software.
Definitions	
User	Any person using the software under its authority, except where the software is used in the course of a personal non-professional activity.
Provider	Any person that develops the software or has the software developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge. Any other person that: • places the software on the market or puts it into service under its name or trademark; • modifies the intended purpose of the software after it has been placed on the market or put into service; • makes a substantial modification to the software.
Importer	Any person established in the EU that places the software on the market or puts it into service if it bears the name or trademark of a person established outside the EU.
Distributor	Any person in the supply chain, other than the provider or the importer, that makes the software available on the EU market without affecting its properties.
Other	• 'Placing on the market' means the first making available of software on the EU market; • 'Making available on the market' means any supply of software for distribution or use on the EU market in the course of a commercial activity, whether in return for payment or free of charge; • 'Putting into service' means the supply of software for first use directly to the user or for own use on the EU market for its intended purpose; • 'Substantial modification' means a change to software following its placing on the market or putting into service which affects the compliance of the software with the requirements for 'high-risk AI systems' or results in a modification to the intended purpose for which the software has been assessed.

Firms will be subject to obligations as a 'user' of an AI system where the software forms part of the firm's own systems (whether the software is proprietary or used under licence from a third party). Firms will also need to consider whether they are subject to obligations as a 'user' where they rely on or otherwise use the systems of third parties, such as group companies, customers, suppliers or market infrastructure. The AI Act does not indicate how to determine when third-party software is used "under [a firm's] authority" resulting in the firm being treated as a 'user'.

Firms may also be subject to obligations as a 'provider' of an AI system used by the firm because the software is developed by an in-house team or is commissioned from a third-party provider, because the firm has modified or adapted third-party software or simply because the firm uses software provided by a third party under the firm's own name or trademark. For example, a firm may be regarded as the 'provider' of a 'high-risk AI system' if it creates a tool for managing its employee appraisal process using generic spreadsheet or database software. The firm may also be regarded as a 'provider' of an AI system used by other group companies or third parties, for example, if the firm developed the software or commissioned it from third parties. In many of these cases, it may be difficult for the firm itself to comply with all the obligations imposed on 'providers' and it will need to consider the extent to which it can rely on contractual arrangements with developers or other third parties to achieve compliance (eg, to demonstrate compliance with the software design requirements or to provide surveillance authorities with access to data sets or source codes).

In addition, firms established in the EU may be subject to obligations as an 'importer' of a high-risk AI system used by them when they put the software into service under the name or trademark of a non-EU person. Additional obligations may apply where the firm makes a high-risk AI system available for use by other group companies, customers or suppliers as the firm may then be regarded as a 'distributor' of the system.

Multiple companies within a financial sector group may be subject to obligations under the AI Act as users, providers, importers or distributors of a single AI system. Many group companies may participate in the procurement, development, ongoing maintenance, management and use of the software and, where relevant, in making the software available to other group companies, customers or suppliers under inter-affiliate service arrangements or other contracts (and perhaps under a common group brand name or trademark). This may make it difficult to identify in what capacities group companies are subject to obligations under the AI Act, especially given the extraterritorial application of the AI Act.

> **Multiple group companies may be subject to obligations under the AI Act as users, providers, importers or distributors of a single AI system.**

What is the extraterritorial impact of the AI Act?

The obligations under the AI Act will apply to EU firms that are users of AI systems and EU firms that are providers, importers or distributors of AI systems placed on the market, put into service or made available on the market in the EU.

However, the AI Act will also apply to:

- non-EU providers of prohibited or high-risk AI systems placing the software on the EU market or putting the software into service on the EU market;
- non-EU providers and users of prohibited or high-risk AI systems, where the output produced by the software is used in the EU (eg, where non-EU firms provide outsourced services to firms located in the EU).

The AI Act does not specifically address how its obligations apply to EU-incorporated entities that operate through branches outside the EU or to non-EU incorporated entities operating through branches in the EU. It also does not specifically address whether the obligations applicable to distributors apply to non-EU firms that make the software available on the EU market.

In some cases, non-EU providers may not be able readily to identify when their software is being placed on the EU market or put into service on the EU market and non-EU providers and users may not be able readily to identify where output produced by their software is being used in the EU. Non-EU firms regarded as providers of software may have particular concerns about the burden of complying with obligations that require the appointment of an EU representative, the assessment and certification of conformity of software in accordance with EU law (especially where that involves an EU official assessment body), registration of software on the Commission database, incident reporting to EU authorities and granting EU authorities access to information, data-sets and source codes. Non-EU providers or users that are not willing or able to comply with the requirements of the AI Act may need to consider whether they can restrict the use or distribution of their software or its output in the EU.

“The AI Act will apply to non-EU providers and users of 'high-risk' software where the output of that software is used in the EU.”

The extraterritorial application of the AI Act may have a particular impact on EU-headquartered financial groups. The group’s EU head office human capital, risk-management or regulatory capital processes are likely to use outputs of human capital management and credit assessment software deployed by their non-EU subsidiaries. As a result, the AI Act may apply both to those non-EU subsidiaries and to non-EU group and non-group companies that are treated as providing that software, at least if any of the individuals affected by the use are located in the EU (and possibly even if not). Non-EU headquartered groups may be able to limit the extent that the output of software deployed outside the EU is used within the EU, but the AI Act will still apply to non-EU entities within those groups if they treated as providing software for use by their EU subsidiaries.

The AI Act does not envisage any relief in relation to software provided or used by non-EU entities subject to equivalent third-country regulatory requirements, even if some other countries were eventually to follow the EU approach of regulating software in this way. The Commission’s impact assessment notes that no other country has enacted a similar regulatory framework for AI, although there are some US legislative initiatives on automated decision-making and facial recognition as well as numerous initiatives providing guidance, principles or voluntary international technical standards which may be applied by the private sector. The AI Act will establish a harmonised EU framework of binding rules that must be applied by all firms, including non-EU firms, that fall within its scope regardless of their compliance with rules or standards that apply elsewhere.

What obligations will apply to financial sector firms in relation to 'high-risk' software?

The principal regulatory obligations of the AI Act will apply in relation to high-risk AI systems and different obligations will apply to firms according to whether they are users, providers, importers or distributors of that software (see Box 3).

Users will be subject to more limited obligations under the AI Act and may be able to rely on existing procedures, systems and controls to meet some of these obligations. However, they may need to put in place new procedures, systems and controls to comply with some obligations, such as the record-keeping, transparency and notification obligations that will apply to them.

In contrast, providers will be subject to extensive and potentially burdensome new obligations which are likely to require the introduction of new procedures, systems and controls. These obligations include obligations to establish or ensure the establishment of prescribed systems for risk management, quality management and post-market monitoring, to ensure that the design of the software meets prescribed standards (eg, to enable effective human oversight), to prepare prescribed technical documentation, to assess the software's conformity with the AI Act before use or distribution (which may require the involvement of a national conformity assessment body in relation to biometric software), to make a declaration of EU conformity and to register the software on a publicly-available Commission database (including the electronic instructions for use even if these are commercially confidential). Non-EU providers will also have to appoint a legal representative in the EU to perform and carry out on its behalf the obligations and procedures established under the AI Act, where an importer cannot be identified.

> Software 'providers' will be subject to extensive and potentially burdensome new obligations.

The Commission is required to adopt measures detailing providers' obligations for post-market monitoring. Member States will need to take action to designate or establish authorities for the purposes of assessing, designating and notifying conformity assessment bodies for the purposes of the AI Act.

Providers may be able to meet some of their obligation under the AI Act by complying with harmonised EU standards where these exist. However, the Commission will have broad powers to adopt measures specifying many of the obligations of providers in relation to high-risk AI systems as well as powers to amend the requirements for the technical documentation, the conformity assessment process and the conformity declaration in relation to high-risk AI systems.

Importers will, among other things, be required to ensure that the provider has carried out the required conformity assessment and drawn up the required technical documentation and to ensure that the software bears the correct conformity marking and is accompanied by the required documentation.. Distributors will be responsible, among other things, for checking that the software carries the required conformity markings and is accompanied by the required documentation and ensuring that the provider and importer have complied with their obligations.

Is there any special treatment for financial sector firms?

EU financial sector firms are already subject to requirements under EU and national financial services legislation that regulate their use of AI. For example, EU banks and investment firms are subject to extensive prudential requirements on corporate governance, systems and controls, risk management, operational resilience, outsourcing and cyber-security, as well as requirements on product governance, conflicts of interest and the protection of customer interests.

The AI Act only recognises that EU financial sector firms are already subject to EU financial services legislation to a limited extent. It includes provisions deeming compliance by EU credit institutions with existing EU regulatory obligations as sufficient for compliance with only a few of the specific obligations under the AI Act, but these provisions do not apply to other financial sector firms or service companies or other members of a group which include a credit institution. It also provides that credit institutions must comply with certain obligations under the AI Act as part of their compliance with their existing governance and risk management obligations under EU legislation.

The AI Act designates EU firms' existing supervisors under EU financial services legislation as the relevant surveillance authorities for the purposes of the AI Act (this may, at least for some purposes, include the European Central Bank in relation to the supervision of banks under the single supervisory mechanism). However, other surveillance authorities designated by Member States will have powers over non-EU or unregulated companies in a financial sector group where these are subject to obligations under the AI Act. The AI Act will require national supervisors that have created 'regulatory sandboxes' to facilitate the development, testing and validation of AI systems within the 'sandbox' under arrangements to be adopted by the Commission.

Other EU sectoral supervisors also have parallel initiatives on AI. Following a 2018 joint report by the European Supervisory Authorities on big data, the European Banking Authority published a report in January 2021 on the use of big data and advanced analytics, including machine learning, in the banking industry with recommendations on how to improve consumer trust. A consultative expert group of the European Insurance and Occupational Pensions Authority published a report in August 2021 on AI governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector, proposing improvements in transparency and explainability to address possible risks to the fair treatment of customers and improvements in governance of AI to safeguard its sound use.

> **"The AI Act only recognises that EU financial sector firms are already subject to EU financial services legislation to a limited extent."**

Will firms have obligations under EU market surveillance legislation?

The AI Act will extend the application of the 2019 EU regulation on market surveillance and compliance of products. Where products are subject to specified EU harmonisation regulation, the 2019 regulation prohibits the commercial supply of those product for distribution, consumption or use in the EU (for payment or free of charge) unless there is an 'economic operator' established in EU that is responsible for the performance of the following tasks:

- where the EU legislation provides for an EU declaration of conformity or performance and technical documentation, verifying that the declaration and documentation have been drawn up and keeping them at the disposal of the surveillance authority so that they can be produced on request;
- providing the surveillance authority, on request, with information and documentation needed to demonstrate the conformity of the product (in a language the authority can easily understand);
- informing the surveillance authority where the economic operator has reason to believe that the product presents a risk to health and safety, protection of consumers, the environment, public security or other public interests protected by the relevant EU legislation;
- cooperating with the surveillance authorities, including taking corrective action on request to remedy non-compliance with EU legislation or, if that is not possible, action to mitigate the risks when required to do so by the authorities or at the operator's own initiative.

The name, registered trade name or mark and contact details (including a postal address) of the relevant economic operator must be indicated on the product or its packaging, parcel or accompanying document. Economic operators must also cooperate with the surveillance authorities on actions that could eliminate or mitigate risks presented by the products they supply.

The AI Act states that for the purposes of the effective enforcement of the AI Act, references to a product and an economic operator in the 2019 regulation shall include all AI systems within the scope of the AI Act and users, providers, appointed representatives, importers and distributors identified for the purposes of the obligations applicable to high-risk AI systems. The latter suggests that these obligations may be limited to the supply of high-risk AI systems and may not apply to other AI systems falling within the scope of the AI Act.

How will the AI Act apply in relation to existing software?

The AI Act will not apply to high-risk AI systems that are placed on the market or put into service before the date of application of the AI Act (two years after it becomes law) unless they are subsequently subject to significant changes in their design or intended purpose. However, users and providers may need to comply with the transparency obligations under the AI Act in relation to existing software and the prohibitions on the deployment of existing prohibited AI systems will apply from the date of the application of the AI Act.

What will be the powers of the surveillance authorities?

Surveillance authorities designated under the AI Act will have wide powers in relation to software that is subject to requirements under the AI Act, including high-risk AI systems and software subject to transparency requirements. They will have the power to obtain full access to the provider's training, validation and testing datasets, including through application programming interfaces or other appropriate technical means and tools enabling remote access (and access to the source code of high-risk AI systems). They will also be able to require access to any documentation created or maintained under the AI Act. Firms will need to consider how to manage the privacy and cyber-security risks of providing this access.

Where an AI system presents a risk to health or safety or fundamental rights, the surveillance authorities will be able to investigate compliance with the requirements of the AI Act and require corrective action (including recall of the system), failing which they may prohibit or restrict the supply of the software (or require its withdrawal or recall). Even if they find that the AI system is compliant with the AI Act, they may still require the taking of appropriate measures to prevent a risk to health and safety or fundamental rights.

The extension of the 2019 EU regulation on market surveillance of products to all AI systems within the scope of the AI Act will also give the surveillance authorities powers to require users, providers, appointed representatives, importers and distributors identified for the purposes of the obligations applicable to high-risk AI systems to provide access to documents and information, to cooperate with investigations and to take corrective action.

What are the penalties for non-compliance?

Member States must create penalty regimes imposing significant administrative fines on firms that do not comply with the AI Act.

Contravention	Administrative fines (up to the higher of)
Non-compliance with the prohibition on the deployment of prohibited AI systems and the data and data governance requirements for high-risk AI systems.	• €30,000,000 or • 6% of total global annual turnover.
Non-compliance with other requirements of the AI Act.	• €20,000,000 or • 4% of total global annual turnover.
Providing incorrect, incomplete or misleading information in response to requests from assessment bodies or national authorities.	• €10,000,000 or • 2% of total global annual turnover.

Persons suffering loss as a result of a contravention of the AI Act may have rights to seek damages under general principles of EU law. There have also been calls to create collective redress mechanisms for consumers in relation to contraventions.

> “Firms will be subject to fines of up to 6% of global turnover for contraventions.”

What actions should firms take now?

Financial sector firms will face significant challenges in complying with the requirements of the AI Act and firms should begin to organise their response even though the regulation is likely to be further amended during the legislative process (which might restrict or expand the obligations applicable to the firm). This may involve a preliminary assessment to determine where the AI Act might impose obligations on the firm and other members of its group (and entities such as investment funds managed by the firm and securitisation and other special entities sponsored or used by the firm) and how compliance might be achieved. Firms will also need to consider how the new rules will interact with other existing and planned sectoral and cross-sectoral regulatory requirements, including their obligations under the EU General Data Protection Regulation. Firms may also wish to monitor the legislative process of the AI Act and make appropriate representations through industry associations or otherwise on key issues. In any event, the scale of the potential penalties means that implementing AI governance and compliance should be a priority for boards.

> “The scale of the potential penalties means that implementing AI governance and compliance should be a priority for boards.”

Box 3: Obligations in relation to 'high-risk AI systems'

Users	
Operation and records	Users must: • use the software in accordance with the user instructions • ensure that input data is relevant to the software's intended purpose • use information provided by the provider to comply with the users' data protection impact assessment obligations • retain logs automatically generated by the software.*
Monitoring	Users must: • monitor the operation of the software on the basis of the instructions;† • inform the provider or distributor when they identify any serious incident or malfunction (and interrupt the use of the software).
Transparency	Users must inform natural persons that the software uses emotion recognition or biometric categorisation and inform exposed persons that 'deep fake' content has been artificially generated or manipulated.
Providers	
Systems	Providers must establish or ensure the establishment of prescribed systems for: • risk management* • quality management† • post-market monitoring.
Software development and design	Providers must ensure that the software is designed and developed: • using data sets meeting prescribed criteria for any training of the system • to automatically log events while operating • so that its operation is sufficiently transparent to users and is accompanied by instructions for use • so that it can be effectively overseen by natural persons while in use • to achieve appropriate levels of accuracy, robustness and cybersecurity and to be resilient to errors, faults or inconsistencies and hacking • so that natural persons interacting with the software are aware that they are dealing with an 'AI system'.
Documentation and records	Before marketing or use, providers must prepare prescribed technical documentation (and keep it up-to-date). Providers must retain logs automatically generated by the software.*
Conformity assessment and registration	Before marketing or use, providers must assess the software's conformity with the AI Act (in relation to biometric systems, this may requirement involving an official assessment body), make a declaration of EU conformity and register the software on the publicly-available Commission database (including the identification of the software, a description of its purpose, a copy of the declaration or certificate of conformity and electronic instructions for use).*
Demonstrating conformity	Providers must, on request, provide information to the authorities to demonstrate the software's conformity with the Regulation.
EU representative	Non-EU providers must appoint an EU authorised representative before marketing the software or making it available for use in the EU (unless an importer can be identified).
Reporting	Providers must report serious incidents and any malfunctions breaching EU obligations on fundamental rights to the authorities (within 15 days).

Corrective action	Where the software does not conform to the AI Act, providers must take corrective action including notifying other operators, authorities or withdrawing or recalling the software.
Supervisory access	Providers must grant surveillance authorities remote access to training, validation and testing datasets and access to source codes.
Importers	
Conformity and documentation	Importers must, before marketing, ensure that: • the provider has carried out the conformity assessment and drawn up the required technical documentation • the software bears the required conformity marking and is accompanied by the required documentation and instructions • the software is brought into conformity with the AI Act if they have reason to consider that the software is not already in conformity Importers must include their name, trademark and contact details on the software or its packaging or documentation and ensure that storage and transport of the software does not jeopardise its conformity to requirements. Importers must, on request, provide information to the authorities to demonstrate the software's conformity with the Regulation.
Distributors	
Conformity and documentation	Distributors must, before marketing the software: • verify that it bears the required conformity marking, is accompanied by required documentation and instructions and that the provider and importer have complied with their obligations • ensure the software is brought into conformity with the AI Act if they have reason to consider that the software is not already in conformity (and notify the provider and importer) • ensure that storage and transport of the software does not jeopardise its conformity to requirements. Distributors must, on request, provide information to the authorities to demonstrate the software's conformity with the Regulation. Where software does not conform to the AI Act, distributors must take corrective action including notifying other operators, authorities or withdrawing or recalling the software.
Users, providers, importers and distributors	
Reporting and supervision	Where software creates risk to health or safety or the protection of fundamental rights, users, providers, importers and distributors must notify other operators and surveillance authorities, cooperate with the authorities and take corrective action. Surveillance authorities can require access to documentation created or maintained under the Regulation.
Economic operator obligations	Users, providers, importers and distributors must comply with the obligations under the 2019 EU regulation on market surveillance and compliance of products as it applies to AI systems.

* Indicates that EU credit institutions must comply with some obligations as part of their obligations under the capital requirements directive.

† Indicates that EU credit institutions may be deemed to have fulfilled some obligations by complying with obligations under the capital requirements directive.

CONTACTS

Caroline Dawson
Partner
London
T: +44 207006 4355
E: caroline.dawson@
cliffordchance.com

Kate Scott
Partner
London
T: +44 207006 4442
E: kate.scott@
cliffordchance.com

Chris Bates
Special Counsel,
Consultant
London
T: +44 207006 1041
E: chris.bates@
cliffordchance.com

Marc Benzler
Partner
Frankfurt
T: +49 69 7199 3304
E: marc.benzler@
cliffordchance.com

Anna Biała
Counsel
Warsaw
T: +48 22429 9692
E: anna.biala@
cliffordchance.com

Lucio Bonavitacola
Partner
Italy
T: +39 02 8063 4238
E: lucio.bonavitacola@
cliffordchance.com

José Manuel Cuenca
Partner
Madrid
T: +34 91 590 7535
E: josemanuel.cuenca@
cliffordchance.com

Lounia Czupper
Partner
Brussels
T: +32 2 533 5987
E: lounia.czupper@
cliffordchance.com

Monica Freely
Senior Associate
London
T: +44 207006 2322
E: monica.freely@
cliffordchance.com

Steve Jacoby
Managing Partner
Luxembourg
T: +352 48 50 50 219
E: steve.jacoby@
cliffordchance.com

Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@
cliffordchance.com

Frédérick Lacroix
Partner
Paris
T: +33 1 4405 5241
E: frederick.lacroix@
cliffordchance.com

Jurgen van der Meer
Partner
Amsterdam
T: +31 20 711 9340
E: jurgen.vandermeer@
cliffordchance.com

Gail Orton
Head of EU
Public Policy
Paris
T: +33 1 4405 2429
E: gail.orton@
cliffordchance.com

Joshua Price
Senior Associate
Knowledge Lawyer
London
T: +44 207006 3267
E: joshua.price@
cliffordchance.com

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@
cliffordchance.com

CLIFFORD
CHANCE

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.