European Union Artificial Intelligence Act

Before the dust settles

How financial services are likely to take a sustainable approach to EU AI Act compliance in a new era for trustworthy AI, ahead of entry into force

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

This report was prepared by Sean Donald John Musch and Michael Charles Borrelli. For more information visit https://www.ai-and-partners.com/.

Moreover, for information on future publications, register your interest for TransformBase 2024, the leading event focused on enterprise adoption of and investment into AI. Join us on 27th June for a key regulatory roundtable moderated by AI & Partners. Discover more and secure your tickets upon their release here.

Contact: Michael Charles Borrelli | Co-CEO/COO | m.borrelli@ai-and-partners.com.

This report is an AI & Partners publication.

Our report finds that financial services companies will, in all likelihood, find it easier to comply with EU AI Act than companies in other sectors because of their long history of meeting strict consumer protection, prudential obligations, and data protection requirements set by financial regulators.

About this report

This report is based on market research, publicly available data, and interviews with AI specialists in AI & Partners, financial services organisations, and relevant third-parties. Moreover, quotations provided on specific topics reflect those of AI specialists at AI & Partners to be as representative as possible of real-world conditions. All references to EU AI Act reflect the version of text valid as at 2 February 2024. Accessible here.

Contents

Executive Summary

The European Union's ("EU") Artificial Intelligence ("AI") Act ("EU AI Act"), which looks set to enter into force during April 2024, regulates how organisations use, develop, deploy, and market AI in the EU. It improves the safety, security, and trustworthiness of AI systems and, among other things, requires organisations to implement risk management systems for high-risk AI systems. It can be difficult and costly to comply with. Penalties for non-compliance can be as high as €35m or 7% of annual global turnover, whichever is higher.

The regulation is set to be supervised and enforced by the national competent authorities ("NCAs") in each member state. The European Data Protection Board ("EDPB"), which is made up of representatives from each EU Member State, AI Office ("AIO"), the European Data Protection Supervisor ("EDPS"), and others ensures that EU AI Act will be applied consistently throughout the EU.

Overview

This report looks at how EU AI Act may affect financial services companies and their personal customers in its first year of operation. It is a prelude to AI & Partners' surveys on EU AI Act implementation, which look at the impact of EU AI Act on companies and their customers in all sectors of the economy.

This new report finds that, in general, financial services companies are likely to take it in their stride than companies in other sectors. This is because they have a long history of complying with strict consumer protection, prudential obligations, and data protection requirements set by financial regulators. Their strategic approach and detailed procedures are therefore likely to be more mature than those of firms in other sectors.

Compliance challenges

Despite generally being better prepared than firms in other sectors, financial firms are likely to find EU AI Act compliance a challenge, because of its broad scope – affecting as it does so many departments, IT systems, and people – and the severe penalties for getting it wrong.

Particular areas of potential difficulty include managing AI system inventories, consolidating vast amounts of AI systems into centralised pools, and complying with the way that EU AI Act has been interpreted in different ways by some EU member states.

High-risk AI system breaches, regulatory enforcement and legal action

There have been no confirmed major AI system breaches by financial services firms pre-April 2024. However, there are likely to be complaints to national NCAs about alleged breaches of EU AI Act by firms in various industries. It is only a matter of time before financial services companies start to fall foul of the regulation and receive large fines. Class action lawsuits may also follow from groups of disgruntled customers.

Impact on business operations and commercial success

In some cases trustworthy AI measures may become so restrictive that they impede the operational effectiveness and revenue generating capabilities of businesses. Fortunately, this is likely to be less of a problem for financial institutions than for other types of businesses. However, fears on how it stifles innovation in AI system deployment by financial institutions, such as their use of emerging forms of AI.

Executive management and board scrutiny

Executive management and supervisory boards in the financial sector tend to be better at monitoring their AI policies and EU AI Act compliance procedures than their counterparts in other industries. This is because their organisations have evolved over decades to meet the strict requirements of a heavily regulated sector, where huge fines can be imposed on those that transgress. National regulators may, however, have some concerns that executive management and boards in financial services companies may not fully understand their AI compliance obligations and that their approach will be simplistic, with a focus on "tick-box" compliance with EU AI Act.

Consumer awareness

Financial services consumers are much more aware of their AI rights now than they were under the previous EU rules. Many financial services companies are likely to witness large volumes of "A right to explanation of individual decision-making" ("RtE") when EU AI Act enters into force.

Recruiting specialist staff and training non-specialist staff

EU AI Act may create a huge demand for specialist staff, so much so that financial institutions struggle to meet their recruitment targets. This has been a particular challenge for the biggest companies which have had to appoint a AI officer. Non-AI specialists dealing with AI systems – such as customer relationship managers, marketing managers, sales managers and telesales operatives – will have to be trained in the basics of EU AI Act compliance and regularly reminded about the procedures and guidelines to follow. There is often a gap between what the AI professionals understand about AI systems and what customer-facing employees understand.

Technology-assisted EU AI Act compliance

Technology plays an important role in safeguarding AI. If respondents are asked if they had invested in tools and technology to help them in areas of EU AI Act compliance, responses are likely to show relatively high levels of investment. Even so, there is scope for much more investment in technology-based compliance tools.

Has it all been worth it? And what's next?

Despite the high envisaged costs of complying with EU AI Act, the consensus is that a cost-benefit analysis would show the benefits to organisations are higher. If respondents are asked to rate the importance of drivers for EU AI Act compliance, they are likely to attach more importance to positive drivers, such as improving customer trust, increasing AI system efficiency, enabling an insight driven organisation, than to negative drivers such as the threat of regulatory fines. So it has been worth it for financial services companies, even before considering the benefits to customers. As for the future, organisations should strive for a "trustworthy AI by design" approach, while recognising that there is no such thing as a perfect state of compliance. It is a constant process – the job is never finished.

1. Overview – the impact of EU AI Act on financial services firms and consumers

This report looks at how the EU AI Act will affect financial services companies and their personal customers when it enters into force during April 2024.

The financial services sector – a long tradition of compliance with data rules

What qualitative assessments can be made about the potential effect of EU AI Act on the financial sector compared with other industries? The consensus is that, in general, financial services companies are likely to take it in their stride. This is because they have a long history of complying with strict consumer protection, prudential obligations, and data protection requirements rules set by financial regulators. Their strategic approach and detailed procedures are therefore likely to be more mature than those of companies in other sectors.

Close monitoring by supervisors over the years has meant that banks, insurers, asset managers and other financial institutions are well attuned to the culture of risk management and compliance with analogous regulations. Core structures have been in place for some time, so the effort needed to comply with EU AI Act will be modest and incremental rather than huge and sudden.

By contrast, non-financial services companies – those in retail, media or technology for example – are generally less mature in their approach to AI. Some may start from scratch with their EU AI Act compliance programmes, as they did not have a trustworthy AI framework in place or a culture of trustworthy AI by design.

Financial services sub-sectors

There are some differences in how various sub-sectors of the financial services industry may adjust to EU AI Act requirements. Retail banks, for example, can adapt well, having traditionally invested heavily in compliance with previous AI laws due to the nature of their business and the fact that they use a vast number of AI systems. They are also used to being scrutinised by their regulators, much more so than companies in other industries.

Retail banks and insurance companies typically use AI systems for multiple business activities in case it is needed in the future. EU AI Act stipulates that businesses must apply risk management requirements for high-risk AI systems. So to comply with EU AI Act's requirements, banks must change their mind-sets and review their AI deployment processes and policies. Banks' capital markets businesses conduct large business using AI systems. They therefore utilise high volumes of AI systems and are likely to be heavily impacted by EU AI Act. They may find it difficult to comply because the size of the task is great.

However, there is also evidence of a potentially relaxed approach to EU AI Act compliance by some US capital markets firms. US AI standards have traditionally been lower than Western Europe's, especially Germany's. A cultural shift is needed if US firms are to match the standards of their European peers.

EU AI Act may have a big impact on the investment management sector compared to the retail banking and insurance sectors because many investment management businesses operate mainly, or only, on a business-to-business ("B2B") basis, rather than on a business-to-consumer ("B2C") basis, and therefore use AI systems extensively. Wealth management firms may make good progress in implementing processes for handling the expected requirements and have few problems in dealing with them, as they are not a new concept.

A mature approach to managing compliance risk

Financial services have for a long time followed the tried-and-tested three lines of defence approach to compliance risk management: the first line being management control of frontline operations; the second being the risk management and compliance oversight functions; and the third being internal audit. The AI Officer ("AIO") in a bank or other financial institution sits clearly in the second line of defence. This mature approach to managing AI risk is less common, or non-existent, in other industries.

The size of the fines levied in the recent past by financial regulators on firms that broke analogous regulations, such as the General Data Protection Regulation ("GDPR") is another factor that has focused minds. It also ensures that EU AI Act may not be as big a shock to financial services executives as it has been to executives in other industries. When an insurance professional uses a low-risk AI system without authorisation and the employer gets hit with a fine, the likelihood of the same thing happening again in the future diminishes. Many lessons have already been learned about the importance of protecting AI.

"The EU AI Act will be a key priority for banks. To comply with its implementation, they will have to make adjustments to their technical tools and contracts, and train their personnel. Trust will remain crucial for banks, especially in their relationships with customers. While banks may not be as trusted as they once were due to past financial crises, they are still considered reliable stewards of data. Any breaches of data security would severely damage their reputation and client relationships."

"However, the impact may be less dramatic in the financial sector compared to other industries, as financial services firms are accustomed to dealing with extensive regulation. For organizations outside the financial sector, adapting to such a groundbreaking regulation will be a new experience, potentially causing greater shock."

"Systems involving a degree of automation and minimal or limited human intervention, such as general purpose AI systems, will be considered AI systems under the EU AI Act. Even though business banks may not face close regulatory scrutiny, they must still prioritize the trustworthiness of the AI systems they deploy."

"Banks will take the EU AI Act seriously and implement meaningful changes to their controls and processes. The focus will then shift to ensuring these changes are integrated into business operations seamlessly, with accountability and effective oversight across all levels of defence. Merely publishing new policies and procedures will not suffice; they must be embedded within a comprehensive accountability framework and operating model to ensure long-term effectiveness."

2. Compliance challenges

Despite potentially being better prepared than firms in other sectors, financial firms may find EU AI Act compliance a challenge, because of its broad scope– affecting as it does so many departments, IT systems, and people – and the severe penalties for getting it wrong. So where are they likely to do well? What are less likely to do well, and where are they likely to come across difficulties - what can they do to improve?

Challenges well met

What they have done well, and have done so for years before EU AI Act looks to enter into force, is instilling a culture of compliance. Financial services firms are used to operating within a broad compliance risk management framework, into which AI can likely be slotted. That is not to say it has been easy. It has still been a challenge to get it right in many cases because of the complexity of their systems covering multiple countries and the volume of AI systems used and/or deployed through those systems in multiple countries.

No matter how good your compliance framework is, there is a lot of AI systems to manage and that is not a simple task. EU AI Act requires companies to be more proactive in demonstrating compliance, as opposed to reactively answering questions from the regulator, and this is something that financial firms do well compared with firms in less regulated or unregulated sectors.

AI system collection and analysis requires new and effective ways of using technology, much of it innovative. It requires automation; it may use advanced forms of AI, e.g. symbolic reasoning, to analyse the AI systems; and it requires broad AI system information sharing. All of these uses of technology must comply with EU AI Act, which is something that financial firms are largely able to manage. They are doing well on demonstrating accountability of board directors and executive managers. They are doing well on staff training and awareness. Financial services are used to the constant introduction of new regulations and all the training that goes with it.

Communicating AI system information (e.g. transparency) to customers is a key requirement of EU AI Act. Organisations must be forthcoming with customers about the information they collect and hold on them, tell them why they hold it, and what they do with it. Financial firms have had to do this for years, and so have had little difficulty with the new rules. In the months, weeks and even days leading up to EU AI Act, a flurry of AI notices from non-financial services are likely to clog up customers' email in-boxes.

These firms may not have properly prepared for EU AI Act, or had even been breaking the previous analogous rules; by contrast, very few, if any, such notices were sent out by financial services firms at the last minute because they had been meeting this requirement for years.

Under EU AI Act, businesses can only deploy high-risk AI systems under certain conditions to ensure the deployment is safe, secure, and lawful. These include, for example, conducting a fundamental rights impact assessment ("FRIA"), establishing a risk management system,

Challenges harder to meet

There are likely to be pressure points for financial services firms. It will be far from easy. What many may find hard to get a grip on is managing their AI system asset inventories. Using the United Kingdom's ("UK") Information Commissioner's Office ("ICO") Guidance[1] as a reference, AI & Partners outlines steps for firms to achieve EU AI Act compliance: organisations should document the AI systems they use, where they are used, and who uses them. An AI system audit may be necessary to ensure that AI system inventories are accurate and up to date.

Knowing where all these AI systems reside is a huge task for firms, especially for large organisations that have grown through acquisition and have complicated and creaking legacy systems. Consolidating vast amounts of AI systems into a centralised pool would make inventory management easier, but such a task is itself a challenge.

In addition to complying with our legal or contractual obligations, we will primarily rely on legitimate interests to process our clients' personal data under the EU AI Act, particularly in a business-to-business context. However, in some cases, we will also utilize consent where it is the most appropriate legal basis for the processing.

"They will be keen to ensure accountability and have the right policies and procedures in place, including fundamental rights impact assessments, and managing requests for an explanation of individual decision-making."

"Banks will take it seriously,"

"They will have a lot of industry discussions about it and be thoughtful about the meaningful changes they need to make."

"At the heart of all of this will be the individual. Compliance strategies under the EU AI Act will need to be client-centric and employee-centric to guard against 'tick-box compliance'. Banks will generally ensure they have executive sponsorship, making trustworthy AI a board-level agenda item."

"Any organization with a retail element will have a lot of AI systems, and we will have huge volumes of data being processed by those AI systems for use in producing outputs, such as predictions, and recommendations."

"The banking sector will receive more requests in regards to the right to explanation of individual decision-making than any other, especially when considering those from credit scoring claims. So losing 10 days off the cycle will be hugely impactful."

"*Banks will be regularly in touch with them at the national level. It will, however, be important to keep in mind that ahead of the implementation of the EU AI Act and even before, because trustworthy AI will be a horizontal and cross-sector issue, some national competent authorities might find it difficult to deal with the increasing number of queries coming from consumers, SMEs, industry, etc. Their resources will remain limited and they will certainly be overwhelmed with requests for advice or information*."

[1] Information Commissioner's Office, (2014), 'Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now', accessible at https://ico.org.uk/media/2014146/gdpr-12-steps-infographic-201705.pdf (last accessed 17th February 2024)

3. AI System Breaches, regulatory enforcement and legal action

To date, as far as we know, there have been no confirmed major AI system breaches by financial services firms ahead of EU AI Act's entry into force in April 2024. However, there may be complaints made to national competent authorities about potential breaches of EU AI Act by firms in various industries.

It is surely only a matter of time before major EU AI Act breaches in the financial sector are confirmed, in which case large fines are likely to follow. The question is, how close to the maximum penalty – €35m or 7% of global annual turnover, whichever is higher – will those fines be? It would be surprising if any NCA pushed for the 7% turnover level for large financial institutions, considering the size of their turnovers, but we can expect the fines to be much higher than in the past.

Under the GDPR, an analogous regulation in terms of, for example, extra-territoriality, national data protection authorities previously had fining powers, but they were small. Some EU data regulators previously had no powers to fine. Now, with an emerging, transformative technology in the form of AI to oversee and supervise, they have been given teeth, they can be expected to use them.

Although national financial regulators and NCAs will liaise closely on the imposition of fines, they do have separate powers. So it is possible that a local authority could levy a 7% of global turnover fine on a firm, and the local financial regulator another fine of similar magnitude – a "double whammy". Post-Brexit, a transgressor could face a "triple whammy" if the breach affected UK and EU citizens: a fine from an EU NCA, one from a UK regulator, such as the Financial Conduct Authority ("FCA"), and one from the UK's ICO under a national AI bill, which implements EU AI Act in that country. It must be stated though that such scenarios are unlikely, with national regulators and authorities co-ordinating their responses to reduce the risk of extreme outcomes.

The biggest fines are more likely to be imposed on software development and big technology companies. EU and national authorities have already fined these types of firms for breaking previous data protection laws, as well as for breaking existing anti-trust laws. Given the nexus between data and AI systems (i.e. data is oil, AI system is the combustion engine), future similar transgressions will result in much bigger fines.

Banks, insurers, and investment managers on the other hand are likely to be much more compliant. Although they are likely to use a great deal of AI systems, they already have established risk management frameworks, processes and procedures, so the risk of non-compliance and large fines is lower.

Class action law suits

In addition to regulatory enforcement and fines, companies also risk class action law suits from consumers demanding significant compensation in the event of major breaches. These can be difficult to defend. Several such class actions may start against major European companies once the EU AI Act enters into force in April 2024, though they are not in the financial sector.

It will only be a matter of time before cases start to be brought against financial firms, but the higher standards in the financial sector is keeping the safe for the time being. It will be instructive to see where such actions lead, how they progress through the courts, how much of a battle there will be, and where the courts settle on the impact of the breaches on individuals.

The key question a court will ask a company is, did it do enough to protect its customers' from the potential harms caused by AI systems? The court may accept that there is no such thing as perfect security, but it will want to know if a company's AI policies and processes were adequate to prevent most breaches and how well it responded after a breach to minimise the negative impact on individuals. If it finds the company lacking, the penalties are likely to be high. Compensation for each individual may be small, but added up across thousands, or hundreds of thousands, of plaintiffs the total would be far higher

The potential class actions that can be brought may take another 12-18 months to complete, and when they do they will set precedents for the level of liability companies are expected to shoulder. In addition to class actions from consumers, there is also the risk of legal action from individual corporate customers. If a direct marketing company, for example, deploys an unacceptable risk AI system for use with clients, it could allege breach of contract.

Reputational damage

The costs of an AI system breach are not limited to the legal costs of defending regulatory and legal actions, and the fines and compensation paid out when such actions are lost. There is also the reputational damage to consider. This can be serious, albeit impossible to quantify. It includes loss of brand value, loss of customer trust, reduced revenues and profits and a falling share price.

The cost of the damage will vary depending on the organisation, the elasticity of supply and demand, and customer relationships. If, for example, a bank suffers a major AI system breach but it has a strong brand, provides excellent services that are difficult for other banks to match and it has built up high levels of customer trust and loyalty, then the reputational damage is unlikely to prove costly. If, on the other hand, it is a bank that is weak in these key areas, then the reputational damage can be much more financially damaging.

For example, customer trust was an important feature of Deloitte's 2018 survey[2] GDPR six months on, in the questions asked of both organisations and consumers. In their responses, 25% of consumers – in all sectors, not just financial services – said their trust in an organisation would decrease if it suffered a data compromise, and 17% said they would stop using its services or buying its products. In this sense, a similar sentiment applies.

"Their likely approach is, in relation to compliance, do I have a defendable position? They may not be able to guarantee that they have got everything 100% right, but if they have tried hard to comply they have a position that is defendable. Regulators will punish those who don't care or are not trying, but not those who are trying to get it right and have just missed something."

[2] Deloitte, (2019), 'After the dust settles How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on.', accessible at https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-the-impact-of-gdpr-on-the-financial-services.pdf (last accessed 17th February 2024)

4. Impact on business operations and commercial success

It is one thing to comply with EU AI Act and avoid, or at least minimise, all the risks highlighted in the previous chapters. It is quite a different thing to ensure that trustworthy AI measures do not become so restrictive that they seriously impede the operational effectiveness and revenue generating capabilities of the business.

These particular obstacles can be less of a problem for financial institutions than for other types of businesses. Multiple banks, insurers and investment managers only target consumers who are more likely to want to buy their services, which means those services are more demand-led, so the return on investment in marketing is already quite high.

In comparison, software development, and big technology companies and others target consumers who are more likely to have to be sold services and products. Their services tend to be more supply-led, so direct marketing is a large overhead that produces a relatively low return. Moreover, financial services firms have largely included “trustworthy by design” principles in their AI system design, data, and models; verification and validation; deployment; and operation and monitoring. Adjusting to EU AI Act therefore potentially creates little or no impediment to their AI system-related business operations.

"*They will promote the right kind of conversations and sometimes save organizations from themselves. The more sophisticated firms will have moved on many years ago, to be fair, from contacting large numbers of people, to now seeking quality leads and conversations that generate trust, and subsequently revenue. The gap between software development and compliance will be much smaller than people originally envisaged before the EU AI Act comes into effect*."

5. Executive management and board scrutiny

Executive managements and supervisory boards in the financial sector are likely to be better at monitoring their AI system policies and EU AI Act compliance procedures than their counterparts in other industries. This is because their organisations have evolved over decades to meet the strict requirements of a heavily regulated sector, where huge fines can be imposed on those that transgress.

In the UK, the introduction by the FCA of the Senior Manager's Regime – for banks and certain investment firms in 2016 and other financial institutions in December 2018 and December 2019 – energised minds even more. The regime requires senior managers and directors to be individually more responsible and accountable for their actions, including compliance with all applicable laws and regulations.

Every senior manager needs to have a "statement of responsibilities" that clearly outlines what they are responsible and accountable for, some of which are prescribed. At least annually, firms need to certify that their senior managers are suitable for their jobs.

When EU AI Act enters into force, it will add yet another layer of responsibility and risk for senior managers in the UK financial services industry, and consequently reviews and internal audits to keep tabs on things. The most advanced companies are likely to create dashboards and metrics for business leaders. At the moment they are likely operating in a business-as-usual environment. It is possible they have developed a false sense of security, believing they are doing everything right, because the regulators have not become active. We are most likely in the archetypal lull before the storm.

When breaches start happening, the regulators take notice and class actions start commencing, that will be the real test of whether executive managers have been in full control and whether board directors can demonstrate they have been able to provide high-quality, independent oversight and constructive challenge to the executive.

6. Consumer awareness

There is little doubt that financial services consumers are much more aware of their AI obligations rights under EU AI Act than they were under the previous EU rules that were introduced beforehand, and under indirectly applicable national rules.

Publicly available data, such as that from appliedAI Initiative GmbH[3], shows that across all industry sectors, not just financial services, the majority of individuals surveyed are unaware of the key rights they have under the regulation – and this mainly focuses on the impact of EU AI Act on start-ups in Europe, rather than consumer awareness. They may know about the right to receive clear and understandable information about who is deploying AI systems, what AI systems are being deployed and why; the right to lodge a complaint with a market surveillance authority (Art. 68b)[4]; the right to explanation of individual decision-making (Art. 68c); and more.

"Financial institutions are likely to see more engagement from their customers about this. At the same time, we still think more needs to be done to explain EU AI Act to customers and to improve general AI literacy. There is still a lot of mistrust of new technology and innovation. That mistrust will hamper innovation if people chose not to engage with the clever technology out there."

[3] appliedAI Initiative GmbH, (2022), 'AI Act Impact Survey: Exploring the impact of the AI Act on Startups in Europe', accessible at https://aai.frb.io/assets/files/AI-Act-Impact-Survey_Report_Dec12.2022.pdf (last accessed 17th February 2024)
[4] European Parliament, (2024), 'Proposal for a regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts 2021/0106(COD) (COM(2021)0206 – C9-0146(2021) – 2021/0106(COD))', accessible at https://www.ai-and-partners.com/_files/ugd/2984b2_d973c1fc464740da9985c5de8fbe97bb.pdf (last accessed 17th February 2024)

7. Recruiting specialist staff and training non-specialist staff

EU AI Act is likely to create such an unprecedented demand for specialist staff that many companies may struggle to meet their recruitment targets. The largest may have to take on AI officers, AI governance managers, and other senior EU AI Act-focused staff to play dedicated roles. Whilst smaller firms have not needed to create specific roles, they have needed to allocate the responsibilities of trustworthy AI to a specified legal or compliance expert to take on these responsibilities as part of a wider role.

Banks, investment managers and other financial firms with larger financial resources than most firms in other sectors, and therefore the ability to offer attractive salaries and employment conditions, may find it easier to take on senior AI professionals. However, for the next tiers down – middle ranking and junior positions – it will likely be more difficult. This is because the talent pool of people who understand trustworthy AI by design principles and EU AI Act compliance is probably small. People in those lower reaches have been snapped up by organisations for senior roles, leaving the pool depleted so that even global banks dangling enticing bait have been left with small catches.

Non-specialists

As for staff who are not AI specialists who work outside the AI systems, legal and compliance departments (such as customer relationship managers, marketing managers, sales managers and telesales operatives), will have to be trained in the basics of EU AI Act compliance and regularly reminded about the procedures and guidelines to follow.

AI professionals in financial firms may get better at communicating to staff what trustworthy AI means and why it's important, but it will not be perfect. There is often a gap between what the professionals understand about the subject and complying with trustworthy AI rules, and what frontline, customer-facing employees understand.

Financial institutions generally had well-resourced training programmes for all kinds of legal and regulatory compliance requirements, including trustworthy AI. They know how to train staff, and then test, evaluate and monitor its effectiveness. All they had to do in preparation for EU AI Act is to update and expand existing training initiatives.

"It is also true that because of a long tradition of looking after technology, and because many European countries already operated under strict laws, a lot of in-house knowledge has been built up in banks so they can rely on such expertise within the organisation,"

"Banks can rely on their staff to understand their AI policies, but because they are so busy doing our day-to-day jobs, it's likely the right training has not been provided to the right people in every case,"

"Knowing where AI systems are and what they are doing with it can be difficult. The business people who know where it is and are using it may not be paying enough attention to AI governance, and therefore may not be telling the AI people all they should be telling them."

8. Technology-assisted EU AI Act compliance

Technology plays an important role in safeguarding AI systems. Risk classifications, which help companies identify, manage and monitor regulatory risks under EU AI Act, are an integral part of a trustworthy AI by design approach.

A large number of solution vendors – long-established ones and start-ups – are likely to offer online and offline risk classification tools that can be tailored to each company's requirements to provide compliance monitoring and oversight, ensuring all processes are adhered to. Other solutions may be available for AI system inventory management, unstructured AI system scanning, algorithm compliance, fundamental rights impact assessments ("FRIA") and high-risk AI system post-market monitoring.

These solutions may not always used as well as they can be by financial institutions. There may be a proliferation of new offerings from existing vendors and new entrants, who will spend a great deal of money on marketing, which may be confusing. Users need to be clear about the value they hope to get from them before committing. Key areas of potential technology investment are shown below:

- Quality Management Systems: Investments in quality management systems that are specifically designed to ensure AI systems' compliance with the EU AI Act. This includes systems that can integrate with existing quality management requirements under financial services legislation (Art. 2 (Quality management system))[4].
- Internal Governance Technologies: Technologies that support robust internal governance, arrangements, or processes, as financial institutions can fulfil certain obligations under the Act by complying with existing rules on internal governance pursuant to relevant Union financial services legislation (Art. 2 (Quality management system) and Art. 29 (Obligations of deployers of high-risk AI systems))[4].
- Automated Log Management: Solutions for the automated generation, management, and retention of logs produced by high-risk AI systems, ensuring they are kept for at least six months or more, as required by the Act and relevant financial services legislation (Art. 29 (Obligations of deployers of high-risk AI systems))[4].
- Data Protection and Privacy: Technologies that enhance data protection and privacy, especially for high-risk AI systems that process personal data, ensuring compliance with the EU's data protection laws alongside the AI Act's requirements (Art. 29 (Obligations of deployers of high-risk AI systems))[4].
- AI System Monitoring Tools: Tools for the active and systematic post-market monitoring of AI systems, allowing financial institutions to collect, document, and analyse relevant data on the performance of high-risk AI systems throughout their lifecycle (Art. 61 (Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems))[4].
- Compliance and Reporting Software: Software solutions that enable financial institutions to efficiently report to the relevant national authority responsible for financial supervision, ensuring compliance with the Act's market surveillance and control provisions (Art. 63 (Market surveillance and control of AI systems in the Union market))[4].

9. Will it all be worth it? And, what is next?

Ahead of the dust settling, we know a lot more about the potential compliance burden EU AI Act looks set to place on financial firms. It has taken a great deal of management time, financial investment and re-engineering of policies, procedures and technology processes to arrive at the current, high-level state of compliance.

Financial regulators, like regulators in any industry, like to conduct cost-benefit analyses for their new rule-making. Balancing the costs and risks that EU AI Act looks set to place on financial services firms, against the benefits that have accrued to their customers, to what extent will it be worth it for both parties?

Based on the data from Deloitte's GDPR analysis, below are potential quotes retrofitted to EU AI Act.

"The EU AI Act will be an incredibly ambitious piece of legislation. Its objective will be to re-write how the handling of artificial intelligence is regulated in Europe. When you consider how much AI is integrated into personalized services and how every company relies on AI-driven technologies, it will be an incredible thing to attempt in one go, but it will succeed."

"Most financial organizations will be comfortable with the individual elements of the regulation. AI portability will be seen as positive. The right to explanation of individual decision-making will be acknowledged as beneficial. These things will be novel and challenging, but firms will not argue against their existence."

"Your clients will expect you to comply. Your employees will expect you to comply, and to get it right. Potential breaches will bring it into sharp focus and will demonstrate the need for smart regulation in this area,"

"It will benefit society as a whole because it will hold organizations to account, will help to prevent future AI misuses, and will increase transparency. Consumers will have a better understanding of how AI is being used and by whom. As a society, we should continue to carefully manage the balance between responsible regulation, our ability to keep pace with AI advancements, and our continued ability to innovate."

What's next

Looking ahead, what more needs to be done to ensure compliance with EU AI Act, and prepare for similar rules being introduced around the world? "Trustworthy AI by design," or "Security by design" as it is referred to in EU AI Act, is the answer.

Companies [and other] organisations may implement technical and organisational measures, at the earliest stages of the design of the AI system deployment process, in such a way that safeguards AI and trustworthy AI principles right from the start ('trustworthy AI by design'). Here are two potential examples:

- **The use of risk classification** – understanding risks of AI systems prior to deployment

How can we help?

AI & Partners

Amsterdam - London - Singapore

AI & Partners – 'AI That You Can Trust'

Your trusted advisor for EU AI Act Compliance. Unlock the full potential of artificial intelligence while ensuring compliance with the EU AI Act by partnering with AI & Partners, a leading professional services firm. We specialize in providing comprehensive and tailored solutions for companies subject to the EU AI Act, guiding them through the intricacies of regulatory requirements and enabling responsible and accountable AI practices. At AI & Partners, we understand the challenges and opportunities that the EU AI Act presents for organizations leveraging AI technologies. Our team of seasoned experts combines in-depth knowledge of AI systems, regulatory frameworks, and industry specific requirements to deliver strategic guidance and practical solutions that align with your business objectives.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Contacts

Sean Donald John Musch, Co-CEO/CEO, s.musch@ai-and-partners.com

Michael Charles Borrelli, Co-CEO/COO, m.borrelli@ai-and-partners.com

Authors

Sean Donald John Musch, Co-CEO/CEO

Michael Charles Borrelli, Co-CEO/COO

Acknowledgements

We are grateful to our network of corporate partners for their invaluable contributions:

We are also grateful to our network of individual supporters for their invaluable contributions:

Doug Hohulin, Business Associate (AI & Partners), Strategy and Technology Advisor on Responsible AI (Ethics, Governance, Policy, Regulation, Compliance, Safety), AI in Healthcare, and AI Operations and Workflows.

Simon Greenman, Co-founder and partner in Best Practice AI, an AI management consultancy that works with executives to help create competitive advantage with AI and digital transformation.

Important notice

This document has been prepared by AI & Partners B.V. for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of AI & Partners B.V. to supply the proposed services.

Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.

AI & Partners B.V. is the Dutch headquarters of AI & Partners, a global professional services firm. Please see https://www.ai-and-partners.com/ to learn more about us.

Designed and produced by AI & Partners B.V.