Unfit for purpose? The legal maze of credit scoring under EU law

Judith Arnal

In-Depth Analysis

Summary

The rules on automated credit scoring in the EU are entering a phase of profound transformation. The European Court of Justice's so-called *SCHUFA* judgment has significantly broadened the scope of Article 22 of the General Data Protection Regulation (GDPR), resulting in widely used scoring practices being placed under greater legal scrutiny.

At the same time, the EU's AI Act introduces a parallel framework that classifies AI systems used for credit scoring as high-risk, imposing far-reaching compliance obligations. This dual regulatory regime creates overlapping – and at times conflicting – requirements for financial institutions, raising serious concerns about legal certainty, operational feasibility and the future of algorithmic innovation in credit markets.

This ECRI In-Depth Analysis paper examines the interaction between the GDPR and the AI Act in the context of credit scoring. It shows why relying on consent or contractual necessity under the GDPR could be challenging and argues that a sector-specific legal basis would provide a more stable and scalable solution. It also identifies ambiguities in the AI Act's scope – particularly regarding what constitutes an 'AI system' – and calls for early supervisory guidance to prevent the overregulation of well-established statistical models and a possible increase in fragmented interpretation by EU Member States (and even within different authorities in the same Member State). Finally, it proposes practical steps to ensure effective coordination between data protection and AI authorities.

This ECRI In-Depth Analysis paper concludes that safeguarding consumer protection and enabling responsible innovation are not mutually exclusive goals, but achieving both requires targeted legal reform, interpretative clarity, regulatory coherence and harmonisation across the entire EU.

1. Introduction

Technological innovation is transforming how financial services are provided, particularly in credit. Credit scoring systems based on automated data processing that are an integral part of risk management processes have become a cornerstone of lending practices. These systems, whether based on traditional statistical methods or more complex Machine Learning techniques/AI, allow lenders to assess risk more efficiently, enabling faster decisions and potentially greater financial inclusion[1]. On the other hand, biases in datasets and algorithms can lead to discrimination and the exclusion of already marginalised groups.

However, the regulatory landscape governing these practices is undergoing a profound shift. On 7 December 2023, the European Court of Justice (CJEU) issued a landmark preliminary ruling in the so-called *SCHUFA* case. It concluded that the automated establishment of repayment probabilities by credit reference agencies (CRAs), when used decisively in lending decisions, constitutes automated decision-making under Article 22(1) of the General Data Protection Regulation (GDPR). Unless specific exceptions apply, such processing is prohibited. This ruling has significant implications not only for CRAs but also for banks and other financial institutions relying on automated credit scoring tools.

The regulatory picture is further complicated by the entry into force of the EU's AI Act in August 2024. Under this new regulation, AI systems used to assess the creditworthiness of natural persons are classified as 'high-risk', triggering extensive compliance obligations. Moreover, recent guidelines issued under the AI Act raise questions about how AI is defined, and over which parts of the credit origination process fall under its scope. Together with the GDPR, this dual framework risks creating overlapping or even conflicting obligations for financial actors – which could ultimately lead to higher costs for consumers.

This ECRI In-Depth Analysis paper examines how the combined effect of the GDPR and the AI Act is reshaping the regulatory landscape for automated credit scoring in the EU. **Section 2** analyses the implications of the *SCHUFA* ruling and explains why the existing legal bases under the GDPR – especially consent and contractual necessity – are inadequate to sustain widely used scoring practices. It argues that only a clear legal basis at EU or national level can resolve the resulting legal uncertainty and sets out a policy proposal for sector-specific financial legislation as the most viable path forward. **Section 3** turns to the AI Act and explores its impact on credit providers, focusing on the classification of credit scoring as a high-risk use case, the ambiguity surrounding the definition of AI, and the need for sectoral guidance to avoid the overregulation of well-established statistical models. **Section 4** addresses the coordination challenges between the GDPR and the AI Act, highlighting the risks of overlapping obligations and decentralised enforcement. It proposes targeted solutions to ensure legal coherence and supervisory convergence.

Together, this analysis supports a central conclusion – in short, the current regulatory architecture is not fit for purpose.

Protecting data subjects must remain a core priority but unless the EU or its Member States provide clear, coherent and harmonised rules, the use of automated credit scoring systems – essential to modern credit markets – will remain trapped in a zone of legal ambiguity. To overcome this, the analysis provides three concrete policy recommendations to align innovation and fundamental rights in the age of algorithmic finance.

2. The so-called *SCHUFA* case and the GDPR framework

2.1. *SCHUFA*: a watershed moment for automated credit scoring

The *SCHUFA* case represents a major turning point in how automated credit scoring is regulated within the EU. The case started when a natural person, known as 'OQ', was denied credit by a bank after having

[1] BIS (2021), *The use of artificial intelligence and machine learning by financial institutions*, Bank for International Settlements.

been the subject of a credit score assessment that was undertaken by SCHUFA (a German private credit bureau), which was then subsequently transmitted to the bank.

Based on the GDPR's Article 15, which allows an individual to access any personal data concerning them held by third parties, OQ subsequently requested SCHUFA to send them the personal data that it held on them and then to erase allegedly incorrect data. SCHUFA responded by informing OQ of their score and the methodology used to calculate it. Unsatisfied with this response, OQ then decided to refer the case to the *Hessischer Beauftragter für Datenschutz und Informationsfreiheit* (the Data Protection and Freedom of Information Commissioner for the German Federal State of Hesse, Germany; 'the HBDI'), asking for full access to their information and the ability to erase what they saw as incorrect data, which the HBDI rejected. It concluded that it couldn't be established that SCHUFA had not complied with Article 31 of the *Bundesdatenschutzgesetz* (Federal Law on Data Protection – BDSG), which deals with the 'protection of trade and commerce in the context of scoring and credit reports'. Thus, based on Article 78 GDPR, OQ then lodged an appeal with the *Verwaltungsgericht Wiesbaden* (Administrative Court, Wiesbaden, Germany), which in turn decided to stay the proceedings and refer the case to the CJEU for a preliminary ruling, which was delivered on 7 December 2023.

The CJEU concluded that the automated calculation of credit scores constitutes 'automated individual decision-making' under Article 22(1) GDPR if those scores significantly influence or determine the outcome of credit decisions made by third parties. This broad interpretation clarifies that it is not merely the final decision-maker who is subject to scrutiny but also upstream actors who contribute decisively to automated decisions.

The implications of the CJEU's reasoning are difficult to reconcile with the operational realities of the credit system. If creating credit scores that are widely used to inform lending decisions is presumptively prohibited under Article 22(1) GDPR, then some of the most established and socially relevant practices in financial markets become legally precarious overnight. This situation is unsustainable – not because the protection of individual rights is excessive but rather because the current framework fails to provide an adequate legal pathway for scoring models that are essential to credit markets' functioning. The pathway proposed by the GDPR, namely relying on individual consent, poses several significant challenges. It would require the individual to agree to SHUFA's credit assessment, but data protection authorities and courts have consistently warned that consent is often invalid in situations involving essential services, power asymmetries or a lack of meaningful alternatives. It may be difficult to argue that using such scores is always necessary in the context of a contract. Additionally, legislation imposing the obligation to carry out adequate creditworthiness assessments should not be removed from the equation.

The optimal solution is a clear legal basis that authorises the use of such systems *ex-ante*, under well-defined conditions and safeguards. Without this, credit scoring becomes a regulatory paradox – simultaneously indispensable for credit access and potentially unlawful under the very rules meant to ensure fairness and inclusion.

2.2. Understanding Article 22 GDPR and its exceptions

Article 22(1) GDPR provides individuals with the right not to be subject to a decision based solely on automated processing, including profiling, where such decisions result in legal effects concerning them or similarly significantly effects that impact them. However, this right is not absolute. Article 22(2) sets out four distinct exceptions allowing such automated decision-making, subject to appropriate safeguards.

These four exceptions can be conceptually grouped according to their legal nature and operational scope[2]. The first category includes exceptions based on an overarching legal mandate, such as when automated decision-making is authorised by EU or Member State law (Article 22(2)(b)), or when it is necessary for carrying out a task in the public interest (linked via Article 6(1)(e)). A second category concerns what may be termed 'micro-level' exceptions, specifically individual transactions: the necessity for entering or performing a contract with the data subject (Article 22(2)(a)), and the explicit consent of the data subject (Article 22(2)(c)).

This typology, increasingly recognised in academic and regulatory commentary, highlights a core tension in the GDPR: between *collective legal authorisation*, which enables the uniform application of automated processes under a public or statutory framework, and *individualised justification*, which requires automation to be defensible in the context of a specific contractual relationship or personal decision[3]. The distinction mirrors broader debates in EU data protection law about the role of consent and necessity as lawful bases for data processing, particularly in environments characterised by information asymmetry and constrained user autonomy.

2.3. The limits of individual-based exceptions: consent and contractual necessity

While these micro-level exceptions offer flexibility, their actual applicability in the context of automated credit scoring is both limited and controversial. The 'contractual necessity' exception under Article 22(2)(a) has been consistently interpreted restrictively by the European Data Protection Board (EDPB) and national data protection authorities. It requires that using automated decision-making is objectively indispensable for performing the contract itself – i.e. not merely useful, convenient or efficient, but essential. This standard seems to exclude practices where automation is utilised for risk management or business optimisation rather than to meet a contractual obligation toward the data subject. In its Guidelines on Article 6(1)(b) GDPR, the EDPB makes clear that even personalised pricing or eligibility assessments often fall outside this narrow interpretation, unless they are essential to delivering the core service.

Similarly, relying on the 'explicit consent' ground under Article 22(2)(c) is fraught with practical and legal difficulties. For consent to be valid under the GDPR, it must be freely given, specific, informed and unambiguous. In many financial services contexts, these conditions are hard to satisfy due to structural power imbalances between the data subject and the controller, the opacity of the underlying algorithmic logic, and the lack of meaningful alternatives to automated decision-making. Several supervisory authorities, including the French CNIL[4] and the German BfDI[5], have expressed scepticism about the viability of consent in scenarios involving essential services such as access to credit. Furthermore, the CJEU has repeatedly emphasised that consent cannot be presumed or bundled, and must be demonstrably active and granular.

[2] Wachter, S., Mittelstadt, B., & Floridi, L. (2017), 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation', *International Data Privacy Law*, Vol. 7, No 2, pp. 76–99.

[3] Veale, M., & Edwards, L. (2018), 'Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling', *Computer Law & Security Review*, Vol. 34, No 2, pp. 398–404.

[4] CNIL (2020), *AI and personal data: what regulatory framework?*

[5] German Federal Commissioner for Data Protection and Freedom of Information (BfDI) (2023), *Position paper on automated decision-making and financial services.*

These strict conditions have led many scholars to question whether consent and necessity, as formulated under the GDPR, can provide a workable legal basis for automated credit scoring[6][7]. In fact, the conceptual emphasis on individual control may become illusory when users are asked to consent to opaque systems whose implications they cannot fully understand. Moreover, in contexts such as banking or insurance, refusing consent often makes it impossible to gain access to the service entirely – raising concerns about voluntariness and fairness.

2.4. The legal basis dilemma: national laws and regulatory fragmentation

Against the background of the structural and practical limitations surrounding the individual-level exceptions under Article 22(2), the most legally sustainable pathway for enabling the use of automated credit scoring systems in the EU lies in the two remaining exceptions – namely those based on legal authorisation. Specifically, these are: (i) when the automated decision is authorised by EU or Member State law to which the controller is subject (Article 22(2)(b)), and (ii) when the processing is necessary for performing a task carried out in the public interest, as provided under Article 6(1)(e) GDPR and read in conjunction with Article 22(2)(b).

These legal exceptions require the existence of a clear and specific legal basis that not only permits automated decision-making, but also incorporates appropriate safeguards to protect the rights, freedoms and legitimate interests of data subjects, in line with Article 22(3). This includes ensuring transparency, the right to human intervention and effective redress mechanisms. According to the EDPB, such legal bases must be sufficiently precise, foreseeable and accessible, and must not be drafted in overly general terms or delegated entirely to private actors' discretion.

Within this framework, the key challenge is that most Member States have not enacted legislation that would provide such a specific legal basis for using automated credit scoring in a way that complies with the strict requirements of Article 22(2)(b). The *SCHUFA* case itself revolved around the question of whether Article 31 of the German Federal Data Protection Act (BDSG) fulfilled this role. The CJEU refrained from issuing a definitive judgment on this matter but clearly indicated that there were 'serious doubts' as to whether the German provision, which regulates only the *use* of scoring outputs but not their *creation*, satisfies the standard of legality and specificity required under EU law.

Legal scholars have widely interpreted this hesitation as a signal that many national laws currently fall short of establishing a valid legal exemption under Article 22(2)(b). Unless EU or Member State law expressly governs both the algorithmic process and the legal effects of the automated decision, including the appropriate safeguards, it cannot be deemed a lawful derogation from the general prohibition under Article 22(1).

Furthermore, while the GDPR envisages the possibility of relying on 'public interest' as a legal basis (Article 6(1)(e)), its compatibility with fully automated decisions under Article 22 GDPR depends on the legal act that establishes that public interest also meets the criteria set in Article 22(2)(b). The result is a narrow and demanding pathway, only available if legislation explicitly regulates the processing operation, its objectives, its necessity and its safeguards – something which is rarely the case in the field of credit.

[6] Selbst, A. D., & Powles, J. (2017), 'Meaningful information and the right to explanation', *International Data Privacy Law*, Vol. 7, No 4, pp. 233–242.

[7] Kaminski, M. E. (2019), 'The Right to Explanation, Explained', *Berkeley Technology Law Journal*, Vol. 34, No 1, pp. 189–218.

In this context and considering the difficulties in relying on individual consent or contractual necessity in several cases, legal authorisation remains the most robust and scalable solution to ensure that automated credit scoring can be lawfully performed under EU law. However, this pathway is not without its own significant limitations. As the *SCHUFA* case illustrates, it's not enough for a Member State to adopt general or partial provisions regarding scoring practices. The legal basis must be sufficiently specific, detailed and complete, covering both the processing operation and its legal effects, and ensuring compliance with all applicable safeguards under Article 22(3) GDPR.

More fundamentally, relying on national legal bases under Article 22(2)(b) GDPR opens the door to regulatory fragmentation across the EU. Some Member States may choose to adopt legislation authorising certain forms of automated credit scoring, while others may refrain from doing so or impose stricter conditions. As a result, what is lawful in one jurisdiction may be unlawful in another, creating inconsistencies regarding individuals' rights and barriers to providing cross-border credit services.

This lack of harmonisation threatens the Single Market's integrity and undermines the level playing field among credit providers, particularly those operating on a pan-European scale. Without a common EU-wide legal basis, CRAs and digital lenders face increased compliance costs, legal uncertainty and potential enforcement disparities. The risk is that legal fragmentation could effectively discourage the development and deployment of innovative credit scoring solutions, reinforcing market concentration and limiting access to finance, especially in smaller Member States.

2.5. Policy recommendations: sectoral reform of EU financial legislation to overcome GDPR deadlock

Considering the legal uncertainty surrounding automated credit scoring under the GDPR – and the limited viability of relying on the current Article 22(2) exceptions – it is worth considering whether a legislative response at EU level is even necessary. However, any attempt to amend the GDPR itself to introduce a harmonised legal basis for credit scoring would likely prove politically and legally unfeasible. The GDPR is a horizontal and deeply embedded regulatory framework. Though the European Commission is expected to present a proposal to simplify the GDPR under the Omnibus III Package in the fourth quarter of 2025, fully opening it for revision could trigger an extensive and contentious process with uncertain outcomes and wide-ranging implications beyond the credit domain.

Against this backdrop, a more viable and legally coherent approach would be to act through sector-specific EU financial legislation. Rather than altering the GDPR, the EU could instead adopt targeted provisions within relevant financial instruments that would explicitly allow the use of automated decision-making for creditworthiness assessments – but under specific conditions and with appropriate safeguards. This vertical approach would be more in line with existing EU practice, where data protection requirements are operationalised within the logic and objectives of each policy field.

The main challenge lies in the fragmentation of the EU legal framework on credit. Consumer credit is governed by the recently revised Consumer Credit Directive. Mortgage credit is regulated under the Mortgage Credit Directive. A range of other instruments, including the Capital Requirements Regulation, the Digital Operational Resilience Act (DORA) and the Anti-Money Laundering Regulation, also touch upon different aspects of credit provision and financial intermediation.

Any effective regulatory solution would therefore require a coordinated effort[8] across multiple legal texts, ideally by introducing a shared legal clause or common legal standard. This could take the form of a cross-referenced provision enabling the use of automated creditworthiness assessments across

[8] European Banking Authority (2022), *Discussion paper on the use of Machine Learning in credit scoring.*

different types of credit products, provided that the core principles of Article 22(3) GDPR – including transparency, human review and redress – are upheld. Another more pragmatic option would be for the Commission to issue an interpretative communication, clarifying the conditions under which national or EU financial law may be deemed to fulfil the requirements of Article 22(2)(b) GDPR in the credit context. While not legally binding, such guidance could foster greater regulatory convergence and legal certainty.

Although institutionally complex, this type of vertical intervention may ultimately offer the most realistic and effective route to reconciling innovation and legal clarity in the field of automated credit scoring. It would also help prevent fragmentation across Member States and safeguard the functioning of the Single Market in retail financial services.

3. The AI Act and its implications for credit scoring

3.1. A new layer of compliance: credit scoring as high-risk AI

The AI Act's entry into force in 2024 adds a new regulatory layer to the already complex framework governing automated decision-making in credit markets. The AI Act introduces a risk-based approach, with AI systems used to assess the creditworthiness of natural persons or establish their credit score explicitly listed as high-risk under Annex III, point 5(b), due to their potential to significantly affect individuals' access to and enjoyment of financial services.

These systems are subject to a comprehensive set of requirements, including risk management procedures, data governance protocols, technical documentation, transparency standards and human oversight mechanisms. They must also undergo conformity assessments prior to deployment and be capable of post-market monitoring and incident reporting[9]. For credit providers, this introduces new substantial compliance requirements, on top of existing obligations under financial regulation and data protection law, particularly burdening smaller lenders and fintech firms.

The classification of AI-driven credit scoring as high risk is not contested. However, the AI Act's practical application to this use case is still evolving. Many institutions aren't yet fully aware of the range of technical and organisational adjustments that will be required. Because of this, the Regulation's implementation timeline becomes critical. While the AI Act entered into force in 2024, the compliance obligations will be staggered over time depending on the type of system involved. The key dates relevant to creditworthiness assessment systems are summarised below in Table 1:

Table 1. Timeline for the AI Act's implementation in the credit sector

Relevant date	Action
2 February 2025	Prohibited practices start to apply
2 May 2025	Codes of practice expected to be published
2 August 2025	Obligations for general-purpose AI systems come into force
2 August 2026	Obligations for **high-risk AI systems in Annex III**, including credit scoring, become applicable
2 August 2027	Obligations for high-risk systems under Annex II take effect

Source: Own elaboration based on the AI Act.

[9] Hacker, P. (2022), 'The EU AI Act: Critical perspectives on rights, risks and regulatory design', *European Law Journal*, Vol. 28, No 1, pp. 63–82.

This timeline confirms that the core obligations affecting credit providers will apply from 2 August 2026[10], giving institutions a limited window to review and redesign their scoring systems. Given the complexity of these requirements, including the need to document model risks, ensure explainability and implement robust human oversight, many providers will probably need to begin their preparatory work well in advance of the final deadline.

At the same time, the lack of sector-specific standards or interpretive guidance from financial supervisors or the European AI Office increases legal uncertainty. Among the uncertainties is how an AI system is defined – which will be discussed shortly. Unless this is addressed, the resulting new regulatory layer would bring with it a significant level of uncertainty and may result in a chilling effect on innovation, with risk-averse institutions reducing automation or outsourcing to third parties with greater compliance capacity – potentially deepening concentration in the credit market[11].

3.2. What is AI? The uncertain boundary between statistical modelling and AI

A central difficulty in implementing the AI Act lies in clearly marking the boundary between what constitutes a regulated 'AI system' and what remains within the realm of traditional data processing. The Regulation broadly defines AI systems in Article 3(1), including a wide range of approaches such as machine learning, logic- and knowledge-based systems. This breadth has raised concerns that longstanding, transparent techniques – such as linear or logistic regression – might fall within the scope of high-risk AI regulation, particularly in credit assessment contexts.

The European Commission's *Guidelines on the definition of an artificial intelligence system established by the AI Act* attempt to provide clarity. Point 42 offers the most relevant elaboration regarding the use of statistical models:

> *'Systems used to improve mathematical optimisation or to accelerate and approximate traditional, well established optimisation methods, such as linear or logistic regression methods, fall outside the scope of the AI system definition. This is because, while those models have the capacity to infer, they do not transcend 'basic data processing'. An indication that a system does not transcend basic data processing could be that it has been used in a consolidated manner for many years. This includes, for example, machine learning-based models that approximate functions or parameters in optimization problems while maintaining performance. The systems aim to improve the efficiency of optimisation algorithms used in computational problems. For example, they help to speed up optimisation tasks by providing learned approximations, heuristics, or search strategies.'*

This clarification is significant: it explicitly recognises that not all predictive or inferential models are to be classified as AI systems. What matters is whether the model is used in a way that 'transcends basic data processing', a threshold that's not fully defined but appears to include considerations such as novelty, complexity, autonomy and adaptive behaviour.

Another aspect of uncertainty is the meaning of 'mathematical optimisation', as any model that attempts to interpolate points with a mathematical function – such as logistic regression – do this via a *mathematical optimisation* (typically error minimisation), regardless of its specific purpose. This aspect

[10] This timeline does not apply to Annex III AI applications placed on the market before that date.

[11] Gekker, A., & Hind, S. (2022), 'AI, Financial Services and Regulatory Chilling Effects: Innovation at Risk?', *Journal of Law, Technology & Policy,* Vol. 1, pp. 41–78.

is of the utmost importance for the financial sector since most of the systems used in the credit scoring area are linear or logistic regressions.

The Guidelines further note that even some machine-learning-based models may fall outside the AI definition if they are used to approximate functions in optimisation problems without assuming broader decisional functions. This introduces a potential exclusion for rules-based, deterministic systems that have been used for many years in the financial sector without significant variation or adaptation.

Nevertheless, the operational uncertainty remains considerable. The concept of 'basic data processing' is not defined in the AI Act, and how it is interpreted will likely vary across sectors and supervisory authorities. In credit scoring, logistic regression models are commonly used to assess the likelihood of default[12]. Whether such techniques – especially when embedded within a broader pipeline of decision automation – constitute 'basic processing' or a regulated AI system, and in the case of being AI, whether they should be classified as high risk, remains unclear.

This ambiguity becomes especially problematic when we consider the multi-step nature of the credit origination process, which includes:

1. Data acquisition,
2. Customer identification,
3. Fraud assessment,
4. Internal IRB rating estimation (where applicable),
5. Creditworthiness assessment,
6. Collateral/guarantee estimation,
7. Final pricing and approval, and
8. Monitoring.

Only the fifth step corresponds to the actual credit scoring in the sense of creditworthiness assessment as described in the AI Act's Annex III. However, AI or statistical models may be used during multiple stages of this process, raising the question of whether their use outside the fifth step could still trigger the obligations associated with high-risk AI systems.

The Guidelines don't provide a definitive answer to this question. The only functional indication is whether a model 'transcends' traditional, basic optimisation. This leaves a grey zone for systems that are not self-learning or adaptive, but that are used to inform key decision points, such as product pricing. The concern is that, absent further clarification, institutions may be incentivised to interpret the Guidelines conservatively, applying full AI compliance procedures even to basic, non-adaptive models, especially considering the high-level sanctions foreseen by the AI Act. Such a conservative approach would lead to high compliance-related costs for EU financial institutions. The Guidelines that the Commission should issue no later than 2 February 2026 would be an excellent opportunity to make these clarifications.

From a regulatory perspective, this uncertainty undermines legal clarity and introduces the risk of overregulation of transparent and explainable tools. Paradoxically, firms may favour more complex and

[12] Crook, J. N., Edelman, D. B., & Thomas, L. C. (2007), 'Recent developments in consumer credit risk assessment', *European Journal of Operational Research,* Vol. 183, No 3, 1447–1465.

opaque AI systems that are designed to meet formal compliance criteria, even if they reduce interpretability and auditability – an outcome at odds with the AI Act's fundamental rights objectives[13].

3.3. Policy recommendations: providing clarity on the AI Act without overregulation

To mitigate legal uncertainty and avoid regulatory overreach when implementing the AI Act, the credit sector should work towards two complementary policy interventions – one short-term and pragmatic, the other more structural and harmonised.

First, financial supervisors at both the EU and national levels – particularly the European Banking Authority, national competent authorities and, where relevant, the Single Supervisory Mechanism (SSM) – should issue early supervisory guidance to clarify expectations for credit providers. This may take the form of supervisory statements or FAQs, explicitly recognising that certain traditional, rules-based scoring models (e.g. logistic regression used in a static and explainable manner) are likely to fall outside the scope of the AI Act's system definition and therefore from its rules. Such guidance would offer immediate legal certainty and help prevent disproportionate compliance costs or defensive de-automation strategies during the transitional period.

Second, the Commission, together with the European AI Office and financial regulators, should develop sector-specific interpretative guidance clarifying how the AI Act should be applied in the credit domain. This should include a functional definition of 'basic data processing' as referenced in Point 42 of the Guidelines, concrete examples of excluded models, and clarifying the boundaries of Annex III(5)(b), particularly regarding which phases of the credit origination process fall under the Regulation. While such guidance will require more time to develop and coordinate, it's essential to ensure consistent enforcement and prevent future fragmentation.

Taken together, these two actions would help strike the right balance between regulatory ambition and proportionality, enabling institutions to comply effectively while maintaining the use of transparent, well-understood statistical tools in credit assessment.

4. Coordination challenges

4.1. The overlap between the GDPR and AI Act

One of the most complex and underexplored aspects of the EU's emerging digital regulatory landscape is the relationship between the AI Act and the GDPR[14]. Both legal instruments apply to systems that involve the automated processing of personal data, and both aim to protect individuals from harm – though they do so through different mechanisms, legal bases and institutional structures[15].

The AI Act, particularly for high-risk systems such as credit scoring, imposes a preventive logic[16]: it requires that systems be designed, tested and documented in advance, and subject to conformity assessments prior to being deployed. In contrast, the GDPR adopts a reactive and individual-rights-

[13] Wachter, S., Mittelstadt, B., & Russell, C. (2021), 'Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI', *Computer Law & Security Review,* Vol. 41, 105567.
[14] Lynskey, O. (2021), 'Governing data in AI: The case of the GDPR and the EU AI Regulation', *European Law Review,* Vol. 46, No 6, pp. 761–780.
[15] Mantelero, A. (2022), 'AI and the GDPR: Two worlds apart? International Data Privacy Law', Vol. 12, No 3, pp. 207–218.
[16] Hacker, P. (2022), 'The preventive logic of the AI Act and its implications for rights protection', *European Law Journal,* Vol. 28, No1, pp. 63–82.

based approach, where data subjects are entitled to access, challenge and seek redress in relation to decisions made about them[17].

Although the AI Act states in Recital 9 that it shall apply without prejudice to the GDPR, the practical overlap is substantial. Both texts regulate profiling, transparency, human oversight and redress. For example, the GDPR (Article 12(1)) requires that information be provided to data subjects in a 'concise, transparent, intelligible and easily accessible form', and additionally the AI Act (Article 14(4)(a)) now also requires that human operators be able to understand the capabilities and limitations of high-risk systems, including their intended purpose and performance. Article 14(4)(b) then mandates that these operators be made aware of the possibility of automation bias, reinforcing the importance of informed and effective oversight.

Nowhere is this overlap more evident than in human involvement in automated decisions[18]. Article 22(3) GDPR requires meaningful human intervention where Article 22(1) applies. The AI Act introduces a parallel requirement for oversight but does so from the perspective of system design rather than individual redress. The divergence in approach raises the risk of conflicting interpretations and obligations for the same scoring model, depending on whether it's assessed under data protection or AI compliance logic.

In institutional terms, there is significant potential for regulatory fragmentation. Data protection authorities remain competent under the GDPR, while AI market surveillance authorities – yet to be fully designated in many Member States – will be responsible for overseeing compliance with the AI Act. Where a credit scoring model involves both personal data and high-risk AI classification, jurisdictional conflicts may arise, particularly in enforcement and supervisory guidance.

Moreover, the risk of divergent interpretation is further heightened by the AI Act's decentralised enforcement structure. While it creates a European AI Office and foresees coordination at EU level, it explicitly leaves designating national market surveillance authorities to the discretion of each Member State (Article 70). In practice, this means that enforcement may be handled by different types of institutions depending on the jurisdiction, ranging from data protection authorities to consumer agencies, sectoral regulators, or entirely new bodies created for the sole purpose of monitoring AI Act compliance.

In the financial sector, some degree of convergence may be expected – particularly under the SSM for significant credit institutions in the euro area. However, even within the SSM, AI-related compliance doesn't currently fall under the ECB's direct remit and will likely remain with national competent authorities. This opens the door to divergent interpretations of what constitutes high-risk AI and how the relevant obligations should be applied in credit scoring practices.

This problem isn't unique to the AI Act. As extensively analysed in previous work[19][20], the GDPR itself suffers from a structurally fragmented enforcement model, despite its formal status as a directly applicable EU regulation. Under the 'one-stop-shop' mechanism and Article 56 GDPR, lead supervisory

[17] Wachter, S., Mittelstadt, B., & Floridi, L. (2017), 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation', *International Data Privacy Law,* Vol. 7, No 2, pp. 76–99.

[18] Wachter, S., Mittelstadt, B., & Russell, C. (2021), 'Why fairness cannot be automated: Bridging EU non-discrimination law and AI', *Computer Law & Security Review,* Vol. 41, 105567.

[19] Kloza, D., & Van Dijk, N. (2020), 'GDPR's enforcement structure: Fragmentation and coordination issues', in R. Leenes & P. de Hert (eds.), *Data Protection and Privacy: Data Protection and Democracy* (pp. 127–149), Springer.

[20] Arnal, J. (2025), 'AI at Risk in the EU: It's Not Regulation, It's Implementation', *European Journal of Risk Regulation*, 1–10.

authorities are appointed at national level, and while the EDPB coordinates consistency, final interpretative and enforcement decisions remain with national bodies. In practice, this has led to variations in enforcement intensity, divergent interpretations of key provisions and regulatory bottlenecks in cross-border cases.

The coexistence of two ambitious regulatory frameworks – both relying on decentralised implementation – amplifies the risks of inconsistency and fragmentation. Rather than converging through mutual reinforcement, the AI Act and GDPR may compound existing divergences, especially when different authorities are involved, operate under separate procedures, and respond to distinct institutional logic. This not only undermines predictability and coherence for market participants but also challenges the legitimacy of EU digital governance in the eyes of citizens and stakeholders[21].

4.2. Policy recommendations: ensuring coherence between the GDPR and the AI Act

To address the overlapping obligations and institutional fragmentation identified above, two targeted policy interventions are especially urgent to safeguard legal certainty and a level playing field in the credit sector.

First, the Commission, in cooperation with the EDPB and the newly created European AI Office, should issue joint guidance clarifying how the GDPR and the AI Act apply concurrently to financial services. This guidance should address the interaction between key provisions – particularly Articles 22 GDPR and 14 AI Act – and define common standards for human oversight, explainability and transparency. Clarifying the scope and complementarity of both regimes would help avoid regulatory duplication and ensure that compliance expectations are coherent and proportionate to actual risks.

Second, to prevent diverging enforcement practices across Member States, the Commission should promote structured cooperation between national market surveillance authorities and data protection authorities. This may include establishing joint supervisory task forces for high-impact sectors such as credit and fostering the exchange of best practices. For cross-border financial institutions, coordination within the SSM could provide an additional layer of convergence – at least for significant credit institutions – though the clear delineation of supervisory mandates remains essential.

These two steps – guidance at the EU level and coordination among national authorities – are critical for avoiding fragmentation, reducing legal uncertainty and enabling responsible innovation in AI-driven credit scoring across the EU.

Conclusions

The combined application of the GDPR and the AI Act to automated credit scoring creates a dense and fragmented regulatory environment for financial institutions in the EU. The SCHUFA judgment significantly expanded the reach of Article 22 GDPR, while the AI Act introduces high-risk classification and prescriptive obligations for systems used to assess creditworthiness. Consequently, institutions now face overlapping and partly ambiguous requirements, which risk hindering innovation, increasing compliance burdens and exacerbating market concentration.

[21] Smuha, N. A. (2021), 'The fundamental rights implications of the AI Act', *Philosophy & Technology,* Vol. 34, pp. 215–219.

These challenges are not rooted in overregulation *per se*, but in the absence of clarity, coherence and coordination. A more balanced and forward-looking regulatory approach is thus needed to ensure legal certainty while supporting responsible innovation.

First, the EU should provide a harmonised legal basis for the use of automated credit scoring systems that aid adequate creditworthiness assessments through sector-specific financial legislation, rather than by amending the GDPR itself. Instruments such as the Consumer Credit Directive, the Mortgage Credit Directive or forthcoming frameworks on digital finance could be adapted to explicitly authorise the use of algorithmic creditworthiness assessments, under the conditions set out in Article 22(2)(b) GDPR. This approach would reduce reliance on fragile individual-level exceptions and help prevent regulatory fragmentation across Member States.

Second, both short-term and medium-term interpretative guidance is needed to clarify how the GDPR and the AI Act apply to automated scoring. In the short term, financial supervisors – both at national and EU level – should issue practical guidance to reassure institutions that rules-based, transparent models like logistic regression are unlikely to fall under the definition of an AI system when used in static and interpretable ways. In the medium term, the Commission, together with the European AI Office, the EDPB and financial regulators, should develop joint guidance on how to operationalise key concepts such as 'basic data processing' or 'mathematical optimisation', and the boundaries of Annex III(5)(b) in the context of the credit origination chain. Clear, sector-specific guidance would allow institutions to align their compliance efforts with actual risk and reduce the tendency to overcomply by default.

Third, institutional coordination must be strengthened to avoid supervisory fragmentation. The AI Act leaves designating national market surveillance authorities to Member States' discretion and the GDPR's one-stop-shop mechanism has already shown its limits in practice. In this context, promoting structured cooperation between AI and data protection authorities, as well as existing sector specific regulators, is essential. This could include joint task forces in the credit domain, shared enforcement protocols and coordinated guidance. Within the Banking Union, the SSM could contribute to convergence, at least for significant institutions that operate cross-border, even if AI supervision does not fall within the ECB's direct mandate.

Taken together, these measures would help to ensure that the EU's digital regulatory framework enables – and not constrains – responsible technological progress in financial services.

Protecting fundamental rights and fostering innovation need not be opposing objectives. With the right legal architecture, they can be mutually reinforced.

European Credit Research Institute

The European Credit Research Institute (ECRI) is an independent, non-profit research institute that develops its expertise from an interdisciplinary team and networks of academic cooperation partners. It was founded in 1999 by a consortium of European banking and financial institutions. ECRI's operations and staff are managed by the Centre for European Policy Studies. ECRI provides in-depth analysis and insight into the structure, evolution, and regulation of retail financial services markets in Europe. Through its research activities, publications and conferences, ECRI keeps its members up to date on a variety of topics in the area of retail financial services at the European level, such as consumer credit and housing loans, credit reporting, consumer protection and electronic payments. ECRI also provides a venue for its members to participate in the EU level policy discussion.

For further information, visit the website: www.ecri.eu.

Centre for European Policy Studies

CEPS is one of Europe's leading think tanks and forums for debate on EU affairs, with an exceptionally strong in-house research capacity and an extensive network of partner institutes throughout the world. As an organisation, CEPS is committed to carrying out state-of-the-art policy research that addresses the challenges facing Europe and maintaining high standards of academic excellence and unqualified independence and impartiality. It provides a forum for discussion among all stakeholders in the European policy process and works to build collaborative networks of researchers, policymakers and business representatives across Europe.

For further information, visit the website: www.ceps.eu.