Decoding Responsibility in the Era of Automated Decisions: Understanding the Implications of the CJEU's SCHUFA Judgment

October 2024

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Decoding Responsibility in the Era of Automated Decisions: Understanding the Implications of the CJEU's SCHUFA Judgment

As part of our broader project on the intersection of financial services and personal data protection, the Centre for Information Policy Leadership ("**CIPL**")[1] has examined the potential implications and practical consequences of the Court of Justice of the European Union ("**CJEU**")'s judgment issued on December 7th, 2023 in the SCHUFA case.[2] To enrich our analysis, we have hosted roundtables and workshops with policymakers and industry leaders to reflect on financial services use cases that could be undermined by an overbroad interpretation of the ruling. This discussion paper provides an overview of the SCHUFA judgment, and explores its implications for financial services. This paper concludes that interpretation of the SCHUFA judgment should be limited to the context of the specific facts of the case to avoid untenable and inconsistent outcomes if applied too broadly.

1) Core Facts of the SCHUFA case

SCHUFA Holdings AG ("**SCHUFA**"), a top credit rating agency in Germany, offers credit scores used to help make lending decisions. SCHUFA's clients include organisations such as financial institutions, retailers, telecom companies, utility companies, and transportation firms.

In the case before the CJEU, a prospective borrower (referred to as OQ) was denied a loan by a bank, which received a credit score relating to OQ from SCHUFA. OQ made a request to SCHUFA under Article 15(1)(h) of the EU General Data Protection Regulation ("**GDPR**") for details about the automated decision-making ("**ADM**"), including profiling, defined in Article 22 of the GDPR, involved in SCHUFA's credit scoring processes.[3]

SCHUFA refused OQ's request, citing trade secrets and explaining that SCHUFA had only performed preparatory acts for the lender's decision. SCHUFA claimed that the lender, not SCHUFA, made the decision to reject OQ's loan application, and thus SCHUFA was not obligated to comply with OQ's request under Article 15.

---

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Case C-634/21, SCHUFA Holding, ECLI:EU:C:2023:957.

[3] Under GDPR Article 15(1)(h), a data subject has the right to information on "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject, and under Article 22, a data subject has the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

2) Key Points of the CJEU's Ruling

The CJEU ruled that SCHUFA did make a decision in scope of Article 22(1) of the GDPR. The court found that SCHUFA's credit score played a "determining role" in the lender's decision to deny the loan. It emphasized that SCHUFA's scoring process significantly influenced the credit decision, thereby making SCHUFA a decision-maker under the GDPR's automated decision-making (ADM) obligations.[4]

The key points from the CJEU's SCHUFA judgment were:

- SCHUFA's credit score played a "determining role" in the granting of credit and therefore the "establishment of that value" in itself constituted a "decision" within the meaning of Article 22(1) GDPR.

- The CJEU ruled that Article 22(1) GDPR must be interpreted as meaning that "the automated establishment" of a credit score by a credit information agency constitutes ADM where a bank or other third party "draws strongly on" that value to establish, implement or terminate a loan or other contract.

- The court interpreted "decision" broadly, acknowledging that multiple actions can impact the data subject. It did not matter that SCHUFA did not make the "actual decision" on granting credit; the Court found there to be a close enough connection between SCHUFA's credit score and the lender's decision.

- SCHUFA was in a better position than the lender to provide "meaningful information," including the logic behind the ADM process, to fulfill the Article 15 request.

Furthermore, on September 12, 2024, Advocate General Richard De La Tour provided an opinion in case CK Dun & Bradstreet Austria, which will supplement the CJEU's SCHUFA judgment by clarifying the scope of the right of access under Article 15 GDPR. In his Opinion, the Advocate General stated that "meaningful information about the logic involved" in automated decision-making must allow the data subject to exercise their rights under the GDPR, particularly Article 22. This requires that the information be:

- Concise, easily accessible, clear, and formulated in plain language, explaining the method and criteria used for the decision; and,

[4] Notably, a previous SCHUFA case in the pre-GDPR era by the German Federal Court of Justice came to a different conclusion than the recent CJEU judgment.In that earlier case, the German court held that credit-scoring systems were outside the scope of the right of access enshrined in Article 12(a) of the Directive. This was because the automated elements of the decision-making process were related only to the preparation of data, with decisions ultimately made by a person, and because the underlying formulas were protected as trade secrets. German Federal Court of Justice judgment of 28 January 2014, VI ZR 156/13.

- Sufficiently complete and contextualized, so the person can verify its accuracy and assess if there is a verifiable consistency and causal link between the method, criteria, and the automated decision's outcome.[5]

In the Advocate General's view, the information that must be disclosed by the controller does not include information of a technical nature, such as the details of the algorithms used, that the data subject would not be in a position to understand. The Advocate General also clarified that if providing this information under the right of access is likely to infringe the rights and freedoms of others (e.g., the controller's trade secrets), the information should be disclosed to the relevant supervisory authority or court. These authorities will then balance the interests and determine the appropriate extent of access that should be granted.[6]

Finally, it's important to highlight that on the same day, the CJEU also delivered another judgment concerning SCHUFA, focusing specifically on the record retention practices of credit agencies.[7]

3) Implications on Financial Services and Necessity for Narrow Interpretation

The CJEU's broad interpretation of ADM under Article 22 may mean that organisations providing key information but not making the final decision in relation to a consumer, could be considered decision-makers if they play a determining role in the outcome.

With an overly broad interpretation, this ruling could also affect not only credit reference agencies but any service providers using automated processes to generate risk-based scores or similar or significant outputs (for example, identity verification, fraud detection, money laundering prevention etc.) that play "a determining role" in decisions by financial services entities impacting individuals. It is therefore important to understand the breadth of differences between service providers using automated processes to generate risk-based scores, and why an overly broad interpretation of this ruling should not be made.

---

[5] Case C-203/22 CK Dun & Bradstreet Austria and Magistrat der Stadt Wien, Opinion of Advocate General Richard De La Tour, delivered on September 12, 2024, para 71, available here.

[6] *Ibid,* para 94

[7] Joined cases C-26/22 and C-64/22 (SCHUFA Holding), delivered on December 7, 2023, available here. In this case, the CJEU ruled that it was contrary to the GDPR for private agencies such as SCHUFA to keep data for a longer period than the public insolvency register under German law. The rationale for this judgement is based on the assumption that the purpose of deleting the information relating to the "discharge from the remaining debt" is to enable the debtor to participate in economic life once again, which is why this information is crucial to those involved - since it can result in a negative judgement about the solvency of a given debtor. In this specific case, given the time limit set by the German lawmaker, the CJEU held that, once this time limit had expired, the rights and interests of the debtor took precedence over the other interests involved in obtaining this information. The CJEU held that keeping the information for more than six months was unlawful and, therefore, the debtor was entitled to have the data deleted and SCHUFA was required to delete it without undue delay.

In practice, an expansive interpretation creates tensions with other legislative obligations. For example:

- In general, credit scoring providers have developed business models that operate on the basis that the customer will make the ultimate decision about the end customer and bear the regulatory risk and responsibility associated with any decision taken, using the service provider's outputs. This is a model also required by financial services regulators which do not permit regulated entities to outsource their regulatory obligations i.e., regulated entities may use third parties to assist them in executing their responsibilities, but the ultimate responsibility must remain with the regulated entities. In line with this approach, credit reference agency contracts typically insist lenders should not base a decision solely on the score and should consider other factors before making a decision in relation to the end customer. This is the established practice across multiple jurisdictions and makes it clear that from a financial services regulatory perspective, the regulated entity is responsible and liable for making credit and other regulated decisions in relation to customers. Going forward, it will be necessary to ensure that the undue reliance is not placed on credit scoring to ensure compliance with the SCHUFA judgment and to ensure alignment with financial services obligations. This will prove difficult for organisations that use an individual's credit score as a key factor in their lending strategy, both for risk management and also wider regulatory obligations not to engage in unsuitable lending.

- Credit scoring applies to corporate customers and not just individual consumers. This process involves evaluating a company's creditworthiness based on financial data and other relevant factors to determine their ability to repay debts. It would be both inconsistent and practically challenging if both the approach and practicalities of leveraging established credit scoring arrangements would, as a result of the SCHUFA judgment, need to be changed. This would lead to two different practices as well as different uses of credit scoring information as between individual and corporate end customers. In addition, this may also result in a higher cost of doing business with individual rather than corporate customers which would have an adverse consequence for individual customers in terms of the increase in costs to them.

- More generally, an overly broad interpretation of the SCHUFA decision within the context of Articles 15 and 22 of the GDPR may undermine and adversely impact the use of credit scoring in the financial services sector. Credit scoring is provided as an expert service which enables organisations of varying size and resource to access consistent and high quality data, to assist in making decisions about credit suitability. While credit scoring in itself is a narrow application and use, credit scoring is also often used to supplement processing activities related to producing risk ratings for anti-money laundering, risk management and so on. Without access to credit scoring data, organisations will have to resort to internal checks and processes or proxy/alternative data instead, which may not be as thorough, consistent or up to date as those provided by credit scoring entities. This lack of consistency will inevitably result in different credit suitability and risk approaches across different organisations, with inconsistent outcomes for those seeking credit, which would not be a helpful or desirable outcome for organisations or customers. In addition, the approach to credit risk would also likely be a more risk averse approach by credit providers

due to lack of access to consistent and expert data, credit decisions would take a longer time to process credits, and consequently there would be less access to credit by customers, particularly those who may need it most.

It is clear that a broad interpretation of the SCHUFA judgment would have potentially numerous and significant adverse impacts for both credit providers, financial services firms and customers. Moreover, it is unclear how a broad interpretation of the SCHUFA judgment aligns with certain industry best practices such as the use of real-time data for fraud prevention or cybersecurity management, and other legal obligations imposed on organisations, e.g., U.S. SEC's cybersecurity disclosure rule and the EU Digital Operational Resilience Act ("**DORA**"). The SCHUFA judgment's ruling should therefore be interpreted narrowly, applying only to credit scoring cases with similar facts, and each situation should be assessed individually.

Another aspect of the SCHUFA decision is that it appears to be following a trend as part of a series of CJEU decisions—such as CJEU IAB Europe (C-604/22)[8] and CJEU Pankki S (C-The579/21)[9]—which reflect an expanding of the scope of GDPR and emphasizing the protection of individual rights. This trend, including the SCHUFA case, raises fundamental questions about how to balance the growing reach of GDPR with the need for society and individuals to benefit from modern technologies and improved risk management innovations.

4) Limiting the Application of SCHUFA

Companies using automated processes in their decision-making can distinguish their processes and business models from those in the SCHUFA case so that the SCHUFA ruling does not apply by considering the following questions:

A) <u>To what extent does the company rely solely or predominantly on the credit rating output of the service provider when making a decision?</u>

- If the output is just one of several factors considered by the company, and especially if the company assigns only moderate weight or significance to externally sourced credit ratings or other outputs, the situation should be sufficiently different. Adequate human oversight by an individual both capable and knowledgeable enough to overturn the automated recommendation can also help distinguish a company's practices from the SCHUFA case. However, the term 'moderate weight' needs clarification from the CJEU or financial authorities. Without such clarification, it is not uncommon practice for financial institutions to deny lending as an initial response based solely on a low credit score due to the associated risk to both the lender and the individual.

[8] C-604/22 IAB Europe, Judgment made on March 7, 2024, available here.
[9] C-579/21 Pankki S, Judgment made on June 22, 2023, available here.

- Special consideration should also be given to the relationship between service providers and financial institutions. In the case of SCHUFA, the automated decision-making (ADM) process is split between two entities—SCHUFA and the lender— and leading to SCHUFA being classified as part of the 'decision-making' process. A further distinction can be made between model scores produced by the service provider and customer scores which is produced with input from the customer. In either case, service providers may not be party to an automated process which involves multiple inputs and may be shared across multiple stakeholders. For example, service providers that use automated systems for risk-based scoring, identity verification, or fraud detection could see their outputs used by other stakeholders (such as customers) in decisions that affect individuals. In a similar vein, in some cases, a party, such as a bank, may not be the primary account holder with the individual to whom the data relates, such as when salary and expense payments are made using the financial services infrastructure, and a transaction is subject to ADM to verify identity, detect fraud, etc. In these situations, the service or intermediary relationship with the bank may lead credit service providers' scoring activities to be weighted more heavily in the decision-making process.

- If the company relies heavily on the output, the service provider must ensure that customers can rely on one of the exceptions of Article 22 (2) GDPR. These exceptions include obtaining explicit consent or demonstrating that the automated processing is necessary for a contract between the customer and the data subject. Additionally, Member State law can authorize such processing for the benefit of both the service provider and the customer, provided it includes "suitable measures" to protect the data subject's rights and freedoms.

- Developments in the credit and risk rating services allow the company to adjust or even set the risk parameters to be used by the service provider, thereby influencing the credit or risk rating output to better reflect the company's risk appetite, parameters and other criteria. In such a scenario, the reliance on the risk rating by the company is a result of the individual customisation by the company, and supports a company's rather than service provider's responsibility for the decision making. In addition, companies can obtain credit scores from multiple service providers, which significantly reduces the responsibility and decision-making role of any single provider.

B) Is the ultimate decision one that has a legal or comparatively significant effect?

- Organisations that use credit scores do so for a range of different purposes and reasons. Not all companies use credit scores for decisions that have a significant effect on the data subject. For example organisations may use credit scores for internal purposes such as analyzing customer segments or credit risk to develop new products and services. These actions do not affect the individual's ability to access the services being offered, but instead inform internal management and development strategies.

C) When considering the legal or comparatively significant effect of ADM decisions, it is important to differentiate between the impact of a credit decision (i.e. assessing suitability for a loan, financial

product or other service) versus a transaction or payment fraud (i.e. assessing whether a transaction is unusual or suspicious) or a financial crime decision (i.e. whether a customer meets the organisations risk criteria, is a suitable customer, or if further due diligence is required).

- In relation to fraud decisions, organisations use a wide range of information resources and transaction analytics to help determine whether a transaction may be fraudulent. It is worth noting that these processes are increasingly automated and effective in identifying potentially fraudulent activity and transactions in near real time. For instance, banks and other providers use ongoing data feeds to assess factors like the device used by the customer, the email and phone number linked to the account, transaction location, and other details. These data points are processed to generate a risk score that determines whether a transaction proceeds. In successful fraud detection and prevention - i.e. where fraud is detected correctly, the potential harms that ADM requirements are designed to guard against (i.e. more intrusive processing, leading to a possibly significant negative decision) have in practice the opposite consequences - i.e. a positive impact on the data subject where their details have been impersonated, and this processing is protecting against wider financial harm. Therefore, it is necessary to analyze each case individually to determine how the output from an automated decision-making system would impact compliance with SCHUFA requirements.

- ADM outputs form an important part of financial crime decisions as they enable organisations to access specialized, consistent and quality data – using objective criteria that is applied consistently to each case – to assist in complying with their legal and regulatory obligations to identify and act on financial crime risks and realities. This is especially important against the background of the increasingly frequent, sophisticated and global nature of financial crime. This responsibility and liability cannot be outsourced or delegated to non-regulated entities, but non-regulated entities provide important and necessary services to support regulated institutions in meeting these obligations. Credit scoring and other ADM outputs form important components of the overall process to ensuring compliance with creditworthiness, affordability and financial crime obligations in a timely and effective manner. Where the outcomes may be the rejection of a customer from a particular product or service or overall relationship, which could be seen to be significant, it is also important to balance the decision against the objectives of identifying, preventing and/or stopping financial crime which adversely impacts all customers. This does not necessarily represent a public interest exception. Instead, it reflects an additional regulatory responsibility for financial service institutions to ensure that potential customers are offered products suited to their specific circumstances. This obligation, governed by financial regulations, goes beyond financial institutions' privacy obligations.

- Cyber-crime is one of the top risks faced by organisations and governments. Organisations of all sizes are subject to obligations and responsibilities to identify and defend against increasingly sophisticated cyber-attacks. This requires data and analytics to assess and identify unusual activity and to identify specific threat actors and new risks. The increased technical sophistication of cyber threats requires automated and swift responses, often acting on the outcomes of ADM outputs

provided by expert third parties. The reliance on expert third party assistance in addressing cyber threats is particularly important for SME organisations, which form the majority of organisations. Swift and timely decision making is key to identify and contain risks; it requires a balance between automated decision making that may have an adverse impact on customers and taking a case-by-case and manual approach to decision making which is out of step with the realities of cyber risks and exposes customers to greater risks.

5) Ensuring Legal, Regulatory and Operational Consistency

When analyzing the practical impacts of the SCHUFA judgment, it's essential to also consider related regulatory developments and case law to gain a thorough and coherent understanding. It is equally important to consider legal and regulatory coherence, to ensure that the outcomes are consistent and aligned across different laws and regulations. The following list of developments should be reviewed in this context.

EU AI Act – The EU AI Act classifies AI systems used for credit scoring as high-risk due to their potential impact on access to essential services such as housing and telecoms. However, the EU AI Act has explicitly noted that AI systems used for fraud detection in financial services shall not be considered high-risk.[10] Given the distinction made in the EU AI Act, it would seem sensible to ensure a consistent and similar approach is followed in relation to the SCHUFA judgment.

EU DORA (EU Digital Operational Resilience Act) - DORA provides a binding, comprehensive information and communication technology risk management framework for the EU financial services sector and aims to harmonise the ICT risk management regulations that already exist in individual EU member states. This involves removing the gaps, overlaps and conflicts that could arise between different regulations in different EU member states. A shared set of rules are aimed at making it easier for financial entities to comply while improving the EU financial system's resilience by ensuring that every institution is held to the same standard. Part of this objective is to enhance their cybersecurity preparedness and responses across the industry. A strategic approach to digitally identifying and verifying customers or clients is an essential element of compliance, much of which is supported by third party experts vendors leveraging automated mechanisms to support these identity and verification processes.

Given the importance of third party suppliers in providing credit and other risk mitigation scores, tools and analysis to the financial services sector, this supports a narrow interpretation of the CJEU SCHUFA judgment, which would otherwise give rise to an inconsistent approach to risk as between individual and corporate customers, and across a range of financial services products and services, where the impact of decisions varies considerably as between marketing, cyber, fraud, credit eligibility etc.

[10] See Recital 58 and Article 5(b) Annex III

6) Governing Principles Related to Automated Decision-making

Any regulatory regime that is designed to govern automated decision-making needs to take into consideration the data protection rules, as well as its practical implementation by organisations, to avoid unnecessary duplication of existing and potentially conflicting obligations, ambiguity and legal uncertainty (particularly in heavily regulated sectors). In addition, to the extent any additional regulation or interpretation specific to automated decision-making is contemplated or deemed necessary, it will need to be designed flexibly with an eye to the future, to anticipate the rapid progress and likely changes in this area. Any new rules or interpretation that is created without these important considerations in mind may do more harm for the development of and leadership on responsible use of automated decision-making than good.

In that regard, CIPL has previously addressed automated decision-making rules on several occasions, including our Comments on "WP29's Profiling and ADM Guidelines," Legal Note on "How the GDPR Regulates AI", as well as our recent discussion paper "Automated Decision-making and Profiling Requirements in U.S. State Privacy Laws, and Current State of Play in State AI Regulations." Key principles enshrined from our papers include:

- The outcomes intended by some data protection principles, especially data minimisation and retention limitation and purpose specification could be achieved through mandating strong accountability-based safeguards, including risk assessments, by organisations collecting, using and storing the data to enable both modern AI processing and a high level of privacy protection for individuals;

- The data protection regulations should recognize the need to process more data in some AI contexts (e.g. processing of sensitive data to prevent, detect and mitigate bias);

- Any transparency requirements should be high-level and principles-based to enable the delivery of appropriate and different forms of transparency for a variety of AI contexts;

- Any rules on automated decision-making should not restrict the ability to engage in ADM but rather focus on ensuring appropriate redress, including through rights of review of automated decisions; and

- The data protection regulations should account for potentially multiple regulatory players in the AI space and how this will impact the role of the DPA, its tasks and powers.

7) Conclusion

The recent SCHUFA judgment by the CJEU has raised a number of questions as to the potential implications of ADM in the context of credit scoring services. The decision that there was a close enough connection between the credit scoring output and the decision of the financial institution so as to play a "determining role" in the decision of the financial institution has raised questions about the extent to which this decision may have wider applicability for ADM and other types of risk scoring across financial services.

Given that this decision came to a different conclusion to that of a prior SCHUFA case under the Data Protection Directive, also raises queries as to the possible scope and limitations of its impact. In addition, considering the many and different obligations imposed on the financial services sector and their suppliers as addressed through DORA and other legislation, it is clear that ensuring a consistent approach to risk management is important for ensuring fair and equitable outcomes for all customers and ensuring the better resilience of the financial services sector.

It is also apparent from the distinctions made in the EU AI Act, between credit worthiness, anti-fraud and cybersecurity measures, that not all decisions based on risk assessment tools are equal in their impact and purpose. This is particularly important when balancing individual rights in the context of determining and acting on fraud and cyber risks where both automation and speed in decision making is essential to containing risks and threats.

The facts in the SCHUFA judgment by the CJEU relate to credit scoring in the context of loans. If the CJEU approach is applied to a wider range of financial services use cases, it yields unhelpful and inconsistent approaches, which therefore supports a narrower interpretation of the decision based on the facts of the case. For example, ADM in the context of identifying cyber risks and fraud require automated, consistent and timely responses to be effective and to comply with financial services and other legal and regulatory obligations and to better safeguard customers. ADM in the context of marketing or non-material decisions also yields a very different impact from decisions about credit (including as between essential or discretionary spend).

The CJEU decision in relation to SCHUFA raises some important issues in the intersection of the GDPR and financial services laws and regulations. However, it is also clear that ADM outputs do give rise to very different outcomes and impacts, and so the complexity and nuances in this area require narrow rather than broader interpretations of the recent CJEU decision to remain credible.