**CJEU Case in SCHUFA Has Far Reaching Implications Beyond Credit Scoring**

**Martin Abrams, Emeritus**
**Lynn Goldstein, Senior Strategist**

The European Court of Justice opinion, SCHUFA, that credit scoring constitutes automated decision-making under GDPR Article 22(1) has broader implications beyond credit-scoring. The ruling by the court "to fill a legal gap" implies that the risk scores produced by businesses like fraud detection and identity verification are automated decisions. It suggests controllers will need to obtain consent before calculating creditworthiness or other types of algorithm-based scoring that are used in a wide variety of business processes.

The court's opinion is inconsistent with modern data analytics and well-established credit scoring practices and may be at odds with the evolving role analytic driven decision-making plays in many aspects of life. These analytic processes reflect the concepts "thinking and acting with data." Thinking with data is the robust use of data to create new insights; use of those insights to affect individuals is acting with data. Although the score in SCHUFA related to a particular individual, until that score was used by a lender – acting with data – that score itself had no impact on an individual. GDPR Article 22 only concerns acting with data. The CJEU overlooks the distinction between thinking and acting with data in order to reach a broad interpretation of the term "decision" in GDPR Article 22(1).

Big data were barely understood, and complex analytics were in their infancy, when the GDPR was adopted in 2016. The GDPR is intended to be technology neutral in many respects, but it has some gaps when it comes to regulating advanced analytics. Based on information contained in the order for reference, the court in SCHUFA determines that, in order to fill a legal gap – the data subject cannot obtain access to meaningful information about the logic involved in the score established by credit information agencies from the financial institution the data subject applied for a loan from and the credit information agency is not obliged to provide that information – that score is an automated decision for the purposes of GDPR Article 22(1). In our view, no such gap exists in the GDPR, but even if it did exist, the court should not have presumed what the relationship between the credit information agency and the financial institution is. In doing so, the CJEU reaches an incorrect decision.

The GDPR does address how to obtain access to the information at issue here. Usually, controllers and processors enter into agreements which require the processor to assist the controller in responding to such access requests. So, data subjects can obtain access to meaningful information about the logic involved in automated decision-making from the controller, the bank.

The issue in the case is what is the relevant decision? The act by which a bank agrees or refuses to grant credit to the applicant? The act by which SCHUFA derives the score from a profiling procedure? The court recognizes that the answer to this question

depends on the facts in each case. The problem with the opinion is that the court goes on to make a series of incorrect presumptions about how credit scores are applied to conclude that the credit score is the decision. Ultimately, because of the fact driven nature of the inquiry, the court's decision may not matter in the financial services industry. However, the broad holding that the court reasoned it should reach because of the absence of a legal definition of the term "decision" in the GDPR means that there are many broader implications for other industries and sectors.

For example, scoring is used in retail transactions to identify fraudulent transactions. "Machine learning scores transactions in real time by analyzing factors such as device information, IP address, and location in order to identify potential fraud in ecommerce transactions. If a customer usually pays with a credit card but suddenly switches to a different payment method, it may indicate that their account has been compromised and a real-time notification is sent." Detecting Retail Fraud

Another example is in healthcare. We all are familiar with the scores we receive when we get our blood test results. Are those decisions? The number determines whether a result is diabetes or not. If the doctor solely relies on the score, is the blood test result an automated decision?

In the SCHUFA case, if the court's determination that there is a gap in the GDPR because the data subject cannot obtain access to meaningful information about the logic involved in automated decision-making from the bank because the credit bureau, not the bank, has it, then the court just should have interpreted the law rather than made new law. This judicial activism in unwarranted particularly when the EU AI Act which governs credit scoring will be coming into effect soon.

While banks and credit information agencies may be able to get around the holding in SCHUFA because the facts are different, the court's ruling has implications for other businesses providing AI or other analytical scoring.

**ANALYSIS OF THE CASE**

SCHUFA Holding AG is a German credit information agency that provides its clients, financial institutions, with information on the credit worthiness of individuals. SCHUFA provided a financial institution with a score for OQ which served as the basis for the refusal to grant the credit for which OQ applied. OQ then requested SCHUFA to erase the entry concerning her and to give her access to her data, but SCHUFA merely informed her of the score and, in broad outline, of the principles underlying the calculation method for the score, without informing her of the specific data included in that calculation or of the relevance accorded to them in that context, asserting that the calculation method is a trade secret.

OQ brought a case against SCHUFA. The court stayed the case and referred to the CJEU for a preliminary ruling on the question of whether GDPR Article 22(1) is to be interpreted as meaning that the automated establishment of a score by the credit

information agency concerning the ability of a data subject to service a loan constitutes a decision within the purview of GDPR Article 22(1).

**CJECU HOLDS CREDIT SCORE IS AN AUTOMATED DECISION**

In holding that the creation of the score, itself, was an automated decision, the CJEU broadly interprets the term "decision. In determining what is the relevant "decision," the CJEU observes there is, on the one hand, the act by which a bank agreed or refused to grant credit to the applicant, and on the other hand, the score derived from a profiling procedure conducted by SCHUFA. The CJEU was unable to answer this question because the answer depends on the way in which the decision-making process is structured in each particular case. The CJEU states that this process typically includes several phases: profiling, establishment of the score, and the actual decision on the grant of credit. The CJEU speculates that although a financial institution can take on this process, there is nothing to prevent it from, by contract, assigning certain tasks, such as profiling and scoring, to a credit information agency. The CJEU then incorrectly speculates that the decision-making process could be conceived in such a way that the scoring by the credit information agency predetermines the decision by the financial institution to grant or refuse to grant credit, Thus, if the scoring were carried out without any human intervention that could verify its result and the fairness of the decision with respect of the credit applicant, the CJEU thinks it logical for the scoring itself to constitute the "decision" under GDPR Article 22(1).

The CJEU then determines the information contained in the order for reference suggested that the score established by a credit information agency and transmitted to a financial institution generally **tends** to predetermine the financial institution's decision to grant or refuse to grant credit to the data subject. Even though the CJEU acknowledges that the facts need to be assessed in each individual case, the CJEU concludes that the score itself is a "decision" within the meaning of GDPR Article 22(1).

**A GAP IN LEGAL PROTECTION?**

The CJEU states that it is reasonable to draw this conclusion because a strict reading of GDPR Article 22(1) would give rise to a gap in legal protection. On the one hand, SCHUFA would not be required to provide information to the data subject under GDPR Article 15(1)(h) since it would not be the one making an "automated decision" within the meaning of GDPR Articles 15(1)(h) and 22(1). On the other hand, the financial institution to whom the score is communicated cannot provide information under these Articles because it does not have it and would be unable to review the evaluation of the creditworthiness of the credit applicant if the decision is contested.

To avoid this perceived gap, the CJEU proposes an interpretation of GDPR Article 22(1) which it thinks considers the real impact of scoring on the data subject. The CJEU thinks this approach logical as the credit information agency, should, in general, be the only entity capable of responding to requests from the data subject based on the rights guaranteed by GDPR Articles 16 (right to rectification) and 17 (right to erasure), The CJEU wrongly observes that the financial institution generally is not involved in either

collecting those data or profiling where those tasks are “assigned” to the credit information agency.

There is no gap in the GDPR. The CJEU says that SCHUFA is the only entity capable of responding, but not obligated to respond, to data subject requests under GDPR Articles 15 – 17, and that the only way to solve this gap is to conclude that a score is a decision under GDPR 22(1). The CJEU is incorrect. The CJEU makes incorrect assumptions about the credit information agency – financial institution relationship (the CJEU does not refer to any information contained in the order for reference about the relationship between the credit information agency and the financial institution). This relationship is fact based and must be determined in every case, but generally the financial institution is the controller, and the credit information agency is the processor.

When there is a controller-processor relationship, under GDPR Article 28(3), the controller and the processor must enter into a contract that governs the processing the processor does for the controller. Under Article 28(3)(3), the contract must provide that the processor assist the controller in fulfilling “the controller’s obligations to respond to requests for exercising the data subject’s rights laid down in Chapter III.” Articles 15 – 17 are in Chapter III. Therefore, even though the financial institution does not have information about the score, when it receives a request from its customer, the contract it has with the credit information agency requires the credit information agency to assist financial institution in:

- Reviewing the evaluation of the creditworthiness of the credit applicant if the decision is contested, and
- Responding to requests based on the right of access to data upon which the decision was based, the right to rectification where personal data to carry out scoring proved to be inaccurate, and the right to erasure where those data have been unlawfully processed.

Thus, there is no “legal protection gap;” the controller can provide the information when the processor has it because the contract between the controller and the processor requires the processor to assist the controller in providing information in response to requests in Chapter III.

**CREDIT SCORING AND THE AI ACT**

The result in SCHUFA is inconsistent with modern data analytics and well-established credit scoring practices. Both of these processes reflect the concepts “thinking and acting with data.”

Thinking with data is the robust use of data to create new insights; use of those insights to affect individuals is acting with data. Part of thinking with data is determining the likelihood of an event happening. In developing the scoring mechanism, SCHUFA was a controller but not using data to make a decision on an individual. Credit scores are not stored by bureaus. They are derived at the time of the request. When SCHUFA determined the credit score at issue here, one could argue about whether it was thinking or acting with data. What is not debatable is that in certain factual situations, the credit information agency is acting as a processor for the bank. Although the score

related to a particular individual, until that score was used by a lender – acting with data – that score itself had no impact on an individual. GDPR Article 22 only concerns acting with data. The CJEU overlooks the distinction between thinking and acting with data in order to reach a broad interpretation of the term “decision” in GDPR Article 22(1).

There is no gap in legal protection; however, if there were, let the new EU AI Act cover it. This broad reading of the term “decision” by the CJEU is unnecessary.. Under the new EU AI Act, high-risk AI systems are those that pose significant risk to fundamental rights, such as those used for credit scoring. High-risk AI systems must comply with strict rules on data quality, transparency, human oversight, accuracy, robustness, and security. Rather than shoehorn the scoring practices at issue in SCHUFA under the GDPR, let the new AI Act come into effect and let the practices at issue in SCHUFA be governed by it. Not every issue involving personal data must go through the GDPR. The GDPR does address how to get the information at issue here, but even if it did not, then the new AI Act addresses how to get it.

**CREDIT SCORING**

Credit scoring has existed for a longer period of time in the U.S. than in the EU. Some learnings in the U.S. have relevance. When David Medine was director of financial practices at the FTC, he said he preferred decisions based on credit scores to those made by lending officers with possible prejudices, Time has shown that scoring expanded credit further and deeper into populations. The inconsistent data pertaining to populations baked prejudice into the process. It was and is a data issue. A credit score is a tool to make better decisions. Not perfect decisions, but better decisions. Credit scores are based on probability. The logic could be explained by saying that if there were a hundred consumers whose data looked like you, x number would go bad over a determined period of time. Bad could be a credit default or a significant delinquency. Explaining the logic in those terms is a doable task by the model developer.

The concept of scoring for significant decisions has been more sensitive in the EU than the U.S. That is why making the logic transparent is important. However, defining the creation of the science behind the score as decisioning has ramifications. GDPR Articles 9 and 89 come into play and impede conducting the science. Scoring has been sensitive in Europe for over 25 years for several reasons. First, the protection of human dignity – preventing the data subject from being subject to a decision based solely on automated processing. Second, the data in Europe was a negative, not full, file.

There is no gap in the GDPR. Going beyond the information contained in the order for reference and making incorrect assumptions about the credit information agency - financial institution relationship led the CJEU to broadly interpret the term “decision” in GDPR Article 22(1) in order to address a nonexistent gap. Even if there were a gap, it is not unusual for gaps to exist in legislation; there is nothing wrong in not having anticipated every possible use of technology when the GDPR was drafted, especially

when new legislation, the AI Act, is awaiting final passage that will address this new technology.