8 February 2024

REPORT ON THE GENERAL DATA PROTECTION REGULATION

OUR RESPONSE TO THE EUROPEAN COMMISSION'S CALL FOR EVIDENCE

A. EXECUTIVE SUMMARY

Ensuring responsible lending practices is paramount in safeguarding consumers from undue financial strain. The pivotal role of credit information in facilitating affordable finance and mitigating over-indebtedness cannot be overstated.

However, challenges arise from inconsistencies in the interpretation and enforcement of the General Data Protection Regulation (GDPR) by national Data Protection Authorities (DPAs) across European Union (EU) Member States. These disparities, coupled with the disproportionate application of GDPR provisions and a lack of unified guidance, impede the establishment of a level playing field for privacy practices. This situation not only poses a risk of increased consumer over-indebtedness but also hinders innovations within the credit information system.

Variations in the interpretation and enforcement of key articles related to data subjects' rights contribute to uncertainties within the Single Market. The processing of publicly available data in credit databases has, until recently, been subject to discrepancies, further complicating matters.

Credit Reporting Agencies (CRAs) express concerns about perceived imbalances in GDPR enforcement, particularly regarding data subjects' rights such as erasure or the right to object. These concerns extend to instances involving credit inquiries that do not result in credit granting or the verification of payment default information.

The absence of clear guidance exacerbates the situation, especially in cases where the GDPR falls short in providing necessary clarity. A notable example is the lack of consistent guidance on the use of legitimate interest as a lawful ground for data processing in credit referencing activities. Compounded by the European Data Protection Board's (EDPB) delays in issuing guidelines, this creates a challenging environment for industry players.

Members of ACCIS assert that the GDPR has not streamlined the adoption of new technologies and methods. Despite claims to the contrary, the GDPR presents challenges for business units to explore, implement, and service emerging opportunities. Additionally, sectoral legislation often complicates matters by either complementing consumer rights recognised in the GDPR or mirroring its provisions with adaptations, leading to duplication of compliance burdens and potential contradictions.

In light of these challenges, we urge the European Commission to ensure consistent application of the GDPR, specifically in the context of credit markets. We stand prepared to collaborate towards this objective, aiming to create a regulatory environment that benefits and protects the rights of citizens involved in credit transactions.

B. INTRODUCTION

ACCIS is the voice of organisations responsibly managing data to assess the financial credibility of consumers and businesses. Established as an association in 1990, ACCIS brings together more than 50 members from countries all over Europe as well as associates and affiliates across the globe.

Responsible lending is vital to prevent consumers from becoming over-indebted. Credit information is central to this process, enabling access to affordable finance and reducing over-indebtedness. Credit reference agencies (CRAs) provide crucial data to credit providers, including credit repayment records, financial data, and publicly available information. CRAs validate, aggregate, and sell comprehensive credit reports to creditors. They also offer services to individuals' consumers and businesses.

More than five years after the GDPR's implementation deadline, CRAs have realised that, although the design of the GDPR works in principle, the very general regulations do not always do justice to the different sector-specific requirements.

Against the backdrop of the European Commission's Call for Evidence to prepare its GDPR report, ACCIS members are concerned about three types of issues:

- Inconsistencies in the interpretation and enforcement of the GDPR by national DPAs across EU Member States
- Disproportionate interpretation and enforcement of GDPR provisions by the said authorities
- Lack of consistent guidance

These problems hinder the establishment of a level playing field for privacy practices and a common understanding of privacy regulations across national credit information markets. Furthermore, these problems negatively affect the credit information system, increasing the risk of consumer over-indebtedness and hindering innovations.

ACCIS members would like to also share additional reflections with regards the intersection between GDPR and innovation.

ACCIS is prepared to collaborate with the European Commission to ensure consistent GDPR application for the benefit of citizens involved in credit markets.

C. INCONSISTENCIES IN INTERPRETATION AND ENFORCEMENT

ACCIS members report several instances of lack of consistency among national DPAs in the interpretation and enforcement of GDPR provisions, in particular in connection to data subjects' rights. The facilitation of those rights by CRAs can be challenging due to the operation of the credit information market. This is particularly true when a weighing of interests is required. CRAs do not possess any client information underlying a registration in a credit database made by a database participant. Collecting all the necessary information to assess the data subject's request is a laborious process. Moreover, the question arises whether receiving such information (which often concerns personal data) is desirable in the context of data minimization. There is also the question of whether the above information is always accurate and up to date, a fact which can hardly be checked. Ultimately, it is up to database contributors to provide CRAs with the necessary information.

Among the inconsistencies encountered, we would like to note:

1. **Inconsistency in the application of Article 14(5)(b) GDPR**. DPAs across different countries apply Article 14(5)(b) differently. For instance, the Norwegian DPA allows data controllers to inform data subjects through their websites when using publicly available personal data. In contrast, the Polish DPA does not accept websites as a valid means of providing information notice. The Hellenic DPA allows the local CRA to inform data subjects through press notifications. Additionally, the Italian DPA has recognised various communication methods, including website privacy notices and digital methods, as acceptable ways to comply with this regulation, especially in the context of the 2019 Italian Code of Conduct for credit reporting systems. Establishing a consistent balancing test under Article 14(5)(b) across the European Economic Area (EEA) would be beneficial. This test would help data controllers compare the cost and

effort associated with fulfilling their information obligations through traditional means like letters with the potential disadvantages to data subjects when providing information on the data controller's website. In any case, the rapid development of technology during the years that have already passed since 2018, when the Regulation came into force, must be taken into account. Consistency in this regard would ensure that data controllers across the EEA make decisions in a manner aligned with their counterparts.

2. **Inconsistencies in the application of Article 15**. DPAs apply Article 15 differently[1]. Some DPAs interpret that Article 15(1)(h) only applies if a decision falls within the meaning of Article 22 of the GDPR. However, other DPAs apply this article to all cases of purely automated processing, extending its scope beyond Article 22 of the GDPR. This inconsistency has led to varying approaches in different jurisdictions regarding data subjects' rights in automated processing scenarios.

> In the case VG Wiesbaden - 6 K 788/20.WI, a German CRA was found to have acted correctly by the DPA. The CRA provided the data subject with some information about their credit score and gave a general explanation of how the scoring system worked. However, the CRA did not disclose specific details about the individual pieces of information used in the calculation of the credit score and how each piece was weighted.
>
> On the other hand, in the case BVwG - W211 2234354-1, a different DPA issued an order to a CRA. This order instructed the CRA to provide the data subject with more comprehensive and meaningful information about the logic behind the credit scoring process. According to this DPA, the information should encompass an explanation of how credit scores are generated, as well as clarifications about the significance of these scores and the expected consequences of the scores for the data subject. This case illustrates a stricter approach by the DPA, emphasizing the need for a more detailed disclosure of the credit scoring process to the data subject. In our view, this approach is not supported by the GDPR.

It is worth noting that the interpretation of the term "copy" varies from one DPA to another. Similarly, the criteria under which a CRA can lawfully charge the data subject for that copy, or the circumstances where data access requests are considered as "manifestly unfounded or excessive," also vary from one DPA to another.

It is also important to emphasise that revealing the logic behind credit scoring process poses a significant risk of potential fraud. Banks highlight that if customers are aware of the scoring model's logic, it may lead them to manipulate specific data or indicators used to generate the score. Additionally, this scoring logic is typically considered a company secret. As a result, information should be provided in general terms avoiding disclosure of too specific details about data inputs and their weights in the calculation.

It is would also be important to clarify the application of Article 15(4): *'the right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others*' The question is whether a CRA, as a controller processing data to protect the banking system and its clients from potential frauds, can refuse to provide a copy of data from the antifraud database based on that paragraph.

3. **Discrepancies in the processing of publicly available credit information.** ACCIS believes that CRAs should not face restrictions in processing publicly available data, as they play a crucial role in providing more accurate data for assessing the creditworthiness of consumers and businesses. However, discrepancies[2] in the processing of publicly available data have created uncertainty in the Single Market. Additionally, there are variations in the length of time that publicly available data can be retained in credit databases, with some countries aligning it with the availability of data in the original source and others being able to retain that data for longer periods for statistical or modelling purposes[3].

[1] The European Court of Justice (ECJ) has clarified in a recent ruling from 7 December 2023 (Case C-634/21) that credit scores must be regarded as an 'automated individual decision' as pert article 22(1) in so far credit score users such as banks, attribute to it a determining role in the granting of credit. Consequently, in those instances and according to the ECJ, the consumer would enjoy under Article 15(1)(h) the right to directly obtain from the CRA 'meaningful information about the logic involved".

[2] For example, in Italy, the DPA-approved code of conduct for credit reporting activities allows business credit information providers to process personal data on unpaid financial obligations made publicly available by the State. The basis for processing is legitimate interest, and consent of the data subject is not required. At the same time, in Spain, a CRA was sanctioned for violating GDPR's purpose limitation principle in its use of publicly available court data on unpaid debts. The Spanish DPA concluded that the CRA could not rely on legitimate interest as the lawful basis for processing this data.

[3] With specific reference to information relating to the granting of a debt discharge, the European Court of Justice has clarified in a recent ruling from 7 December 2023 (Joined Cases C-26/22 and C-64/22) that it is contrary to the GDPR to keep such information in credit databases for longer than the public insolvency register.

D. DISPROPORTIONATE INTERPRETATION AND ENFORCEMENT OF GDPR PROVISIONS

1. **Disproportionate use the of right of erasure in Article 17.** A particular problem reported by an ACCIS member is that, due to a recent national verdict, the local credit database is obliged to process removal requests initiated by data subjects, whereas these requests were earlier referred to data furnishers, i.e., the creditors. This has led to a significant increase in removal requests. The fact that a data subject can invoke the right of erasure, as well as other rights, against CRAs as well as against database participants, leads to additional challenges: when a data subject has had their request rejected by a creditor, such a data subject should not be allowed to force a reassessment of the rejection by the CRA, as this could potentially turn it into a body of appeal.

2. **Disproportionate use of the right of to object in Article 21.** Article 21 is most used by data subjects to object to the processing of their payment default data i.e., they have not fulfilled their credit obligations. A member of ACCIS reports that Article 21 is often invoked by unreasonable data subjects, who have several payment defaults and have no realistic use for the Article. This creates an unreasonable administrative burden.

3. **Processing of credit inquiries**[4] **not resulting in credit granting**. In Poland, the DPA opposes the processing and retention of credit inquiries that do not lead to credit being granted by CRAs. This approach disproportionately goes against the fundamental functioning of credit information systems and differs from the approach taken by other DPAs in the Single Market.

4. **Disproportionate verification of payment default information**. The Estonian DPA has issued guidelines that require local CRAs to check all loan documents and payment information for every negative payment remark entered into the database by contributors. This level of verification, while acknowledging the data accuracy principle, is seen as disproportionate by all market participants, especially when CRAs are not parties to the documentation or transactions being verified. This would create an unreasonable administrative burden for the local CRA (i.e., it would require approximately 60-80 lawyers to daily verify payment default underlying loan information).

E. LACK OF CONSISTENT GUIDANCE

CRAs, like any other business entities, require a clear legal framework for their operations. In cases where the law is insufficient in providing this clarity, CRAs seek guidance from their local DPAs. It is crucial for DPAs to allocate resources effectively to provide CRAs with the necessary advice and guidance, enabling them to navigate the legislation in alignment with the legislators' intended objectives.

Some members of ACCIS report that initiating a dialogue with their local DPAs is challenging. This is in stark contrast to their experience with other authorities, such as competition authorities. While still supervisory authorities, DPAs could improve their engagement with data controllers and processors.

1. **Lack of consistent guidance on legitimate interest**. There is a lack of consistent guidance regarding the use of legitimate interest as a lawful ground for data processing in credit referencing activities. Many CRAs have traditionally relied on legitimate interest for processing personal data, especially for purposes like responsible lending, fraud prevention, and economic behaviour prediction. Some European data protection bodies and authorities[5] have recognised the legitimacy of using legitimate interest for these

[4] When a data subject applies for a credit card or any other type of loan, they typically grant permission to the issuer or lender to review their credit report. This credit check is conducted to evaluate the data subject's creditworthiness and determine their eligibility for the loan. Importantly, each such credit inquiry is recorded in the data subject's credit history, but it remains on the credit report for a limited duration. If multiple credit inquiries appear on a data subject's credit report within a short period of time, it can signal to potential lenders that the data subject might be facing financial stress. This pattern of frequent credit inquiries suggests an increased risk for future borrowing because it statistically indicates a higher level of risk. Lenders often interpret a high frequency of recent credit inquiries as a sign that the data subject may be seeking credit urgently or struggling financially, which could affect their creditworthiness and the terms offered for a new loan or credit line.

[5] As way example, in its opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, the former Article 29 Working Party stated that “Credit reference checks prior to the grant of a loan are also not made at the request of the data subject under Article 7(b), but rather, under Article 7(f), or under Article 7(c) in compliance with a legal obligation of banks to consult an official list of registered debtors”. The UK ICO applies a rather flexible interpretation of legitimate interest, including direct marketing and commercial interests. In Italy the in Italy, the DPA-approved code of conduct for credit reporting activities links legitimate interest to credit worthiness assessment. The Spanish DPA accepts marketing purposes as a lawful legitimate interest. German DPAs permits

purposes and others, such as marketing. However, certain DPAs have taken a restrictive stance on the use of legitimate interest as a legal basis for data processing[6].

The EDPB has failed to meet its self-imposed deadlines for issuing guidelines and providing legal clarity on this matter. This lack of guidance creates uncertainty for CRAs and their clients regarding the use of legitimate interest in data processing.

2. **Lack of guidance on substantial public interest regarding the use of public interest as a lawful ground for processing biometric data**. Banks are obliged to process personal data for the purpose of preventing fraud and to protect the safety of the banking system, which is allowed under EU anti-money laundering and payment regulations. Given the potential of biometric data for Strong Customer Authentication (SCA) in payment transactions, there is an urgent need to clarify whether such purposes of processing personal data (preventing fraud and the safety of the banking system) shall be deemed as a substantial public interest in the meaning of Article 9(2)(g) of GDPR[7].

3. **Ineffectiveness of specific EDPB Guidelines**. The EDPB has tried to address inconsistencies in the interpretation and enforcement of rules on right of access by means of EDPB Guidelines 01/2022. Our industry does have however lingering concerns about the practicality and burden of complying with those guidelines. Concerns revolve around data controllers facing excessive burdens and disproportionate expectations. Is important here to mention that data controllers remain legally bound to protect the accountability principle. For example, data controllers are expected to tailor information to each requesting data subject, and they may be required to provide meaningful information and clarify the scope of Data Subject Access Requests (DSARs) upon individual requests.

F. GDPR AND INNOVATION / NEW TECHNOLOGIES

In a broader sense, GDPR has not simplified the facilitation of new technologies and methods. It presents a challenge for the relevant business units to explore, implement, and service emerging opportunities within the intricate GDPR framework.

GDPR aims to ensure that new technologies are developed responsibly. For instance, privacy by design mandates the consideration of data protection from the outset and throughout a product's lifecycle. Since GDPR itself is intended to remain neutral regarding technology, its overall impact has been to encourage the creation of products with privacy as a fundamental consideration.

We would like to specifically comment on the intersection between GDPR and the revised Consumer Credit Directive, the Artificial Intelligence Act, and the proposal for a Financial Data Access (FIDA) framework.

1. **Consumer Credit Directive II (CCD II).** Article 18(6) in the revised CCD II introduces "complementary" consumer rights related to creditworthiness assessments (CWAs) that involve profiling or automated processing of personal data. The objective is to extend the existing Article 22 of the GDPR, which grants rights to consumers when decisions with significant legal effects are solely based on automated processing. The argument made by ACCIS is that introducing these additional rights, irrespective of the degree of human involvement in credit decisions, could lead to a situation where consumers request manual reviews for almost every decision. This could disrupt processes, increase costs, reduce efficiency, and hinder innovation in the lending sector. We strongly believe that digitalization and automation are advantageous for providing faster, more efficient, and objective credit assessments.

processing of positive and negative credit data based on legitimate interest or compliance with legal obligations. Romania DPA also has interpretations favoring the use of positive credit data.

[6] Indicatively, the Dutch DPA seems to apply a strict interpretation of legitimate interest excluding commercial interests, interests of profit maximization and monetizing personal data (see Case C-621/22, currently in front of the European Court of Justice).
See Case C-621/22, currently in front of the European Court of Justice, where the Dutch DPA argues that Article 6(1)(f) of the GDPR covers only interests enshrined in law (positive test). in Spain, the DPA has rejected the notion of legitimate interest for private companies to process credit information unless the data pertained to unpaid debts.

[7] It is important to highlight that both behavioral biometrics and artificial intelligence are acknowledged as crucial tools or technologies intended for deployment in the effort to minimize and forestall fraud within the payments market. This recognition is explicitly outlined in recital 103 of the 2023 proposal for a Payments Services Regulation, underscoring the substantial public interest in ensuring the effective operation of the payments market, as duly acknowledged in Recital 98 of the same policy document.

2. **Artificial Intelligence (AI).** The EU AI Act classifies AI systems used for evaluating the creditworthiness of individuals or establishing their credit scores as high-risk (Annex III 5.b). The impact assessment for this classification aims to justify the potential risks associated with using AI in the credit industry, including threats to fundamental rights and the possibility of discriminatory outcomes. ACCIS's standpoint is that CWAs and credit scoring should be excluded from this high-risk classification because the risks associated with AI in their industry are already effectively mitigated by existing regulations, especially the GDPR. The GDPR provides rights and protections for consumers, such as access to profiling data and the ability to challenge input data, which are seen as adequate safeguards. These rights ensure that the use of AI in credit assessments complies with the GDPR principles and fundamental rights, eliminating the need for additional regulation.

Details of relevant GDPR provisions for the AI Act:

1. Notification of data use. Lenders must inform consumers if they gather data about them from external databases or use credit scoring. This information is typically provided in the lender's privacy notices, as required by the GDPR.
2. Right of access to profiling data. Consumers have the right to access details of the personal data used for profiling. This is in accordance with Article 15 of GDPR. They can verify the information held by the lender or third parties, such as databases.
3. Scoring models. Scoring models, including those used for credit scoring, must adhere to the fundamental principles of GDPR, such as lawfulness, fairness, transparency, accuracy, data minimization, and purpose limitation. They must also comply with EU Charter of Fundamental Rights principles, including non-discrimination.
4. Right to challenge input data: Consumers have the right to challenge the input data used in their credit scores (right to rectification, Article 16 GDPR) and the right to request erasure (Article 17 GDPR).
5. Enhanced protections for solely automated decisions: When a credit decision is solely based on an automated process and has a significant legal effect on the individual (e.g., an online credit rejection), consumers enjoy greater protection. This includes the right to receive meaningful information about the logic and consequences of the automated decision-making (as per Articles 13(2)(f) and 14(2)(f) GDPR). Consumers also have the right to request a manual review, express their opinion, and contest the decision (Article 22 GDPR). Additionally, high-risk data processing may require a data protection impact assessment (DPIA) and consultation with the supervisory authority (Articles 35 and 36 GDPR).

3. **FIDA:** FIDA is a legislative proposal to extend Open Banking data-sharing obligations, which currently apply exclusively to payment accounts data, to encompass nearly all financial services data. The FIDA framework would establish clear rights and obligations for managing customer data sharing in the financial sector beyond payment accounts. This includes granting customers the option, though not an obligation, to share their data with data users, and imposing the obligation on customer data holders to provide these data to users. While FIDA uses the term "permission" rather than "consent" or "explicit consent," it is evident that the regulator's intention is to establish data access from the perspective of individuals and companies owning the data. As mentioned earlier, CRAs primarily rely on legitimate interest and, also, public interest as a legal basis for processing personal financial data, which could potentially result in a clash of legal bases.

In essence, the European Commission and other legislative bodies appear to increasingly treat the GDPR as a "lex generalis" or a general framework for data protection. In simpler terms, while the GDPR provides a general set of rules for data protection, sector-specific laws are being introduced that can potentially contradict or go beyond GDPR rules. This situation is creating confusion among businesses and individuals about which rules to follow and is causing legal uncertainty in how data protection is regulated across different sectors.

To conclude, we would like to address the **treatment of profiling in recent legislative acts**. In the Digital Markets Act, gatekeepers are required to provide independently audited descriptions of how profiling is conducted (Article 15). The Digital Services Act mandates that online platforms ensure that users of social media and search engines are aware of the data collected for targeted advertisements (Article 27). In the draft final text of the AI Act, AI systems involving any form of profiling are considered high-risk, irrespective of whether a specific AI system poses a significant risk to the health, safety, or fundamental rights of individuals.

A common thread running through these legislative acts is the notion that profiling is inadequately regulated within the GDPR, and therefore, new legislation is needed to address unattended risks. ACCIS holds a different perspective. Profiling is a form of data processing already covered by the GDPR. The GDPR offers a higher level of protection for automated decisions, including profiling, that have legal or similarly significant effects on individuals (Article 22 GDPR). Consequently, a "data protection impact assessment" (DPIA), required for high-risk data processing, is not inherently mandated for profiling, except in cases covered by Article 22 GDPR (refer to Article 35.3.a GDPR).

Moreover, the interpretation of profiling provided by the Working Party 29, endorsed by the European Data Protection Board (as seen in the Guidelines on automated individual decision-making and profiling), clarifies that profiling is merely a specific type of processing activity and does not necessitate any special requirements. In fact, it can even be conducted under the legal basis of legitimate interest as defined in Article 6.1.f of the GDPR.

ACCIS

ACCIS represents the largest group of credit reference agencies in the world. ACCIS brings together 40 members across 28 European countries and 11 associate and affiliate members from all other continents.
EU Transparency Register: 21868711871-63

Contact

ACCIS Secretariat
Rue du Luxembourg 22-24
1000 Brussels
Belgium
Tel: +32 2 761 66 93
secretariat@accis.eu

Follow us !

Twitter
Linkedin
Youtube