FEBIS Comments on EDPB Guidelines on Legitimate Interest – 2024

FEBIS members are business information providers ("BIP") whose core business model is to provide creditworthiness assessments, credit scores and business information reports on businesses for businesses. Contrary to credit rating, credit scores are done on all businesses' population of a country, using data management and processing, statistical analysis and analysis technologies owned by business information providers. The raw data used is composed in part of public and open data made available for re-use (as outlined by the Open Data directive 2019/1024 and its implementing regulation 2023/138) but also a lot of value-added data managed by business information providers under proprietary databases and technologies. Credit scores and business information reports are then used by credit managers and *businesses when assessing their trade counterparts, making trade credit decisions, doing compliance checks, and fulfilling Know-Your-Customer obligations inter alia. Important to say, business information and credit scoring providers are* ***not*** *financial institutions or financial providers as they do not lend money; they provide data solutions helping the assessment for trade credit decisions to be made***.**

The decision whether to engage with a trade counterpart remains with the company receiving the credit risk assessment or other information. ***SME companies have less data themselves and therefore run a higher risk on not collecting receivables. Business information providers help to equalize that competitive disadvantage****. Losses from not collectable receivables led to the banking crisis. The bailout was in big part done with taxpayers' money. All paying customers therefore have a high interest in a solid credit management and in consequence in effectively working business information providers.*

FEBIS welcomes the European Data Protection Board guidelines' objective to better qualify the use of legitimate interest as a valid data processing ground and the will to better qualify the use of legitimate interest for data processing. Some guidelines are quite useful as they bring clearer context on the use of legitimate interest, but we also feel that some points would require further clarification in the way business information providers can rely on legitimate interest for data processing.

We would like to take the opportunity to enhance our views and interpretations of the guidelines on the following elements, outlining where we support the guidelines but also where we could welcome further details to be addressed.

- **All legal bases for data processing are equal**: as outlined in the **introduction** part of the guidelines, article 6 of the GDPR provides for several data processing grounds and none of them should have prominence over the other. FEBIS welcomes this approach which ensures that legitimate interest is as valid as consent or any other legal ground for data processing. However, the **executive summary** of the guidelines somehow seems to put in place a problematic potential subordination of the legitimate interest to other legal

bases of art 6. This should not be inferred by any means, and we would welcome a clearer recognition that legitimate interest is as valid a ground as others and that there is indeed no hidden hierarchy of data processing grounds outlined in article 6 of the GDPR.

- **Legitimate interest can be used for commercial purposes:** as outlined in the CJEU, judgement of 4 October 2024, Case C-621/22, Koninklijke Nederlandse Lawn Tennisbond, the fact that data is used or reused for commercial purposes does not rule out the possibility to rely on the legitimate interest as data processing ground. This judgement is of great importance also for business information providers who rely on legitimate interest to process the personal data that they use for their services and products. Another valid recognition in the guidelines is the reference to the CJEU Schufa case (Case C-634/21), which recognizes the legitimate interest possibility for credit scoring. A business information provider can have a legitimate interest to process data for a commercial purpose, especially when this purpose is based on the needs / requirements of its customers, i.e. businesses.

- **The weight of the balancing test elements**: Paragraph 6 of the EDPB guidelines brings the useful clarification that the interests or fundamental freedoms and rights of data subjects do not override the legitimate interests of the controller **or those of a third party**. This is welcome by FEBIS members as it shows the balancing test is on equal footing between interests of the data subject and legitimate interest of the data controller and the ones of the third parties that are represented. However, paragraph 45 lists factors that must be considered in the balancing of interests and that may affect the rights, freedom and interests of the data subjects. This list has a strong focus on data processing and contractual decisions in the financial environment and could risk putting in place a de-facto hierarchy of the balancing test items, which would be quite problematic and would lack explanation on how the factors can be assessed. Furthermore paragraph 33 states that disproportionate effects are to be avoided in the balancing process, which is fine, but we would also like to get more clarification on what constitutes a disproportionate impact. What would be logical is that the «consequences» be restricted here to consequences outside of the «legitimate interest». The «side consequences» one might say. To be set apart from the consequences which are the logical suit of the intended interest and purpose should be set apart.

  In addition, considering that paragraph 37 states “The fundamental rights and freedoms of the data subjects include the right to data protection and privacy, but also other fundamental rights and freedoms, such as the right to liberty and security, freedom of expression and information, …”, it is important to underline that AML/CTF (Anti-Money Laundering and Combating the Financing of Terrorism) measures are essential in all the financial system to contribute to freedom, liberty, security and better known decisions. For this reason, BIPs need to have a legitimate interest by default in having access to the business registers, including the UBO-register (Ultimate Beneficial Owner).

- **The ability to take third-party interests into account** is recognized by paragraph 20 which is welcomed and in line with the prevailing opinion to date and the decisions of the CJEU, and therefore hardly surprising. But paragraph 30 could be understood as a supposedly higher hurdle for processing based on third-party interests and increases the requirements for balancing due to an assumed lower expect ability of processing in the third-party interest. This should not mean that processing data for third-party interests is lower, as, in many cases, third parties have either their own legitimate interest or even a legal obligation to access and process data such as in the AML and fight against corruption or fraud context, where the legitimate interest of providers such as business information providers has been recognized by the 6th AML directive. It should therefore be clear that business information providers can process data based on their legitimate interests but also on the legitimate interests of their clients or obliged entities and that this also applies in the weighting of the balancing test elements.

- **No exhaustive list of legitimate interests**: Paragraph 16 of the guidelines clarify that there is no exhaustive list of interests that can be considered legitimate. In the absence of a definition of this term in the General Data Protection Regulation, a wide range of interests can in principle be considered legitimate. In addition, explicit reference to the assessment of the creditworthiness as a legitimate interest is made through the mention of the CJEU Schufa case, showing therefore that case law recognizes that our sector has the possibility to have legitimate interest. Information sharing (including sharing information of personal data) is of fundamental importance for any democratic society e.g. in supporting economic transparency, fostering fair competition, promoting financial stability, contributing to economic development and contributing to sustainable business decision-making and practices. Business information providers role in helping businesses validate information (e.g. validating the accuracy of information shared by a data subject) is a legitimate interest as it is of outmost importance for correct decision making. Moreover, regarding right to objection (point 4) and right to erasure (point 5), business information providers have compelling legitimate grounds and overriding legitimate grounds to keep the registers updated, correct and complete.

- **Not all profiling are automated decisions**: as outlined in paragraph 82, not all data processing activities that involve profiling are to fall under art 22 of the GDPR and be recognised as automated decisions.

- **Data collected from third parties should be deemed as accurate as first-party data**
In the paragraph 84, the EDPB implies that if the data was not collected from the data subject, the likelihood of inaccuracies and incompleteness is generally higher in such situations. FEBIS opposes this assertion as their members perform high data validation processes and ensures that the data they collect from or for third parties, and in particular business registers is accurate and updated. Especially in fraud and late payment cases it is evident that the data subject itself is not a reliable source, whereas BIPs add values to “first party data”, increasing the informative power.

- **Legitimate interest to be subsumed under fraud prevention**: FEBIS welcomes paragraph 102 that indicates a comprehensive understanding by the EDPB of the facts / processing to be subsumed under fraud prevention, thus recognizing also the provisions of the 6th AML directive. But point 101 states that the requirements for data processing for the purpose of fraud prevention are strict in light of the impact that such processing can have on the data subjects. This creates the impression of a particularly high hurdle for the balancing of interests due to the intrusiveness of data processing for fraud prevention and could be detrimental to getting accurate information. This could also lead to negative consequences as fraud prevention is both necessary and beneficial to businesses as it protects them from fraud and financial harm. Point 106 also mentions that a generic reference to the purpose of "fraud prevention" in for example the privacy policy is not sufficient. This raises the question of the depth and detail with which the EDPB believes processing purposes should be named and documented. It should be recognized that setting too detailed requirements can lead to too complex privacy policies and overly burdensome documentation requirements as well as leading to the disclosure of information which in itself could counteract the fraud prevention purpose.

- **Demonstrating that the processing meets the reasonable expectations of the data subjects**: Paragraph 53 of the guidelines states that compliance with the information obligations is not sufficient in itself to consider that the data subjects can reasonably expect a given processing. FEBIS considers that conscientious fulfillment of the information obligations should be seen as a measure of high importance in the assessment of the data subject's reasonable expectation and that this should be reflected in the guidelines.

Furthermore, we think the following points are missing from the guidelines and could usefully be addressed:

- **The question of sole traders acting in their business capacity**: The question of **sole traders** is key because depending on the EU regulation considered, one finds different approaches. GDPR does not explicitly mention sole trader's data being established as a legal person but some interpretation from the EDPB and some DPAs consider some sole traders' data as personal data. This opposes to general EU Consumer law which defines a consumer as "*a natural person who is acting for purposes other than his or her trade, business or profession*;" and therefore someone who is acting for purposes which belong to his trade, business or profession should not be seen as a consumer but as a business. The EU Data Act also talks about **enterprises** and defines an enterprise as "*a natural or legal person which in relation to contracts and practices covered by this Regulation is acting for purposes which are related to that person's trade, business, craft or profession*" (art 2 -8 of the Data Act).
  The draft FIDA proposal does not give a definition of sole traders but it would infer from the difference between consumer and customer that sole traders should be seen as customers and therefore have their data in the scope of FIDA.

For sole traders, VAT is deductible. That is not the case for private persons. If sole traders are businesses from tax perspectives it doesn't make sense to treat them as private persons from a data protection perspective.

FEBIS would strongly recommend a clarification based on the CAPACITY under which a natural person interacts and to consider that natural persons acting in business capacity should be considered equal to legal persons in all relevant legislation. It is the capacity in which an individual interacts which should be considered ie private for private capacity, and available for re-use for legitimate purposes for business capacity.

- **The interplay of the GDPR and the Open Data Directive** : although the guidelines do not mention EU open data policies that put in place a right to access and re-use public sector information, a former mention of this intertwine had been done by the article 29 working party in its opinion on Open Data and PSI reuse. As business information providers are re-using PSI data for economic transparency and the fight against fraud, clarifying the interplay between the Open Data application and the GDPR is also quite crucial, especially when tackling the sole traders or legal directors and shareholders' information that is needed for economic transparency and for which a legitimate interest of data processing is applicable.