16.01.2020

# ACCIS' contribution
# EDPB's Guidelines 4/2019
# Art. 25 Data Protection by Design and by Default

*Established in Dublin in 1990, the Association of Consumer Credit Information Suppliers (ACCIS) represents the largest group of credit reference agencies in the world. ACCIS brings together 42 members across 28 European countries and 8 associate and affiliate members from all other continents.*

ACCIS welcomes the European Data Protection Board's (EDPB) draft guidelines on Article 25, Data Protection by Design and by Default (DPbDD), under the General Data Protection Regulation (GDPR), and invites the EDPB to address the issues below to provide the necessary legal certainty to credit reference agencies.

1. Our key **concerns in this document are in regard to the examples** under "*Lawfulness*" i.e. a bank plans to offer a service to improve efficiency in the management of loan applications; under "*Accuracy*" i.e. a bank wishes to use artificial intelligence (AI) to profile customers applying for bank loans as a basis for their decision making; and under "*Storage limitation*" i.e. a controller that administers a membership.

2. In connection to the **management of loan applications**, we suggest that the following should be taken under consideration:

   - Contrary to what the guidelines seem to imply, creditworthiness assessments should and rely in practice as much on the information provided by the data subject as they do on data provided from other sources, like Credit Reference Agencies (CRAs). So, there is no preference "by default" for the information provided by the data subject. An example is when the data subject is not interested that certain information - for example, record of a missed repayment held by a CRA - enters the creditworthiness assessment process.

   - It is very unusual that a credit institution asks for data to a public authority, so the example is misleading.

   - The guidelines imply that access by the bank to a specific, external set of information about the data subject needs to happen on the basis of consent. In relation to the example in the first bullet point above, a data subject that knows that a negative record about his/her creditworthiness is held in an external database is not in a position to freely provide consent. It is hence apparent that the appropriate legal basis for the processing in question is not the data subject's consent, but art. 6 para.1 (f): the bank has a legitimate interest to consult external sources in order to evaluate creditworthiness of the applicant. Because of that legitimate interest, there is no consent needed. In recognition of that, some European Data Protection Authorities - for example, in Germany - have stated that consent is not an admissible legal ground for consulting external databases before a loan is granted by a bank.

   For the reasons provided above, **we recommend that this example is either deleted or radically redrafted**, to ensure it is consistent with current loan origination practices in the financial industry.



**ACCIS IVZW • p/a Interel • Rue du Luxembourg 22-24 • B-1000 Brussels**
+ 32 2 761 66 93 / secretariat@accis.eu / www.accis.eu / EU Transparency Register: 21868711871-63

3. In connection to the **use of artificial intelligence**, we think that the example as it stands could be taken to indicate that solely automated decision-making based on AI is never permitted, which is not what the GDPR says, as it is permitted in specified circumstances[1]. We, therefore, suggest the following **alternative wording**:

   *A bank wishes to use artificial intelligence (AI) to profile customers applying for bank loans as a basis for their decision making. When determining how their AI solutions should be developed, they are determining the means of processing and must consider data protection by design when choosing an AI from a vendor and when deciding on how to train the AI.*

   *When determining how to train the AI, the controller must have accurate data to achieve precise results. Therefore, the controller must ensure that the data used to train the AI is accurate.*

   *Granted they have the legal basis to train the AI using personal data from a large pool of their existing customers, the controller chooses a pool of customers that is representative of the population to also avoid bias.*

   *Customer data is gathered from their own systems, gathering data about the existing loan customers' payment history, bank transactions, credit card debt, they conduct new credit checks, and they gather data from public registries that they have legal access to use.*

   *To ensure that the data used for AI training is as accurate as possible, the controller only collects data from data sources with correct and up-to date information.*

   *Finally, the bank tests whether the AI is reliable and provides non-discriminatory results. When the AI is fully trained and operative, the bank uses the results as a part of the loan assessments.* ~~***and will never rely solely on the AI to decide whether to grant loans.***~~

   *The bank will also review the reliability of the results from the AI at regular intervals.*

4. Driven by the issue of development of AI, we also suggest that the guidelines refer to the obligations and the liability of "designers of technical systems", i.e. producers, suppliers, importers etc., as it is already the case under product liability law.

5. In connection to the example on the **administration of a membership**, we think that the example as it stands could be taken to indicate that deletion of data is always automatic at the end of a given contractual relationship. This is contrary to GDPR, as it is possible to keep data as long as it is necessary for the purposes for which it is processed[2]. It should be kept in mind that "administration of membership" could be just one of several purposes for which the data are being lawfully processed by the controller and not all of those purposes cease to exist on the termination of the membership e.g. the controller could be required to further process the data for compliance with a legal obligation and/or the establishment, exercise or defense of legal claims. We, therefore, suggest the following **alternative wording**:

   *The controller collects personal data where the purpose of the processing is to administer a membership with the data subject, the personal data shall be deleted when the membership is terminated and there is no* ***legal basis for further storage of the data****.*

   *The controller makes an internal procedure for data retention and deletion. According to this, employees must manually delete personal data after the retention period ends. The employee follows the procedure to regularly delete and correct data from any devices, from backups, logs, e-mails and other relevant storage media.*

[1] See art. 20.2 GDPR.
[2] See art. 5.1(e) GDPR.



**ACCIS IVZW • p/a Interel • Rue du Luxembourg 22-24 • B-1000 Brussels**
+ 32 2 761 66 93 / secretariat@accis.eu / www.accis.eu / EU Transparency Register: 21868711871-63

*To make deletion more effective, the controller instead implements an automatic system to delete data automatically and more regularly. The system is configured to follow the given procedure for data deletion which then occurs at a predefined regular interval to remove personal data from all of the company's storage media. The controller reviews and tests the retention policy regularly.*

6. In connection with the **context** mentioned in art. 25 GDPR and **paragraphs 25 and 26** of the guidelines, it should be clear that the compliance landscape for consumer credit information suppliers is wider than just the GDPR. For example, conduct of business requirements with legislative force are imposed on CRAs in a number of EU Member States. A relevant part of that context ("*circumstances of the processing, which may influence the expectations of the data subject*") is the legal framework of the activities of CRAs in those countries. It is, therefore, important that examples and EDPB guidance do not extend further than the requirements flowing from the GDPR as CRAs are balancing compliance across a number of different areas.

7. In various paragraphs of the document - for example, under the **Executive Summary and in paragraphs 2, 35 and 63** - the Guidelines place obligations on controllers to "*demonstrate*" compliance. However, they fail to explain in what way compliance would have to be demonstrated. They also fail to clarify to whom should compliance be demonstrated. We recommend that the guidelines detail how to demonstrate compliance and state that compliance will be routinely demonstrated **"*at the request of the competent supervisory authority*"** unless explicitly stated otherwise. In a similar vein, paragraph 67 mandates the controller to test the privacy design against purpose limitation but fails to explain how.

8. In **paragraph 10**, the guidelines list a few examples of necessary safeguards that act as a second tier to secure data subjects' rights and freedoms in the processing. One of those safeguards is the provision of "***automatic and repeated information about what personal data is being stored***". We think that this safeguard is disproportionate and not consistent with the requirements of Articles 13 and 14 GDPR. A repeated information is not intended there. **We recommend that this safeguard should be deleted**.

9. In **paragraph 61**, the guidelines list key design and default elements in relation to transparency. Among them is "***Universal design***" i.e. information shall be accessible to all, including use of "*machine-readable languages*". Assuming that the objective of this provision is that the privacy notice is provided in a text format (as opposed to an image of text) so that screen-readers can read it, **we recommend that "machine-readable languages" is replaced by "machine-readable text".**

10. Also, in **paragraphs 60-61**, it could be helpful to mention that information to data subjects can be provided "by layers", as suggested in paragraph 35 of WP29 Guidelines on transparency under Regulation 2016/679 (WP260 rev.01). As a business standard, comprehensive information about the data processing is usually provided in the webpage of different credit reference agencies. Layered privacy statements/ notices are effective in helping resolve the tension between completeness and understanding. For that reason, **we recommend that the "layered approach" is explicitly referred to in the guidelines**.

11. In **paragraph 63**, the guidelines list key design and default elements in relation to "*Lawfulness*". Among them is "***Autonomy***" i.e. the data subject should be granted the highest degree of autonomy as possible with respect to control over personal data. In our opinion, data subjects could have been given full autonomy over their personal data if the GDPR had required all processing to be based on consent, and/or had included an absolute right to erasure. This is not what the GDPR did. Instead, there are legal bases other than consent, and the right to erasure is qualified and limited. Suggesting that data subjects should have as much autonomy as possible potentially overrides the balance that has been struck by the GDPR itself. **We recommend that the element "Autonomy" is deleted from the list**.



**ACCIS IVZW • p/a Interel • Rue du Luxembourg 22-24 • B-1000 Brussels**
+ 32 2 761 66 93 / secretariat@accis.eu / www.accis.eu / EU Transparency Register: 21868711871-63

12. Under the same **paragraph 63**, the guidelines refer to "**Balancing of interests**" - where legitimate interest is the legal basis. The guidelines do not clarify to whom should the controller disclose the assessment of the balancing of interests. As disclosure to data subjects would be inconsistent with Article 13(1)(d) / 14(2)(b) GDPR - which just require the controller to disclose in privacy notices what interests are being pursued but not how those interests weigh up against the impact on data subjects - we recommend that this provision clarifies that the disclosure is provided **"*at the request of the competent supervisory authority*".** Similarly, under **paragraph 77** - Key design and default elements for storage limitation – we recommend that the "disclose rationale" behind the retention period is provided **"*at the request of the competent supervisory authority*"**.

13. In the same **paragraph 63**, it is not clearly explained why *"If there is a valid change of legal basis for the processing, the actual processing **must** be adjusted in accordance with the new legal basis."*. We suggest the wording *"If there is a valid change of legal basis for the processing, the actual processing ~~**must**~~ **may** need to be adjusted in accordance with the new legal basis"*

14. In **paragraph 64**, the guidelines define the principle of "*Fairness*". We find that too broad a definition of fairness. It must be possible to process data in a way that is detrimental to the data subject, or else it would never be possible to make any decisions that are adverse to anyone, to flag anyone as a potential credit risk or fraud risk, to disclose data about an individual to a police force in support of a criminal investigation against them, etc. What matters is whether any detrimental effect is justified[3]. **We, therefore, recommend that the word "*unjustifiably*" is inserted before "detrimental, discriminatory, unexpected or misleading to the data subject"**. Consequently, we also recommend that the **word "*unlawfully*" is inserted under the "*Non-discrimination*" element mentioned in paragraph 65** i.e. the controller shall not unlawfully discriminate against data subjects.

15. In **paragraph 65**, the guidelines list key design and default elements in relation to "*Fairness*". For the reasons stated cfr.11 above, **we recommend that the element "Autonomy" is deleted from the list**. In the same list, the element "**Human intervention**" needs clarification. If it means that humans should from time to time review automated decision-making systems, then it is acceptable. If it means that human intervention is always required in any decision-making process, it would be contrary to the GDPR since, as already mentioned in cfr.3 above solely automated decision-making is permitted in specified circumstances.

16. In **paragraph 76**, the guidelines state that measures and safeguards that implement the principle of "*Storage Limitation*" complement certain rights and freedoms of the data subjects, including the right to "profiling". We are unsure why this reference to profiling is made here. **We recommend that the word "profiling" is deleted**.

17. In **paragraph 77**, there is a suggestion that controllers must seek for a 'temporary' storage of personal data. It would be clearer and more according to GRPD to clarify that data can be stored for a period of time necessary in order to achieve the purposes for which the personal data was processed.

18. In **paragraph 86**, the guidelines refer to how technology providers can help controllers effectively implement the principles and the rights of data subjects into the processing. The guidelines, however, refer to one obligation i.e. "*controllers should demand that their technology providers are transparent and demonstrate the costs of developing the solution*" that, although potentially sensible, in unrelated to data protection. **We, therefore, recommend that this obligation is deleted from the list**.

[3] See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/ under "What is fairness?".



**ACCIS IVZW • p/a Interel • Rue du Luxembourg 22-24 • B-1000 Brussels**
+ 32 2 761 66 93 / secretariat@accis.eu / www.accis.eu / EU Transparency Register: 21868711871-63

Contact: Enrique Velázquez, Director General
e.velazquez@accis.eu