Brussels, 28 November 2017

EACB's views on the Article 29 Working Party draft Guidelines on Automated individual decision-making and Profiling and on Personal data breach notification under Regulation 2016/679

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Introduction

The European Association of Co-operative Banks (EACB) welcomes the opportunity to provide the Article 29 Working Party (WP29) with its comments on the draft Guidelines on automated individual decision-making and profiling as well as on personal data breach notification under the General Data Protection Regulation (GDPR) adopted in October 2017.

Comments on the Guidelines on Automated individual decision-making and Profiling

I. Definitions

Letter A 'Profiling' (pp. 6-7 of the draft Guidelines)
EACB members believe that the Guidelines might be putting too much emphasis on data processing operations that have more to do with the simple identification of customers than with the adoption of decisions that might have an impact on them. For instance, the draft Guidelines (p. 7) state that "*simply assessing or classifying individuals based on characteristics such as their age, sex, and height could be considered profiling, regardless of any predictive purpose*". We believe, on the contrary, that the pure processing of static data about an individual cannot be considered, in and of itself, a form of profiling in the absence of activities on the part of the controller aimed at evaluating, analysing or predicting elements linked to the data subject.

II. Specific provisions on automated decision-making as defined in Article 22:

Letter B '"legal" or "similarly significant" effects' (p. 10 of the draft Guidelines) and Letter C 'Exceptions from the prohibition'

EACB members believe that 'legal' or 'similarly significant' effects are interpreted too broadly when it comes to marketing. As a consequence, the draft Guidelines set too strict conditions for profiling where it is '*necessary for the performance of or entering into a contract'.*

- According to Art. 22, the controller can undertake the processing described in Art. 22(1) if one of the exceptions listed in Art. 22(2) applies.
  The WP29 states that controllers may wish to use automated decision making, for example, when conditions presented in the bullet points on page 12 are met. At the same time, it also states that *'these considerations alone are not always sufficient to show that this type of processing is necessary under article 22(2)(a) for entering into, or performance of, a contract.'*
- The example described in the box on page 20 is problematic as well because it questions the necessity of profiling.
- On p. 25 and with regard to the additional conditions that the controller needs to prove in case it continues to process personal data against the data subject's will ('*The controller would also need to prove that: the impact on data subjects is limited to the minimum necessary to meet the particular objective (i.e. the profiling is the least intrusive way to achieve this); and the objective is critical for the organisation.'*), we believe these are too burdensome for the controller and go too far compared with the Regulation's text.

Letter D point 1 'Meaningful information about the "logic involved" and "significance" and "envisaged consequences"'

EACB members welcome the interpretation given to the wording '*meaningful information about the logic involved'* to the effect that the controller should find simple ways to tell the data subject about the rationale behind the automated decision. We appreciate the effort to give an example

(p. 14), including provision to the data subject of the main characteristics considered in reaching the decision, so long as the provision of such information remains general and does not disclose strategic information to competitors.

With regard to the example given under the wording 'significance' and 'envisaged consequences' (p. 15), we agree so long as it provides a simple possibility of implementation and not a requirement. Notably, the development of apps or graphics for the purpose of complying, while certainly possible should the controller wish to pursue such route, is not an obligation that can be derived from the text of the Regulation. We therefore suggest removing this part of the example.

We believe that it should be clear that it is up to the insurer to make use/not use tools (such as apps or graphics) to provide information to the data subject and that the example doesn't give the impression of an implicit obligation for the insurer to provide an app or graphics.

Annex 1 – Good practice recommendations

EACB members believe that the WP29 gives an extensive interpretation of the scope of the GDPR with regards to 'general profiling' (Chapter I, letter C(i)) by recommending to provide information identical to that required by Articles 13(2)(f), 14(2)(g) and 15(h).

Despite the lack of precision in the Guidelines related to the perimeter of the general profiling, it is understood that it mainly concerns profiling for prospecting purposes (advertising, marketing). However, Articles 13.2(f), 14.2(g) and 15(h) of the GDPR require controllers to provide specific information about automated decision-making, based solely on automated decision making, including profiling that produces legal or similarly significant effects referred to in Article 22(1) and (4) of the GDPR. These requirements relate exclusively to the specific processing of profiling described in Article 22 of the GDPR. According to the GDPR's provisions above mentioned, there is no legal basis requiring the same level of information for 'general profiling'. General profiling is only submitted to the general provisions of the GDPR.

Nevertheless, Annex 1 of the Guidelines recommends the same level of information, whatever the type of profiling (general profiling and automated decision making). In this regards, the WP29 mentions also in the Guidelines (D – Rights of the data subject, point 1, page 13) that *'It is good practice to provide the above information (13(2)(f)/14(2)(g) whether or not the processing falls within the narrow Article 22(1) definition*'. The WP29 seems to go too far in establishing these good practice recommendations for the reasons above mentioned. We would suggest, therefore, to ask WP29 deleting any request for additional information applicable to the general profiling as referred to in Annex 1 and the concerned sentences in the draft Guidelines.

Comments on the Guidelines on Personal data breach notification

I. Personal data breach notification under the GDPR: Letter B point 2 'Types of personal data breaches' (pp. 6-7 of the draft Guidelines)

The EACB acknowledges the definition of 'personal data breach' in the GDPR as '*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'* (Art. 4(12)).

However and with regard to the three information security principles with which breached have been categorised (i.e. 'confidentiality breach', 'availability breach' and 'integrity breach'), we are not convinced that the 'availability breach' should be counted as a personal data breach. We understand that in the context of a hospital, the availability of critical medical data, even temporarily, could present a risk to individuals' rights and freedoms. However, this is not a case

in many other industries such as banking and insurance. All of the service breaks or loss of access are not critical and this type of data breach category should be limited only to the health care industry.

II. Article 33 – Notification to the supervisory authority: Letter A point 3 'Processor obligations' (p. 11 of the draft Guidelines)

We acknowledge that Art. 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a personal data breach, it must notify the controller 'without undue delay'.

However, we do not agree with the WP29's interpretation that *'in principle, the controller should be considered as "aware" once the processor has become aware'*. As stated in the draft Guidelines, the GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so 'without undue delay'. Therefore, though we understand the the importance for an immediate notification by the processor to the controller, with further information about the breach provided in phases as information becomes available, we cannot support the above-mentioned sentence because we believe that the controller is 'aware' of a breach after the processor has made an official notification to/informed the controller and not simultaneously when just the processor has become aware of a breach.

For this reason, we suggest deleting the concerned sentence in the draft Guidelines.

V. Accountability and record keeping: Letter A 'Documenting breaches' (p. 23 of the draft Guidelines)

With regard to this topic, EACB members would like to understand whether there is a retention time of the documentation relating to data breaches.

VI. Notification obligations under other legal instruments (p. 24 of the draft Guidelines)

EACB members appreciate the fact that the WP29 recalls the existence of additional notification and communication breaches under other legislation controllers should comply with.

However and as reported in the report following the second FabLab (5 and 6 April 2017), not only the banking industry but also other sectors such as telecoms called on the WP29 to take into consideration the different deadlines for notifications set by other EU legislation and the usefulness of having a single organisation to notify in relation to the same incident.

EACB members strongly stress the need for articulation between the three reporting obligation burdens (i.e. data breach under GDPR (Art. 33), incident reporting under PSD2 (Art. 96 + EBA draft Guidelines on major incidents reporting under PSD2) and NIS Directive (Articles 14(3) and 16(3)), which also applies to banks). The problem of banking institutions is the concurrence of three notification obligations, with different deadlines, in the event of incidents with different authorities.

We don't see the sectors' request being reflected in the current draft Guidelines.

Incident reporting under both the PSD2 and the NIS Directive could also concern data breach under the GDPR. For this reason, although the Article 29 Working Party might not be the right forum to solve this issue, we would nevertheless appreciate a recognition on the part of national competent authorities of the procedural burden that might result from the co-existence of different and sometimes parallel processes for notifying breaches.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Payments, Financial Markets (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Adviser, Consumer and Retail Banking (chiara.delloro@eacb.coop)