Brussels, 23 May 2017

EACB's views on the Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679

The European Association of Co-operative Banks (EACB) is the voice of the co-operative banks in Europe. It represents, promotes and defends the common interests of its 28 member institutions and of co-operative banks in general. Co-operative banks form decentralised networks which are subject to banking as well as co-operative legislation. Democracy, transparency and proximity are the three key characteristics of the co-operative banks' business model. With 4,050 locally operating banks and 58,000 outlets co-operative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 210 million customers, mainly consumers, retailers and communities. The co-operative banks in Europe represent 79 million members and 749,000 employees and have a total average market share of about 20%.

For further details, please visit www.eacb.coop

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 'Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679' adopted in April 2016.

Comments on the Guidelines on Data Protection Impact Assessment (DPIA)

General Comments

EACB members believe that the requirements set out by the WP29 can lead to a considerable but unnecessary increase in workload for co-operative banks. Requirements effectively leading to DPIAs for a large number of data processing activities, where this is not necessary, would have a significant negative impact on the operations of credit institutions compared to the status quo, where only a 'pre-control' is needed.

Moreover, we would like to bring to the attention of the WP29 that the Anti-Money Laundering Directive requires a systematic monitoring of customers in order to fulfil its objectives. We believe processing activities falling under such legal requirement clearly fall under the exceptions identified in the draft Guidelines, whereby a DPIA is not required where a processing operation has a legal basis in EU or Member State law (page 11). Processing data in order to apply AML rules should be out of the scope of DPIAs and the EACB would appreciate an explicit mention of this in the final Guidelines.

Similarly processing carried out conforming to guidelines issued by the European Supervisory Authorities (ESAs) as part of the implementation of banking regulation, e.g. guidelines on arrears and foreclosure and on creditworthiness assessment under the Mortgage Credit Directive (MCD), should also fall under such exception.

Specific concerns

Chapter III. DPIA: the Regulation explained

A. What does a DPIA address? (Page 6 of the WP29 guidelines)

EACB members believe the Guidelines should clarify that controllers have the flexibility to include different types of processing activities under a single DPIA, where possible.

B. Which processing operations are subject to a DPIA? (Page 7 of the WP29 guidelines)

It is true that a DPIA is to be carried out according to the specifications of the GDPR if a processing is 'likely to result in a high risk to the rights and freedoms of natural persons'. It is also true that Article 35(3) provides some examples and so it should not be interpreted as an exhaustive list.

However, EACB members believe the criteria listed on pages 7, 8, 9, which have the purpose to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, are too broad. When read in conjunction with the 'rule of thumb' that 'processing operations which meet at least two of these criteria will require a DPIA', such list would effectively

make DPIAs mandatory for virtually all processing operations – thus taking resources away from genuinely risky processing activities, contrary to a risk-based approach.

Moreover, the guidelines only give two examples of situations where a DPIA is not needed. EACB members would appreciate a more concrete and exhaustive list of examples of situations where a DPIA is not necessary.

Looking at the specific criteria, EACB members would like to note the following:

- Point 2. Automated decision making with legal or similar significant effect: the current text is too generic and we would welcome further explanation in the upcoming Guidelines on profiling.

- Point 3. Systematic monitoring: EACB members deploy video surveillance systems in their branches for basic purposes such as ensuring security of their premises and operations. We believe it would be disproportionate to require a DPIA for such basic processing activities and would welcome a more granular approach in the Guidelines, possibly specifying examples of systematic monitoring activities that do not require a DPIA.

- Point 4. Sensitive data: EACB members disagree with the draft Guidelines' statement that 'sensitive data' also includes 'electronic communication data, location data, financial data (that might be used for payment fraud)'. Both Articles 9 and 10 as Recital 51 are clear on the specific types of data that fall under special categories – the Guidelines should in no circumstances add to this exhaustive list.

- Point 5. Data processed on a large scale: Data processing in credit institutions always happens on a large scale, and by a literal interpretation should therefore always lead to a DPIA. Although this criterion needs to be assessed in light of other criteria, we believe it illustrate the need for further granularity in the Guidelines, possibly specifying examples of large-scale processing activities that do not require a DPIA.

- Point 7. Data concerning vulnerable data subjects (Recital 75): EACB members would like to point out that Member State legislation[1] already takes into account the position of employees in the employer/employee cooperation procedure. This should be enough to apply these requirements.

We do appreciate and support the clarification as to when DPIAs are necessary for already existing processing operations (page 11 of the guidelines), in particular when the Guidelines specify that DPIAs are needed for processing operations created after May 2018 or which change significantly. However, disagree with the draft Guidelines' statement (page 12) that DPIAs 'as a matter of good practice' should be re-assessed every three years at the latest. We believe this requirement would be superfluous when no conditions have changed and that it has no basis in the GDPR (Article 35(11) only provides that a review should only be performed '[w]here necessary' and 'where there is a change of the risk represented by processing operations'). We believe the decision as to how often a DPIA should be re-assessed should be left to the controller based on the specifics of the processing operations at hand, rather than setting one-size-fits-all limits as in the draft Guidelines.

[1] For example in Finland the position of employees is alread is taken into account in the Act on Co-operation within Undertakings".

C How to carry out a DPIA? (Page 13 of the WP29 guidelines)

b) Who is obliged to carry out a DPIA?

EACB members believe that the requirement to 'seek the views of data subjects or their representatives' (Article 35(9)) 'where appropriate' (page 13) is particularly difficult to carry out in practice.

Given the considerable time and resources involved in a DPIA, we would welcome further clarity in the Guidelines specifying that this obligation is likely to be appropriate in circumstances where potential risks for data subjects are very high, possibly including examples of when the requirement applies as well as of when it does not.

d) Should the DPIA be published?

As stated in the guidelines, 'publishing a DPIA is not a legal requirement of the GDPR. It is left upon the controller's decision'. We strongly support this position. We do believe that any recommendations or publishing requirements should be avoided.

D When shall the supervisory authority be consulted? (Page 18 of the WP29 guidelines)

EACB members would appreciate further clarity as to the situations where residual risk might still be identified following a DPIA, thus requiring consultation with the supervisory authority. We regard the current text as too generic, leaving it to each controller to identify the relevant threshold.

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)

We hereby consent to the publication of personal data contained in this document.