Brussels, 9 September 2019
Final

EACB comments on Guidelines 3/2019 on processing of personal data through video devices adopted on 10 July 2019

The **European Association of Co-operative Banks** (EACB) represents, promotes and defends the common interests of its 27 member institutions and of cooperative banks, with regard to banking as well as to co-operative legislation. Founded in 1970, today the EACB is a leading professional lobbying association in the European banking industry. Co-operative banks play a major role in the financial and economic system. They contribute widely to stability thanks to their anti-cyclical behaviour, they are driver of local and social growth with 2.914 locally operating banks and 53,000 outlets, they serve 209 million customers, mainly consumers, SMEs and communities. Europe's co-operative banks represent 81 million members and 719,000 employees and have an average market share in Europe 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

Comment on the Guidelines on Codes of Conduct and Monitoring Bodies

The European Association of Co-operative Banks (EACB) welcomes the opportunity to provide the European Data Protection Board (EDPB) with its comments on the draft Guidelines on processing of personal data through video devices adopted on 10 July this year.

General observations

As a preliminary observation, many Member States' legislation has specific legal requirements for video and photo data processing. As a consequence, it must be kept in mind that the requirements of both the EDPB Guidelines and such national legislation must be complied with.

Overall, we are concerned that the draft Guidelines' requirements are in conflict with the concept of proportionality as defined in the EU law, as they often exceed the scope of the articles set out in the GDPR and the measures proposed are not suitable to achieve a legitimate aim. The Guidelines practically ignore all safety-at-work and security aspects of video surveillance.

Furthermore, the draft Guidelines also expect the production and keeping of extensive documentation, including:

- Detailed documentation on the video cameras in use, the monitoring purpose, the legal basis / legitimate interest etc. (paragraphs 15 et sequ.);
- Transparency and information obligations with very extensive first-layer information 'warning signs' (paragraphs 112-113); these go well beyond the current requirements under the national legislation of some Member States;
- General video surveillance policies and procedures (paragraph 128);
- Because of the generally intrusive nature of video surveillance, often a DPIA (apart from the limited exceptions in the respective 'white list').

We would like to note that such extensive documentation and information (e.g. the first-layer information) would not be strictly necessary/required under the GDPR.

Specific observations

We would like to put forward the following specific observations:

- Paragraph 5 (as well as paragraphs 24, 25 and 32): We believe that stating that 'Video surveillance is not by default a necessity when there are other means to achieve the underlying purpose. Otherwise we risk a change in cultural norms leading to the acceptance of lack of privacy as the general outset' sets the bar of using video surveillance very high. It is always possible find other ways to achieve the underlying purpose.

- Paragraph 15: In some Member States the common practice is completely different and safety is a justified reason to use video surveillance.

- Paragraph 20: The paragraph states that 'the legitimate interest needs to be of real existence and has to be a present issue (i.e. it must not be fictional or speculative). A real-life situation of distress needs to be at hand – such as damages of serious incidents in the past – before starting the surveillance'. This is an exceptional requirement and is not in line with the general accountability requirement.

- Paragraph 22 under section 3.1.1. 'Existence of legitimate interests' of the draft Guidelines (page 8). We would appreciate it if the final Guidelines could specify that the same logic used for the examples concerning jewellers and petrol stations also applies to banks. Banks have a legitimate interest to use bank security cameras/video surveillance due to banks' peculiar functions and activities. Indeed, banks are among the top potential high-stake targets by robbers and fraudsters and the use of installed video surveillance systems will deter robberies and fraud, while also providing important evidence to law enforcement (which can be used to track down or identify suspects). Moreover, we believe that the above interpretation – banks having a legitimate interest to install cameras – is also consistent with paragraph 36 page 11 under the section on 'Data subjects' reasonable expectations', which says: 'the customer of a bank might expect that he/she is monitored inside the bank or by the ATM'. The customer's expectation mentioned is, among other things, certainly due to the fact that banks are sensitive locations as they deal with customers' wealth.

- Paragraph 26 states that 'Before operating a camera system, the controller is obliged to assess where and when video surveillance measures are strictly necessary. Usually a surveillance system operating at night-time as well as outside the regular working hours will meet the needs of the controller to prevent any dangers to his property.' The 'strictly necessary' requirement is not based on the law and is not in line with common practice related to video surveillance.

- Disclosure of video footage to law enforcement agencies, section 4.2 page 13: The explanations and examples for disclosure of video footage to law enforcement agencies mainly relate to a legal obligation. In practice that would mean a formal request by the police. It would be helpful to have further guidance as to under what circumstances disclosure to the police would be justified on the grounds of legitimate interest. The second example in paragraph 57 leaves the question open.

- Rights of the data subject, section 6, page 18: At paragraph 93, it is stated that a data subject's request of access could adversely affect other data subjects because of the necessary viewing, editing and disclosing of video footage. However, on the basis of the explanations and examples, it appears difficult to refuse a data subject's access request on that ground. The example at paragraph 95 would require the controller to go through two-hour video footage with several thousand visitors to extract the part with the data subject, edit it by blurring/pixeling/anonymising other persons and hand it over to the data subject. The question is under which conditions the controller could refuse the right of access based on Articles 15(4), 11(2) or 12 GDPR, e.g. because of the practical difficulties of identifying the data subject in the footage, the possible adverse effects of the screening and extracting for other data subjects or that the request could be considered excessive or unfounded.

- Right to erasure and right to object, section 6.2, page 20: The erasure of one individual in video footage with many different data subjects is difficult. It should be the controller's responsibility to assess the applicable retention time (and the legitimate interest).

- According to paragraph 102, it appears that an individual person must be erased/blurred upon his/her request, where the video footage is further kept. It would be helpful if the Guidelines discussed cases where the deletion request could be rejected on the basis that the erasure/blurring of the individual would not be justified following a balance of interest test (e.g. because the data subject does not give a reasons for his/her request, the necessary deletion/blurring would be difficult or complicated, etc.).

We believe that paragraph 111 should not be applied to banks. We agree that the data subject should be aware of the existence of a video surveillance system but we cannot share the idea that in banks, data subjects should have no doubt as to where a video camera is located so as for her/him to be able to estimate which area is captured by a camera so that he or she is able to avoid surveillance or adapt his or her behaviour. As said earlier under paragraph 22, banks are among the top potential high-stake targets by robbers and fraudsters and the use of installed video surveillance systems will deter robberies and fraud. Making robbers aware of the exact areas subject to video surveillance in banks would help them in their malicious action. Banks do not disclose specific areas due to security reasons.

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, Senior Adviser, Consumer and Retail Banking (chiara.delloro@eacb.coop)