POSITION PAPER

General Data Protection Regulation 2012/0011 (COD) – Priorities for the Trialogue

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID 8765978796-80

July 2015

ESBG

General Data Protection Regulation: ESBG's priorities for the Trialogue

1. Article 6 and others - Explicit vs. unambiguous consent of the data subject

Background: While Commission and Parliament prefer explicit 'consent' the Council requires only 'unambiguous consent'.

ESBG Position: In line with the EBIC position ESBG thinks that the requirement of 'explicit' consent in all cases is unrealistic and that the Council's proposal including **'ambiguous' consent** is **preferable**. The requirement of an only written consent should in any case be prevented. ESBG supports a transparent approach regarding the customer's consent. To ensure the practicability in the every-day business ESBG thinks that unambiguous consent is preferable to explicit consent.

2. Article 6 paragraph 4 – Use of data by controller for other purposes

Background: In the context of the consent of the data subject to the use of its data the Council has added a provision which allows a wider use of data by the same controller. The Council has added the following regulation: "*Further processing [of data] by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject.*" The Parliament and Commission proposals do not contain a similar regulation.

ESBG Position: ESBG supports the Council proposal which allows a **wider use of data** and thus makes **big data processing**, an area in which Europe should not lag behind the global development, easier.

3. Article 20 - Profiling and information to be provided to the data subject

Background: While the Commission did not explicitly mention profiling in its proposal, the Parliament has considerably tightened the rules by banning profiling with discriminatory effect and adding that profiling which leads to measures producing legal effects shall not be based solely or predominantly on automated processing and shall include human assessment. The Council wants to add limits to the use of "profiling", i.e. automated processing of personal data to assess personal aspects, such as performance at work, economic situation, health, personal preferences etc. The European Parliament's final Report foresees an opt-out concept – the data subject shall have a "right to object to profiling" (opt-out), instead of "a right not to be subject to profiling" (opt-in) following the Commission's/Council's proposal.

ESBG Position: The Parliament proposal is insofar problematic for the European savings and retail banks as it would **prohibit/hinder the use of scoring procedures**. Scoring is a common procedure in Member States to calculate the default risk in lending, prevent fraud and money-laundering or to support the development of tailor-made products, services for customers or to propose "suitable" investment products. Thus, it should be continuously possible to use this procedure throughout Europe. Neither the Council nor the Parliament proposal clearly state that profiling by financial institutions is allowed at a pre-contractual stage (for instance in case of a

customer's lack of credit capacity or in case of his/her lack of risk-awareness for financial instruments). It should be avoided that the regulation would either drive the financial institutions indirectly to force their customers to share their data if those want to have a credit or force savings banks to provide credits in cases without being able to assess related risks. Also, it would not be proportionate if on the one hand data controller are obliged to do a data protection impact assessment while on the other hand financial intuitions are prevented from assessing financial risks. This cannot be the intention of the European institutions. As a consequence, **ESBG** rather **supports** the **opt-out concept**. This provision provides consumer protection but does not provoke confrontations between customers and financial institutions.

Finally, any concept should consider that the "right to object"/"right not to be subject to profiling" cannot apply if profiling is requested by law (e.g. anti-money laundering requirements, combating fraud, and creditworthiness assessment). ESBG thinks that the lawfulness of the processing of personal data is strictly necessary for the purpose of preventing fraud and for the purposes of ensuring network and information security and should constitute a legitimate interest of the data controller which should be expressly mentioned in the regulation.

4. Art. 15 paragraph 2a (Parliament) and 18 paragraph 2 (Council) – Data portability

Background: The Commission proposal could be interpreted in a way that the data controller would have to transmit all personal data concerning a data subject, including data the controller has collected on its own, to a competitor (Art. 18). Contrarily, the Parliament clarifies this point by formulating under Art. 18 paragraph 2: "*The data subject shall have the right to transmit the personal data concerning him or her* ***which he or she has provided to a controlle****r to another controller*". Also the Council proposal contains a similar limitation under Art. 15 paragraph 2a ("*Where the data subject has* ***provided*** *the personal data* […]").

ESBG position: ESBG thinks that there should be no loophole in the regulation which would oblige competitors to provide each other with data which they have collected on their own. Thus, following the Council and Parliament proposal the transmission of data to competitors should be limited to data which has been provided by the data subject.

5. Article 22 – Intra group exemption

Background: The Parliament alone has added a regulation under Article 22 paragraph 3a for an intra group exemption: "*The controller shall have the right to transmit personal data inside the Union within the group of undertakings the controller is part of, where such processing is necessary for legitimate internal administrative purposes between connected business areas of the group of undertakings and an adequate level of data protection as well as the interests of the data subjects are safeguarded by internal data protection provisions or equivalent codes of conduct as referred to in Article 38.*"

ESBG Position: ESBG thinks that if such an exemption is added for groups of undertakings it should be **clarified** in the recitals that **savings and retail banks** with their specific local structure **are** also **allowed** to **exchange** data accordingly.

6. Article 31 and 33 - Data breach notification and impact assessment

Background: Contrary to the Commission and Parliament proposals the Council proposal limits the notification requirement to the supervisory authority to serious breaches. Otherwise, the Commission proposal imposes an overall obligation of an impact assessment on controllers to seek the views of data subjects, regardless of the sector, before any data processing took place. The proposals of Council and Parliament require such a data protection impact assessment only in case of a (high) impact for the data subject.

ESBG position: The **notification requirement** to the supervisory authority should be **limited to serious breaches** as in the Council proposal. Such a regulation better takes into account the principle of proportionality. In particular it should be considered in which cases the notification requirement is necessary to achieve the aim and whether this requirement is still reasonable, considering all interests of the groups concerned. Furthermore, the Commission proposal imposes an overall obligation of an impact assessment on controllers to seek the views of data subjects, regardless of the sector, before any data processing took place. The proposals of Council and Parliament which require such a data protection impact assessment only in case of a (high) impact for the data subject are more balanced and therefore preferable.

7. Article 35 and others - Obligation to have a data protection officer

Background: According to the European Parliament, the appointment of a data protection officer (DPO) is mandatory if "*the processing is carried out by a legal person and relates to more than 5000 data subjects in any consecutive 12-month period*" the Commission thinks that the size of the company should be decisive (enterprise employing 250 persons or more). The Council wants to leave the decision whether a DPO is mandatory up to the Member States. The Parliament has indicated that this would be unacceptable as it would lead to a race to the bottom. The Parliament has clarified that the DPO does not have to be a full-time position and can also be an external contractor.

ESBG Position: ESBG thinks that the **administrative burden** regarding the data protection officer should be as low as possible and **consider Member States' particularities**.

8. Article 79 (Council 79a) - Height of sanctions

Background: The Parliament argues that in case of severe illegal data processing it is important that companies face tough sanctions. The Commission has proposed fines which shall not exceed 1 Million EUR or in case of an enterprise up to two per cent of its annual worldwide turnover. The Council proposal is similar and includes maximum fines "*that shall not exceed 1 Million EUR or, in case of an undertaking, 2 % of its total worldwide annual turnover of the preceding financial year*". The Parliament wants to considerably increase the possible sanctions up to five per cent of the global annual turnover, or 100 Million Euros.

ESBG position: ESBG thinks that any **fines** shall stay **justifiable** in the whole legislative context.

About ESBG (European Savings and Retail Banking Group)

ESBG brings together savings and retail banks of the European Union and European Economic Area that believe in a common identity for European policies. ESBG members support the development of a single market for Europe that adheres to the principle of subsidiarity, whereby the European Union only acts when individual Member States cannot sufficiently do so. They believe that pluralism and diversity in the European banking sector safeguard the market against shocks that arise from time to time, whether caused by internal or external forces. Members seek to de-fend the European social and economic model that combines economic growth with high living standards and good working conditions. To these ends, ESBG members come together to agree on and promote common positions on relevant matters of a regulatory or supervisory nature.

ESBG members represent one of the largest European retail banking networks, comprising of approximately one-third of the retail banking market in Europe, with total assets of over €7,300 billion, non-bank deposits of €3,480 billion and non-bank loans of €3,950 billion (31 December 2012).

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ▪ B-1000 Brussels ▪ Tel: +32 2 211 11 11 ▪ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ▪ www.esbg.eu

Published by ESBG. July 2015