European Federation of Building Societies
Fédération Européenne d'Epargne et de Crédit pour le Logement
Europäische Bausparkassenvereinigung

Brussels, 17 August 2012

Position paper of the Bausparkassen on the European Commission's proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

The European Federation of Building Societies (EFBS) is an association of credit institutions and establishments which promote and support the financing of home ownership. It also pursues the aim, in a politically and economically converging Europe, of promoting the idea of the acquisition of home ownership. Bausparkassen finance housing in retail business through loans secured by residential property. The saving-for-home-ownership business is conducted using modern data processing and communications technology and is subject to strict national data protection legislation.

The EFBS has the following observations on the proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), published by the European Commission on 25 January 2012:

1. Framework in the form of a Regulation

The EFBS supports the efforts of the European Commission to modernise data protection law and to adapt to technological progress, as well as the aim to further standardise data protection law to counter the existing fragmentation and to reduce the administrative burden. However, in so far as these objectives are to be achieved through the adoption of a Regulation, we venture to point out the following aspects.

A Regulation by the European legislature is certainly a suitable instrument to regulate cross-border issues. However, since in terms of its regulatory content the Regulation also covers purely national issues, it will displace the data protection legislation which has been tried and tested in the Member States, especially in banking and banking supervision law, and which takes account of the local particularities.

Against this background, in the view of the EFBS, there is first a need to clarify the relationship between the Regulation and the existing data protection arrangements in other EU legal instruments, such as, for example, the Consumer Credit Directive. In addition, the possibility should be granted for the Regulation to be put into practice through national legislation or to maintain special legal provisions, such as, for example, banking supervision standards to combat money laundering, corruption and fraud and on scoring. If these regulations order or allow the processing of personal data, these special legal provisions must continue to exist alongside the Regulation.

In the opinion of the EFBS, it is necessary overall – if the Regulation approach is retained – to avoid regulatory duplication and contradictions which are already beginning to emerge.

2. Delegated acts

The EFBS views the power of the European Commission to adopt delegated acts to specify the provisions of the Regulation particularly critically. According to the Lisbon Treaty, the European Commission should be empowered to adopt delegated acts only to regulate technical details. However, the proposal for a Regulation provides in 26 places (see Article 86) for the power of the Commission to adopt supplementary provisions and in so doing far exceeds the limits for delegated acts laid down in Articles 289 ff. TFEU.

In the opinion of the EFBS, this extensive power of the Commission entails the risk of undermining the principle of separation of powers. It results from the combination of Articles 289 and 290 TFEU that a Regulation, as a basic legislative act, may not transfer the essential material provisions to the act deriving therefrom. However, in many cases, the legislative powers of the proposal for a Regulation are not confined to the transfer of such competence to specify, but often contain the power to lay down the regulatory content independently.

In this respect, it is necessary to confine the power of the European Commission to adopt delegated acts to the extent that is admissible and necessary. Otherwise, the data protection law could become a permanent construction site and the aim of legal certainty, also strived for through the Regulation, would not be achieved but rather thwarted.

3. Definitions, Article 4

Article 4 of the proposal for a Regulation, like Article 2 of Directive 95/46/EC already, contains a large number of definitions. In contrast to the definition of the concepts 'data subject' and 'personal data' contained in Article 2(a) of Directive 95/46/EC, the definitions in the proposal for a Regulation appear to be considerably wider. For instance, it is no longer only the identifiability of the person by the respective controller that is taken into account, but also identifiability by any person is deemed sufficient. This results in the elimination of the incentives existing so far for the use of pseudonyms and encryption techniques. To maintain the relevant incentives, in our opinion, the concepts of 'pseudonymisation' and also 'anonymisation' should first be defined in the Regulation. Furthermore, both measures should be acknowledged as conducive to data protection in the appropriate place in the Regulation.

In addition, in the opinion of the EFBS, the concept of 'blocking' should be included in the definition of Article 4(3) of the Regulation. As a subform of processing, this means the marking of stored data for the purpose of restricting its further processing or use. In recognising the principles of data avoidance and data economy, this possibility should be accorded in the Regulation.

Furthermore, the EFBS considers that the concept of 'recipient' in Article 4(7) has been defined too widely. According to the wording, it covers all persons or bodies to which the personal data are 'disclosed'. This formulation would also cover internal disclosure of personal data within a company, so this too would have to be authorised under data protection law. This cannot be implemented in practice. In the view of the EFBS, the fact of receiving data described in Directive 95/46/EC should continue to be taken into account.

4. Consent in the case of 'significant imbalance', Article 7(4)

The EFBS is against the provision contained in Article 7(4), according to which the data subject's consent cannot provide a sufficient legal basis for the data processing where there is a 'significant imbalance' between the position of the data subject and the controller. According to recital 34, such

an imbalance exists especially in a situation of dependence. As an example, recital 34 then cites the employment relationship between employee and employer.

In the view of the EFBS, Article 7(4) entails the risk in this respect that an imbalance will also be seen in general in the relationship between customer and bank and the consent given by the customer in this field will no longer be recognised as a sufficient legal basis for the data processing.

Here, however, the generally valid principle of legitimate expectations should apply, according to which the controller may rely on the lawfulness of the consent underlying the processing, in so far as it is voluntary. Against this background, Article 7(4) should be deleted.

5. Transfer of data to credit information exchanges

Furthermore, it should be clarified expressly in the Regulation that also the transfer of personal data to credit information exchanges is admissible, in so far as this is necessary to safeguard legitimate interests of the controller or a third party. In contrast to the provisions of Directive 95/46/EC, under the proposal for a Regulation, the interest of a third party to whom the data are disclosed is not longer sufficient to legitimise such a procedure. However, this is of particular importance precisely in the field of housing credit, especially as the draft EU Directive on this subject under discussion requires institutions to undertake a careful creditworthiness assessment (see Article 15 [Council] or 14 [ECON]) and in this connection expressly requires the use of credit information exchanges (see Article 17 [Council] or 16 [ECON] and in particular recital 42 [Council] or 27 [ECON]).

6. Excessive bureaucratisation

The provisions in Articles 11 to 15 of the proposal for a Regulation entail the risk of excessive bureaucratisation of the data processing process:

a. Obligation to provide information to the data subject, Article 14

A basic condition for the data subject to be able to exercise his rights is certainly sufficient information on the key data of the data processing. However, the EFBS opposes overloading the data subject with a large amount of information, as provided for in Article 14 of the proposal for a Regulation. It seems more expedient to organise the information to be provided to the data subject in two stages. In this way, he could first be provided with general information and only if necessary on actual request will more far-reaching information be made available. In this way, it would on the one hand be ensured that the data subject is not overwhelmed by a flood of no longer comprehensible information, which is often even interpreted as harassment. On the other hand, the burden of the controllers would be reduced significantly and they would be able to concentrate on cases in which there is in fact a more far-reaching need for information.

b. Right of access for the data subject, Article 15

The right of access for the data subject arising from Article 15 of the proposal for a Regulation should also be organised appropriately. In particular, rights of access should exist only in so far as there is no legitimate interest in confidentiality on the part of the controller. This should be clarified in the Regulation.

7. Right to data portability, Article 18

The right to data portability provided for in Article 18 should not apply for 'conventional data processing'. There may be good reason for a corresponding right with regard to the use of social networks by the data subject and the associated disclosure of private data. The data posted by the

data subject remain his private business and should be subject to his sole right of disposal, which can be ensured through a right to data portability.

It is a different matter, however, in the case of conventional data processing by economic operators. Here, data are collected only in so far as this is necessary to execute a concrete business relationship. Accordingly, this refers to business data to which the data subject himself regularly has no direct access. Corresponding 'electronic customer files' serve to meet contractual and legal obligations of the undertaking and cannot be seen as belonging to the 'intellectual property' of the data subject, but rather represent an asset of the undertaking. For this reason, no right should exist to the surrender of these data.

8. Data processor, Article 26

Under Article 26, it should be clarified that disclosure of personal data to a data processor is not 'data transfer' and consequently not 'processing' and therefore does not have to be additionally authorised pursuant to Article 6. This corresponds to the concept already used in Directive 95/46/EC which has proved itself in practice.

9. Use of personal data for advertising purposes

Whereas national data protection laws (e.g. in Germany) contain explicit regulations on the use of personal data for advertising purposes, no provision is made for this in the proposal for a Regulation. Accordingly, the lawfulness of the use for advertising purposes would have to be measured against the general provisions on the lawfulness of data processing in Article 6 and – without the corresponding consent of the customer – would be admissible at most pursuant to the general regulation in paragraph 1(f) (legitimate interests of the undertaking). In this connection, however, it is questionable whether the interest of the data subject to receive advertising only after prior consent to the use of their data for advertising purposes is not classified as higher-ranking than the interest of the undertaking to use these data for advertising purposes. If this were the case, use of the data for advertising purposes would also not be possible pursuant to Article 6(1)(f).

There is still a risk that the generally formulated provision in Article 20(1), through which measures based on profiling are prohibited, excludes customer selection for advertising measures.

According to the current version of the proposal for a Regulation, it is therefore unclear whether undertakings may use the data of their customers without their express consent to advertise their own offers (e.g. new products) to these customers. This would in particular disadvantage financial service providers which – like the Bausparkassen – market their products through independent intermediaries and cooperating credit institutions or insurance undertakings, as the sales partners referred to would be termed as 'third parties' under data protection law, with the consequence that the undertakings named could not transfer to them the data necessary to serve the customers.

The EFBS is therefore emphatically in favour of including an express regulation on advertising in the Regulation, in order to eliminate this legal uncertainty. This should provide that the processing, and especially the use and transfer of personal data, is admissible provided that this involves data aggregated in a list or in another way on members of a group of persons which can be determined by specific criteria (e.g. 'own customer') and the processing for advertising purposes is necessary for the controller's own offers.

10. Notification of a personal data breach to the supervisory authority and communication to the data subject, Articles 31 and 32

The EFBS advocates limiting notification of data leaks to the competent authority to cases in which there is a threat of serious impairment to the rights or legitimate interests of the data subject. While safeguarding the principle of proportionality, this could allow overburdening of the controller and the competent authority through notification of trifling cases to be avoided.

Furthermore, the deadline for notification of 24 hours is clearly too short and practically impossible to implement. Here only notification without delay should be required.

11. Data protection impact assessment, Article 33

The data protection impact assessment provided for in Article 33 of the proposal for a Regulation without any exceptions represents a disproportionate effort and leads to considerable legal uncertainty, since on account of the general wording, it is not clear which areas are to be subject to an impact assessment at all. In addition, it is not feasible in practice in the context of the impact assessment to seek the views of data subjects or their representatives on the intended processing, as provided for in Article 33(4).

Article 33 should therefore be drafted more clearly and exceptions should be added. In particular, an impact assessment should not be necessary if the data processing is based on a legal obligation or the consent of the data subject has been given or is required to fulfil or carry out an agreement or to carry out pre-contractual measures in the interests of the data subject.

Article 33(4) on the other hand should be deleted entirely. Alternatively, provision could be made at this point for the inclusion of data protection officers, in so far as one has been appointed.

12. Appointment of a data protection officer, Article 35

The EFBS is in favour of maintaining the significance of the company data protection officer. This instrument has proved to be extremely valuable especially in the credit sector. The company data protection officer plays an important role in self-monitoring and works towards data processing within the undertaking in accordance with the law. For this reason, it should also be considered providing more incentives for the appointment of a data protection officer. In this connection, thought should also be given to whether the obligation provided for in Article 35(1)(b) to appoint a data protection officer only from the employment of 250 persons or more is appropriate. Here the focus should be more on the special circumstances of the undertaking. For instance, in particular undertakings which collect, process and use data on behalf of others and undertakings which have particularly sensitive data at their disposal, should already have to appoint a data protection officer from a lower number of employees.

Finally, it should be made possible for Member States to adopt national regulations on the requirements on the appointment and dismissal of the data protection officer which extend beyond the Regulation. In this way, the existing level of data protection is ensured without negative effects resulting from this for the internal market.

13. Legal remedies and penalties, Articles 78 and 79

The differentiation made in Article 78 and Article 79 between ‘penalties’ and ‘administrative sanctions’ is not revealed. In this way, under no circumstances may dual penalties be imposed for a breach. In addition, it should be pointed out that provisions on administrative fines come under criminal law and therefore do not fall within the regulatory competence of the European Union. This

competence would be bypassed if the 'administrative fine' contemplated in Article 79(4) to (6) were to be introduced.

In addition, the fines provided for in Article 79 of the proposal for a Regulation of up to a maximum of EUR 1 000 000 for natural persons or in the case of an enterprise of up to 2% of its annual worldwide turnover are completely disproportionate and entail the risk that natural persons or enterprises are exposed to sanctions which jeopardise their continued existence.

14. Transitional provisions

Finally, in the view of the EFBS, it is absolutely essential to include transitional provisions for old cases. Therefore, declarations of consent for data processing given under the current law should remain valid at least for a transitional period in order not to thwart the right of the individual to determine the disclosure and use of his personal data and to facilitate the conversion to the new rules for the controller.