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

To the members of the
European Federation of Building Societies

Brussels, 17 February 2012

Reform of the legal framework of data protection in the EU

Dear members,

We enclose, for your information, the European Commission's proposal for a Regulation on the reform of data protection in the EU, which was adopted on 25 January 2012 together with a proposal for a Directive.

The proposal for a Directive deals with the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and is intended to safeguard the free movement of such data. The proposal for a Regulation deals with the protection of individuals with regard to the processing of personal data and is intended to safeguard the free movement of such data. The proposal for a Regulation therefore aims to clarify the relationship between the controller and the data subject. In common with all other companies which undertake processing of data, the building societies are affected by the proposal for a Regulation. The Regulation would be directly applicable in all Member States, substituting European law for national law, and would be immediately enforceable as law. We wish to draw your attention to the following provisions of the proposed Regulation in particular.

Lawfulness of processing (Article 6)
Pursuant to Article 6 of the proposal for a Regulation, processing of personal data will be lawful only if and to the extent that the data subject has given consent to the processing of their personal data for one or more specific purposes, processing is necessary for the performance of a contract to which the data subject is party or in order to take steps prior to entering into a contract, or other grounds specified in Article 6 apply. Data processing for a purpose which is not compatible with the initial one for which the data are collected will only be lawful if it is compatible with another purpose specified in Article 6(a) to (e). If the data subject contends that he or she has not consented to the processing of their personal data, the controller, pursuant to Article 7(1) of the proposal for a Regulation, will bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.

The controller's information obligations towards the data subject (Article 14)
Prior to initial processing of the data or during further operations, the controller must provide the data subject with specific information in an intelligible manner, including the

purposes of the processing, the recipients to whom the personal data are to be or have been disclosed, and the right to rectification or erasure of the personal data.

Right to be forgotten and to erasure (Article 17)

Pursuant to this provision, the data subject will have the right to obtain the erasure of personal data relating to them and the abstention from further dissemination of their data if the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, the data subject withdraws consent, or processing of the data does not comply with this Regulation. If the personal data have been made public, the controller must take all reasonable steps to inform third parties who are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data (Article 17(2)).

Right to data portability (Article 18)

Article 18 grants the data subject the right, where personal data are processed by electronic means, to obtain from the controller a copy of data undergoing processing; this must be provided in a format which is commonly used and allows for transmission into another system.

"Profiling" (Article 20)

Article 20 concerns the data subject's right not to be subject, in general, to a measure based on profiling. "Profiling" by means of automated processing to compare personal data with the desired customer criteria (for example, to assess creditworthiness) should only be allowed when data processing is carried out in the course of entering or performance of a contract, initiated at the request of the data subject, or when the data subject has given his or her consent, when such a measure is expressly authorised by Member State or national law. In any case, such processing should be subject to suitable safeguards relating to the data subject's legitimate interests.

Responsibilities of the controller (Articles 22, 28, 31 - 33, 35)

Each controller has a responsibility, inter alia, to maintain documentation of all processing operations in accordance with the provisions of Article 28.

Pursuant to Article 31, in the case of a personal data breach, the controller is required to notify and document the personal data breach to the supervisory authority immediately, not later than 24 hours after having become aware of it. Pursuant to Article 32(1), the data subject must be notified of the data breach without undue delay "when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject".

Where processing operations present specific risks to the rights and freedoms of data subjects, the controller is required to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (see Article 33).

In certain cases specified in Article 34, authorisation must be obtained from the supervisory authority, or the supervisory authority must be consulted, prior to the processing of personal data.

Pursuant to Article 35(1) (b), a data protection officer must be designated in any case where the processing is carried out by an enterprise employing 250 persons or more; the data protection officer must be designated for a period of at least two years.

Competence (Article 51)

Generally, each supervisory authority exercises, on the territory of its own Member State, the powers conferred on it in accordance with the Regulation. Where the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor is competent for the supervision of the processing activities of the controller or the processor in all Member States.

Penalties (Articles 78 and 79)

The sanctions are fixed with due regard to the gravity of the breach of the provisions of the proposed Regulation. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities. Otherwise, in the event of a breach, the supervisory authority may impose a fine up to 250 000 EUR, or in case of an enterprise up to 0.5 % of its annual worldwide turnover. For a serious violation, the supervisory authority may impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover. The maximum penalty is a fine up to 1 000 000 EUR. For an enterprise, the penalty may not exceed 2 % of its annual worldwide turnover.

We enclose a copy of the Commission's proposal for a Regulation for your information.

You are invited to send your views and comments about the Commission's proposal for a Regulation to the EFBS office by Friday, 16 March 2012.

If you have further questions, please contact us at any time.

Yours sincerely,

Andreas J. Zehnder
Managing Director
European Federation of Building Societies

Annex

- 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)