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

Mailing list Consumer protection/Data protection

Brussels, 27 March 2014

European Parliament vote in plenary session on amendments to the European Commission proposal for a General Data Protection Regulation

Dear Madam or Sir,

On 12 March 2014, the European Parliament in plenary session passed a Legislative Resolution on the amendments to the European Commission proposal on a General Data Protection Regulation from the report of the Committee on Civil Liberties, Justice and Home Affairs.

1. Definitions

It is to be welcomed that the instruments of anonymisation and pseudonymisation are now considered in the proposal. According to Article 4(2a), "pseudonymous data" are personal data that cannot be attributed to a specific data subject without the use of additional information.

In addition, it is clarified that the Regulation is not applicable to the processing of anonymised data. According to recital 23, data are anonymised if they cannot be connected to an identified or identifiable natural person.

In Article 4(7), a recipient is defined as the person to whom the data are disclosed. However, Article 4(7a) specifies that the term "third party" refers to any person or body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data. Accordingly, disclosure of data to third parties who are operating under the authority of the controller/processor acting on the controller's behalf should be possible even without the consent given by the data subject, which is required in principle pursuant to Article 6(1a), 4 (3).

2. Lawfulness of data processing, Article 6

According to Article 6(1)(a), data processing is lawful if the data subject of the personal data to be processed has given his consent to the processing for one or more specific purposes (Article 5 (b)).

If this consent is not given, processing of the data may also be lawful if it is necessary for the performance of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract (Article 6(1)(b)).

Data processing may also be lawful if is necessary for the purposes of the legitimate interests pursued by the controller, although subject to the requirement that these interests are not overridden by the interests or fundamental rights of the data subject (Article 6(1)(f)). The disclosure of data to a third party may also be justified provided that, on assessment, the interests/fundamental rights of the data subject do not override the legitimate interests of the third party and, in the case of disclosure, the "reasonable expectations" of the data subject regarding the existing contractual relationship with the controller are met (recital 38). This should ensure that the notification on defaults in the credit relationship to credit information exchanges continues to be admissible without renewed consent. However, what is meant by "reasonable expectations" remains

an open question. In the case of processing of pseudonymised data, it is to be presumed that the reasonable expectations are met (recital 38).

The controller must inform the data subject on his legitimate interests and on the right to object to the data processing without the need for justification, in accordance with Article 19(2). The controller must document the legitimate interests (recital 38).

3. Consent to data processing, Article 7

The MEPs maintain the European Commission's proposal in Article 7(3) to grant the data subject a right to withdraw his consent to the data processing at any time. According to Article 7(4), the consent loses its validity if the purpose for which it was granted ceases to exist or the processing is no longer necessary for carrying out the purpose for which the data were originally collected. As called for by the EFBS, the first sentence of Article 7(4), according to which consent given for data processing is invalid where there is a significant imbalance between controller and data subject, has been deleted. This also applies to recital 34, which cited the example of the employment relationship and therefore entailed the risk of this understanding being transferred to the relationship between a bank and its customer.

4. Obligation to inform the data subject and right to information, Articles 13, 13a, 14 and 15

Compared to the Commission proposal, the controller's obligations to provide information are even more far-reaching in the Parliament text. Article 13, which previously contained an obligation to communicate any rectification or erasure to recipients of data, has been extended to provide that the data subject is informed, at his request, about the recipients to whom data were disclosed.

The newly included Article 13a requires a controller to carry out standardised information policies. Before the provision of information pursuant to Article 14, the controller will have to provide the data subject with a large number of particulars and information in standardised form on the data processing procedure (data possibly collected and retained beyond that needed for the purpose of the processing, dissemination of data to commercial third parties, delivery of data against payment, data retained in encrypted form). The information is to be presented using symbols (Icons), which are listed in Annex I to the Regulation.

Article 14 now provides that in addition to the identity of the controller and the purpose of the processing, further information is to be made available to the data subject including regarding the security of the processing, the period for which the data will be stored, the identity of the recipients and the time of the first dissemination where information is disclosed, information on profiling measures and the logic involved in automated processing, and the provision of information to public authorities in the past twelve months.

Article 14(5) and recital 50 limit the obligation to provide information if the data subject has already been informed or the recording or disclosure of the data is laid down by law or would involve a disproportionate effort on the part of the controller.

The data subject's right to information is similarly configured in Article 15 to the obligation to provide information. No provision is made for a limitation resulting from the interest in confidentiality of the processing body.

5. Right to data portability, Article 18

The right to data portability has been deleted from Article 18. It is now to be found in Article 15(2) and clear limits have been placed on it. It is therefore to be welcomed that the data subject can now procure an electronic copy covering only the data which he had himself originally made available to the controller. Accordingly, a credit institution is not required to provide data it has validly collected concerning the customer (such as, for example, concerning the regular payment of instalments to reimburse a loan).

6. Use of personal data for advertising purposes

Recital 39b contains the presumption that direct marketing for own or external products is carried out in the legitimate interest of the controller or a third party if the expectations of the data subject concerning the business relationship with the controller are met. Furthermore, the right of the data subject to object and the source of the information must be clearly identifiable for the data subject.

However, this does not apply if the interests of the data subject override the legitimate interests of the controller. In the case of processing of data for advertising purposes, there is therefore no secure legal basis which would also allow processing without the consent of the data subject.

What is more, Article 20 still provides that the data subject can object to profiling. Profiling is defined in very general terms in Article 4(3a): Profiling means any form of automated processing of customer data intended to evaluate certain personal aspects relating to a person. The profiling important for canvassing of customers is to be lawful if no objection is made, even though it produces legal effects for the customer, if it occurs inter alia for the conclusion or performance of a contract. In the case of profiling of pseudonymised data, it is to be presumed that the profiling produces no legal effects on the rights of the data subject and the process is therefore lawful (recital 58a).

7. Data processing, Article 26

Article 4(7a) clarifies that the processor is not a third party (cf. under point 1). Accordingly, disclosure of data to the processor should be possible even without the consent of the data subject.

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

As also called for by the EFBS, the deadline for notification of a breach to the supervisory authority of within 24 hours of becoming aware of it has been deleted (Article 31). Notification of the competent supervisory authority is now to occur without undue delay. In recital 67, this period is limited to a maximum of 72 hours. All breaches are to be notified, irrespective of their gravity.

Communication must be made to the data subject when the personal data breach is likely to adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject. The communication is to be made without undue delay following the notification pursuant to Article 31. Communication to the data subject may be waived if the controller demonstrates that it has implemented appropriate technological measures which prevent access to the data by unauthorised persons (Article 32(3)).

9. Risk analysis and data protection impact assessment, Articles 32a, 33 and 33a

The obligation to carry out a data protection impact assessment still exists, but only if it is necessary to carry it out pursuant to Article 32a(3). Article 32a requires the controller to carry out a risk analysis of the data processing on the rights of the data subject. Paragraph 2 lists a series of risky

operations, which includes profiling (Article 32a(2)(c)). Where profiling is involved, an impact assessment must be carried out pursuant to Article 32a(3)(c). It is to be welcomed that, in accordance with the request of the EFBS, the views of the data subject on the intended processing of his data no longer have to be sought, Article 33(4).

In this connection, reference should also be made to Article 33a, which requires the controller, no later than two years after the impact assessment, to carry out a data protection compliance review and to repeat this at regular intervals, but at least every two years. The documentation of the results of this review is to be made available on request to the competent supervisory authority.

10. Designation of a data protection officer, Article 35

It is to be welcomed that the threshold of 250 employees for the designation of a data protection officer, proposed by the European Commission, has been deleted. However, the European Parliament has advocated that a data protection officer must be designated if a legal person processes data of more than 5,000 data subjects over a 12-month period.

11. Penalties, Articles 78, 79

The MEPs consider a warning in writing to be sufficient in cases of first and non-intentional non-compliance with the data protection regulations. If the controller is in possession of a European data protection seal, a fine may be imposed only in cases of intentional or negligent non-compliance. The MEPs advocate even higher sanctions than the Commission: a fine of up to EUR 100,000,000 or 5% of the annual worldwide turnover of an enterprise. However, when imposing the sanctions, various factors detailed in Article 79(2)(c), for instance concerning the nature, gravity and duration of the non-compliance, will be taken into consideration. The Commission proposal had provided for graduated amounts of up to a maximum of EUR 1,000,000, or 2% of annual worldwide turnover.

12. Future procedure

The European Parliament ended the first reading with the vote. This reflected the desire to ensure that the negotiated results are upheld in the coming legislative period of the European Parliament. At the Council, on the other hand, the negotiations are continuing. There are still a number of Member States which reject the proposal in the form of a Regulation. It is still unclear when a common position will be reached by the Member States. For this reason, it is currently also not foreseeable when the trialogue negotiations between the two EU institutions can be started.

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

Yours sincerely,

Andreas J. Zehnder
Managing Director
European Federation of Building Societies

Annex: European Parliament Legislative Resolution on the proposal for a General Data Protection Regulation