Informal comments of the EDPS on the exchange of personal data to combat fraud and error in the field of cross-border social security coordination under Regulations (EC) Nos 883/2004 and 987/2009

I. Introduction

In your letter of 15 November 2013 you asked our views 'on a proposal under consideration to amend Regulations (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems ('the basic Regulation') and its implementing Regulation, Regulation (EC) No 987/2009 ('the implementing Regulation') to establish a clear legal ground providing for processing personal data to combat fraud and error in the context of cross-border co-ordination of social security between Member States.

As you explained in your letter, 'it is generally accepted ... that the Regulations provide sufficiently clear legal grounds for the exchange of data between Member States in individual cases of suspected fraud or error to take place'.

At the same time, your concern is that 'there is a divergence of views ... on the extent to which the obligations to exchange data under the basic and implementing Regulations include data-matching to address fraud and error in the proper implementation of those Regulations'. As you noted further in your letter, 'this difference of views and in legal approach to sharing data creates practical problems for Member States in obtaining the necessary data to establish the validity of social security claims'.

II. General comments

We welcome the Commission's intention to modify the current legal framework relating to the coordination of social security systems in order to provide more clarity with regard to the exchange of bulk data in the form of 'data-matching'. We also welcome that we were consulted at an early stage in the procedure, ahead of the inter-service consultation.

We recommend that when drafting the proposal of the change in the legal framework, you carefully assess:

- what data should be exchanged under 'data-matching', by what entities, under what circumstances, in what way, and for what specific purposes;
- whether any such data exchange is necessary and proportionate;
- what specific safeguards, technical and organisational measures, are required to ensure the protection of the individuals with regard to their personal data.

We further recommend that you carefully assess whether data-matching should be optional or mandatory and what this means in practice.

Based on the results of this assessment, we recommend that the items mentioned above be specifically considered and discussed in the proposal to be drafted. A carefully considered

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax: 02-283 19 50

change in the legislative framework may contribute towards clarity, legal certainty, and may also provide appropriate safeguards to better protect the individuals concerned.

Below are a number of preliminary considerations and recommendations that we suggest considering when carrying out the assessment and preparing the first draft of the proposal for a revised regulatory framework. In addition, in Section VI, we also address your questions regarding the legal ground of the processing, which you raise in your letter.

III. The legal framework should clarify what is data-matching

In order to ensure legal certainty and predictability, and also to help decide what specific safeguards are needed to protect the individuals, the amended legal framework should clearly define what data matching is.

IV. The legal framework should clarify what data are matched, by what entities, under what circumstances, in what way, and for what specific purposes

Further, it is important that the legislation does not simply provide a blanket authorisation to carry-out any data-matching using any personal data available, but that it also describes, as clearly and specifically as possible, what data are matched, by what entities, under what circumstances, in what way, and for what specific purposes.

To provide the necessary specificity, the information under the following two headings, already included in your letter may provide a useful starting point.

If it is foreseen that additional data-matching not specifically explained in your letter will also take place, this should also be clarified in the proposed changes to the legislative framework. For each type of data-matching for each specific purpose, we recommend you assess the necessity and proportionality of the data exchange.

While we acknowledge that it may not be possible to specifically foresee all types of possible future data-matching in advance, and therefore, it may be necessary for the legal framework to allow some degree of flexibility, the more clearly you will be able to define the types of data-matching in the proposed legal framework, the more transparency and protection this may afford to data subjects, and the more likely it is that you will be able to rely on the proposed legislation to support the legitimacy of the data-matching.

Matching the list of persons entitled to pension contributions against data regarding deaths

On page 3 of your letter, you explain that 'some Member States operate a monthly system of electronic exchange of personal information whereby, for example, Member State A in which a number of pensioners from Member State B are living provides death data to Member State B. In this way, Member State B can check the death data against its list of pensioners living in Member State B to identify any anomalies between the two sets of data, i.e. are pensions being paid in respect of persons who have died'.

Although we would welcome if you provided further detail and specific evidence of the necessity and proportionality of the data-matching described above with regard to pension contributions, in principle, we do not expect that we would question the necessity or proportionality of data-matching in this context, provided it only takes place to the limited degree described in your letter. This is, however, with the important caveats that the details of the information exchange should also not raise proportionality concerns. For example, no

more data should be processed than necessary during the matching procedure, and appropriate retention periods should be applied.

Data matching regarding unemployment benefits

Further in your letter, you provide another example of data-matching: 'one administration sends a list of people it pays unemployment benefit to who are resident in another State to check if any of those people are registered as employed i.e. whether they are wrongly claiming unemployment benefit in the first State, in which case further investigation would be required'.

Here also, while in principle we do not question the necessity and proportionality of data-matching in this context, care should be taken that all details of the processing be designed in such a way that also complies with the principles of necessity and proportionality.

IV. Necessity and proportionality of the data-matching

In addition to carrying out a proportionality analysis, and taking into account the results of such an assessment when drafting the proposed legislation, we also recommend that the proposed legislation also refer to the requirement that any data exchange must be necessary and proportionate for its purposes (which, in turn, must be clearly specified in the proposal).

V. Is data-matching mandatory or optional?

To ensure legal certainty, we also recommend that the proposal unambiguously specify, in each case, whether the data-matching is optional or mandatory, and what this means more specifically. For example, it should be clear whether optional data-matching means that each Member State is free to adopt national legislation allowing or not data-matching or whether it is up to each competent authority whether it wishes to exchange data with a competent authority in another Member State. It should be equally clear whether mandatory data-matching simply means that a competent authority must provide the data upon request; or whether Member States must also set up a mechanism to enable their competent authorities to exchange the data and whether competent authorities then be obliged to use such mechanism for any exchanges.

What the exact rules are in this regard may also have - as a side effect - an effect on what legal ground may be available for competent authorities among the six options foreseen in Article 7 of Directive 95/46/EC. This brings us to our next point, the legal grounds applicable to the processing, with regard to which you also sought our advice.

VI. Overview of legal grounds

Article 7 requires that personal data shall only be processed if at least one of six legal grounds listed in that Article apply. In particular, personal data shall only be processed (a) based on the data subject's unambiguous consent; or if - briefly put - processing is necessary for:

(b) performance of a contract with the data subject;
(c) compliance with a legal obligation imposed on the controller;
(d) protection of the vital interests of the data subject;
(e) performance of a task carried out in the public interest; or
(f) legitimate interests pursued by the controller, subject to an additional balancing test against the data subject’s rights and interests.

While it is not necessary to specify in the proposal for a legislative text which ground applies, this issue should nevertheless be carefully considered when drafting the proposal and it must be ensured that one of the grounds will indeed apply.

Relevant legal grounds: Article 7(c) or (e)?

The two grounds that are most likely to apply to the data-matching are Article 7(c) in case of mandatory data-matching - and Article 7(e) in case of optional data-matching.

Article 7(c) presents similarities with Article 7(e), as a legal obligation may also be imposed in order to perform a public interest task. For Article 7(c) to apply, the obligation must be imposed by law. The law must fulfil all relevant conditions to make the obligation valid and binding, and must also comply with data protection law, including the requirements of lawfulness, necessity, proportionality, and purpose limitation.

In case the data-matching is optional (in the sense that competent authorities are free to decide themselves whether to match-data, and neither EU nor national law imposes a clear obligation to carry out data-matching), Article 7(c) is not an appropriate legal ground to be used, due to the fact that there is no 'legal obligation imposed' on the competent authority which can decide, optionally, whether or not to match the data.

This does not, however, mean that the data-matching in these optional cases is necessarily illegitimate as such. If appropriate, Article 7(e) may be considered instead.

Unlike in the case of Article 7(c), there is no requirement for the controller to act under a legal obligation. However, the processing must be 'necessary for the performance of a task carried out in the public interest'. Alternatively, either the controller or the third party to whom the controller discloses the data must be vested with an official authority and the data processing must be necessary to exercise the authority.

This official authority or public task will have been typically attributed in statutory laws or other legal regulations, especially if it implies an invasion of privacy. In such case, the legal basis should be specific and precise enough in framing the kind of data processing that may be allowed.

It is also relevant to note that Article 7(e) has potentially a very broad scope of application, which pleads for a strict interpretation and a clear identification, on a case by case basis, of the public interest at stake and the official authority justifying the processing. This broad scope also explains why a right to object has been foreseen in Article 14 when processing is based on Article 7(e)[1].

Based on the foregoing, irrespective whether or not Article 7(c) or (e) is used as a legal ground for the processing, in order to help ensure predictability and legal certainty, we strongly recommend that the legislative framework clearly specify the conditions under which data-matching is permissible (or required) and provide for the necessary safeguards. This brings us to our last point.

VII. Need for adequate safeguards

[1] This possibility to object does not exist in some Member States (e.g. Sweden) for processing of data based on Article 7(e).

In addition to bringing more predictability and legal certainty as to whether data-matching is permissible or not, and if so, to what extent and under what circumstances, the revision of the existing legal framework would also be an opportunity to provide for additional safeguards to protect the individuals concerned.

For example, as already suggested in your letter, it would be desirable if the security of the information exchange could be strengthened, possibly by using an existing European information technology system for the exchange of data, such as the Internal Market Information system (IMI) or another cross-border IT system, two options that the letter seems to suggest are currently considered.

In addition, the accuracy of the results of the data-matching is of particular importance. This is the case especially considering the significant consequences (ultimately, possible denial of benefits) of any inaccurate conclusions drawn as a result of data-matching. For this reason, we recommend that the revised legal framework calls for procedural safeguards to:

- ensure transparency about what data-matching consists of,
- ensure that there should be no automatic denial of benefits based on the results of the data-matching procedure, and
- guarantee fair procedures for individuals to contest any decisions that were taken on the basis of automatic matching procedures.

Brussels, 17 January 2014