Informal Meeting of European Data Protection Authorities

Bonn, 27 July 2006

Opinion on the data protection aspects of the

Convention

between

the Kingdom of Belgium,
the Federal Republic of Germany,
the Kingdom of Spain,
the French Republic,
the Grand Duchy of Luxembourg,
the Kingdom of the Netherlands and
the Republic of Austria

on the

stepping up of cross-border cooperation,
particularly in combating terrorism, cross-border crime and illegal migration
(Prüm-Convention)

1. Art. 1 para 4

The assessment of experience mentioned in this paragraph must also contain comments of data protection commissioners about the implementation of the Treaty. Data protection commissioners should be participated in this assessment.

2. Art. 2 para. 2

It should be clarified in the implementation agreement, that all data processed within the framework of this Treaty, except Art. 13, are personal data. That means that also databases containing only DNA profiles and reference data are to be considered collections with personal data. Therefore it should be referred to the definition of personal data given by the 95/46/CE directive : 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'

It seemed not to be clear what "untraceables" does mean. In the implementation agreement this should be defined as "biological traces from unknown persons collected during a legal procedure".

3. Art. 2 para. 3

The implementation agreement should include an annex with the list of all national DNA analysis files as referred to from articles 2 to 6 of the Treaty.

All Contracting Parties and DPA's of the contracting parties should know which data are in the national databases and what are the legal provisions for these databases. It must be clear which data are provided for access by the other parties.

4. Art. 5

It would be useful to specify e. g. by way of an enumeration, which "further personal data" are meant.
It should be clarified that all information transferred under this article has to be processed in compliance with Article 35 of the Prüm-Treaty.

5. Art. 6

The responsibility of the national contact point should be clarified in the implementation agreement.

6. Art. 8

The access to fingerprinting data should only be allowed if they are collected for the prevention and prosecution of crimes. Access should not be allowed if they are collected for administrative purposes, such as files for asylum purposes or for short-stay visas or even for identity documents.

7. Art. 9 para. 2

There should be a clarification in the implementing agreement on how the firm matching process of fingerprinting data may lead to a clear match.

8. Art. 12 para. 1

It should be defined which “other offences coming within…” are meant. In this context it should be listed in an annex of the implementation agreement precise categories of offences. It should also be clarified that administrative purposes/minor offences and automated searching will not justify direct access to vehicle registration data.
For the purpose of more transparency criteria for the access to the data should also be specified.

In this context referring to annex C-1 of the ATIA document Rev 5, setting out common data for automated search of vehicle registration data, it is not clear the inclusion in the table of a heading dedicated to “ID number” corresponding to an identifier of a person or a company. What are the aim and the justification for such a heading ?
In the same table in annex C-1, it seems not be justified in the light of the purpose of this register to have a heading providing for complete data relating to insurances.

9. Art. 13

Pursuant to this provision, it should be clarified that data by which persons can be identified directly or indirectly must not be transferred.

10. Art. 14 para. 1

The meaning of: “major events” and “cross-border dimension” has to be clarified. Not every event of international interest will justify data transfer (principle of proportionality). The use of data should only be allowed for the specific event.

It should be specified which data files might be subject to searches in the purpose of these article. A reference to the data files concerned needs to be provided for in the implementation agreement.
Access and transmission of the personal data by the authorities shall be strictly and adequately limited to the category of suspected persons.

In the implementation agreement the limitations and conditions of the “circumstances (that) give reason to believe that a data subject will commit criminal offences” should be elaborated. Especially where personal data can be supplied without request the conditions of those data should be clear.
Only sufficiently definite data files on suspects should be qualified for supply.

11. Art. 14 para. 2

It should be clarified what “without delay” does mean.

12. Art. 16

The supply of personal data should be limited to data on suspects.

13. Art. 33 para. 1 no. 4

It should be specified that “blocking” shall also mean to deny an access to the data concerned.

14. Art. 34 para. 1

The standards referred to in this paragraph have to be implemented in the Contracting States as a prerequisite for any data transfer.
If necessary, important aspects of these standards should be included in the implementation agreement.

15. Art. 34 para. 2

Before the decision on the transposition of the provisions of chapter 7 by the Committee of Ministers has been taken, the data protection authorities are to be heard prior to the implementation of the Treaty.

16. Art. 35

It should be clarified that this article refers to all personal data supplied within the framework of the Prüm-Treaty (e. g. index data and the further personal data). So far no exceptions are elaborated in bilateral agreements (Art. 47 para. 2).

17. Art. 36

The reference to « other entities » should be made clear in the annex :
- by a definition of the authorities or persons referred to : legal police services, magistrates (judges)...
- or the list of the competent authorities in compliance with the applicable national law
- and the list of the specifically authorized services or persons to receive the information.

All contracting parties must be aware of the situation in the other contracting parties.

18. Art. 37 para. 1

The obligation of the Contracting Parties to correct or delete an incorrect data refers to all data pools, especially records and files. This should be clarified in the implementing regulations.

19. Art. 37 para. 3

It is not clear which could be the concrete situation illustrating in article 37 para. 3 no. 1 the reservation for deletion of the data supplied without any request.

20. Art. 39 para. 1

It should be laid down a common standard of log data/log files. For this purpose, in each Contracting State the recorded data should be structured identically and be collected in a standardised way on the basis of agreed, pre-defined and generally comprehensible parameters.
It should be clarified that the use of logged data is only allowed for data security and monitoring data protection.

21. Art. 39 para. 3

In the implementing regulation the form and the manner of the foreseen communication of recorded data should be clarified.

22. Art. 39 para. 4

It should be taken into consideration, that a processing procedure has to guarantee the content-related correctness, informational value, confidentiality and integrity of the recorded data.
In so far provisions concerning the procedure would be necessary guaranteeing that the staff in charge of the operational service cannot access recorded data (e.g. blocking of these data).
Moreover it should be ensured e. g. by giving differentiated system administration rights to different persons that the recorded data should not be accessible to system administrators or that it is not possible for administrators to manipulate such data secretly,
Based on the fact that it is necessary to ensure that either the application or the user was indeed the one responsible for recording data, particular requirements emerge concerning the reliability of the separately done authentication and authorisation procedures, e. g. by appropriate logging analysis tools and by software-programmes.
Furthermore it should be considered that for an effective and targeted evaluation of quite large amount of accumulated data, the implementation of adequate automated evaluation programmes seems indispensable.

23. Art. 39 para. 5 sentence 3

It should be specified what “random checks” does mean. In the implementation agreement it should be determined a minimum of random checks, e. g. a certain quantity or a certain average of checks.
The carrying out of random checks should not only be binding for data protection authorities, but also for data controllers
The result of such checks only makes sense if it is disclosed to the data controller.

24. Art. 39 para. 5 sentences 6 and 7

The cooperation of the Contracting Parties’ data protection bodies should be institutionalised. In this framework it could be decided for example on the necessary arrangements concerning the transposition of concrete procedures, the harmonisation of individual or joint controls and regular exchange of experience.
The cooperation of the data protection authorities should be supported by the governments of the Contracting Parties.

'

25. Art. 40

Reference in the implementation agreement should be made to the logical imposition of effective, proportionate and dissuasive criminal sanction in accordance with the national law of the respective state for offences committed implying infringements of the rules of data protection

Moreover it should be clarified or concretised in connection with the required proof of identity, the reasonability of expenses and of any delay taking into consideration that the right of information is one of the data subjects' central rights.

In cases in which data of a person making a request are contained in data pools of several or of all Contracting States, the petitioner should not be referred to the competent bodies of the other Contracting States holding the respective data, but the body contacted by the petitioner should be able to provide the information by cooperating with other competent bodies of the Contracting Parties.

26. Art. 43 para. 1

It should be provided for that data protection authorities are to be heard as far as data protection questions are concerned. Concerning the implementation of agreements, it should also be possible that data protection authorities have the opportunity to contribute to this agreement before finalising it.

27. Art. 44

The implementation agreement should be published.