

ARTICLE 29 Data Protection Working Party



Brussels, 22 June 2015

Directorate-General for Communications
Networks, content and Technology
Task Force Legislation Team (eIDAS)
Mr. Andrea Servida
Head of Task Force
European Commission
B - 1049 BRUSSELS Belgium

Dear Mr Servida,

Thank you for your letter, the email from May 5th and the enclosed drafts of the non-papers as well as your kind invitation to Dr Amandine Jambert (CNIL, France) and Dr Sabine Sosna (BfDI, Germany) of the EGovernment Subgroup to attend the meetings of the eIDAS Expert Group on the 21st of April and 12th of May.

On that occasion we had the possibility to point out our major concern regarding the draft of the non-paper on interoperability framework (in the versions that were presented at the meetings), which is the wording with regard to personal data, technical data and the storage of such data in the nodes.

In particular Article 7 (2) states that, “The nodes shall not store any personal data, but only technical information”. According to the new Article 10 (3) (former Article 7 (3)) “the [stored] data shall, as a minimum, consist of a node’s ID, message ID, message date and time”. In this context we highlighted, that technical data may constitute personal data, depending on the possibility to relate them to a natural person. Article 2 (a) of the Data Protection Directive 95/46/EC defines personal data as “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”. Further explanations can be found in the WP29 Opinion WP136.

In this regard we welcome the requirement that personal data is not stored by the nodes. We also appreciate that the Expert Group is willing to address the purpose of storing and categories of data to be stored. However it seems that the message ID can be linked to the data subject in some cases. For example, when an error occurs, some member states keep both the data which raised the error and the message ID. In those cases, the message ID would thereby constitute personal data.

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental rights and Union citizenship) of the European Commission, Directorate-General for Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 02/13

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

For that reason the WP29 highlights the need to revise the wording of Article 7 (2) or, at least, specify the categories of data to be stored in the nodes as long as they can be related to a natural person.

Two further aspects of the implementing acts affecting data protection issues, which the representatives of WP29 did not have the opportunity to discuss at the meeting on 12th of May, should be addressed.

The first one is related to the duration of the storage of technical data in the nodes, in the case that the data constitutes personal data. Article 10 (3) (former Article 7 (3)) states that the mentioned data shall “be stored for a period of time in accordance with national requirements”. We have learned that this wording is the compromise of a discussion between the Experts because the retention period varies significantly in the Member States from a minimum period to a maximum period (i.e. from days to months). We understand that there are different requirements in the Member States and therefore an agreement could not be reached. However it should be taken into consideration that the processing of data in the node is not covered by national legislation. The national legislation covers only data processing in the Member States. Cross-border transfer of the technical data is an operation prescribed by the Regulation as an aspect of the trusted electronic identification framework which the European Legislator aims at establishing with a view to ensuring the interoperability of electronic identification schemes. Therefore, it is up to the implementing acts to define a retention period of such data which should not exceed the time that is necessary for the purpose it is required for.

The second issue we would like to raise is the wording concerning identification and authentication in the non-papers. Electronic identity systems in Europe seem to serve the following different functions:

1. identification of an individual among the population (e.g. through the use of a specific identifier or of a list of attributes sufficient to define only one individual in the EU or the world);
2. proof of the validity of a claimed identity data (e.g. proof of first name and surname);
3. demonstration of some attributes (i.e. citizenship, age, etc.) ;
4. authentication of an individual to a service (i.e. proof that she is the same as the enrolled person, which is usually done by proving a link with an alias).

The definition of electronic identification in Article. 3 (1) of the Regulation 910/2014 is referring to the first function by stating that it is a “process of using person identification data in electronic form uniquely representing either a natural or legal person or a natural person representing a legal person”.

Authentication in point 5 of the same article is defined as the “electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data on electronic form to be confirmed”. Thus it refers to the second function by allowing the electronic identification of a person and implies the fourth function by confirming the origin and integrity of data.

In this regard, it should be underlined that Article 5 (1) of the Regulation states that processing of personal data shall be carried out in accordance with Directive 95/46/EC. Moreover, Recital 11 of the Regulation affirms that “(...) In this respect, having regard to the principle of mutual recognition established by this Regulation, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online.”

The implementation acts seem to only consider authentication as the identification of one individual among the population and thus equals to the first function. Moreover, this process is defined by the verification of (at least) a fixed set of attributes defined as the “minimum data set”, this set being optionally extendable to additional attributes in order to “uniquely represent a person”.

According to the data minimization principle, which is a general data protection principle but also more precisely defined in Recital 11 of this act, the authentication system, as resulting by the implementing acts, will not be adequate in all circumstances, namely in cases in which some of the attributes in the minimum data set are not relevant for a given service or when it is only needed to prove that a person has enrolled before.

Furthermore Article 5 (2) of the Regulation states that “Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.” Nonetheless the implementation acts do not take into due account the usage of pseudonyms. In fact, pseudonyms are not mentioned (even as an optional additional attribute) in the lists of attributes defined in the interoperability non-paper, while current first name, family name, date of birth as well as a unique identifier will be given at each authentication process. Thus the use of pseudonyms where full identification data are not required for the service provided is not foreseen in the draft.

Yours sincerely,

On behalf of the Article 29 Working Party,

Isabelle FALQUE-PIERROTIN
Chairwoman

Attachment:

- [WP 136 Opinion 4/2007 on the concept of personal data](#)