

**Executive summary of the Opinion of the European Data Protection Supervisor on the Commission proposal for a regulation of the European Parliament and of the Council on trust and confidence in electronic transactions in the internal market (Electronic Trust Services Regulation)**

*(The full text of this Opinion can be found in English, French and German on the EDPS website: <http://www.edps.europa.eu>)*

(2013/C 28/04)

## **I. Introduction**

### *I.1. The proposal*

1. On 4 June 2012, the Commission adopted a proposal for a regulation of the European Parliament and of the Council amending Directive 1999/93/EC of the European Parliament and of the Council as regards electronic identification and trust services for electronic transactions in the internal market (the proposal) <sup>(1)</sup>.

2. The proposal is part of the measures put forward by the Commission to strengthen the deployment of electronic transactions in the European Union. It follows up on the actions foreseen in the Digital Agenda for Europe <sup>(2)</sup> relating to improving the legislation on e-signatures (Key Action 3) and providing a coherent framework for the mutual recognition of e-identification and authentication (Key Action 16).

3. The proposal is expected to enhance trust in pan-European electronic transactions and to ensure cross-border legal recognition of electronic identification, authentication, signature and related trust services in the internal market while guaranteeing a high level of data protection and user empowerment.

4. A high level of data protection is essential for the use of electronic identification schemes and trust services. The development and use of such electronic means must rely upon the adequate processing of personal data by trust service providers and electronic identity issuers. This is all the more important as such processing will be relied upon, amongst other things, for identifying and authenticating natural (or legal) persons in the most reliable manner.

### *I.2. Consultation of the EDPS*

5. Before the adoption of the proposal, the EDPS was given the possibility to provide informal comments. Many of these comments have been taken into account in the proposal. As a result, the data protection safeguards in the proposal have been strengthened.

6. The EDPS welcomes the fact that he is also formally consulted by the Commission in accordance with Article 28(2) of Regulation (EC) No 45/2001.

### *I.3. Background of the proposal*

7. The proposal is based on Article 114 of the Treaty on the Functioning of the European Union and sets forth the conditions and mechanisms for mutual recognition and acceptance of electronic identification and trust services among Member States. In particular, it lays down the principles relating to the provision of identification and trusted electronic services, including the rules applicable to recognition and acceptance. It also provides the requirements for the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication and electronic certificates.

8. In addition, the proposed regulation lays down the rules for the supervision of the provision of trust services and obliges Member States to establish supervisory bodies for this purpose. These bodies will, amongst other tasks, assess the compliance of the technical and organisational measures implemented by the providers of electronic trust services.

<sup>(1)</sup> COM(2012) 238 final.

<sup>(2)</sup> COM(2010) 245 of 19.5.2010.

9. Chapter II deals with electronic identification services while Chapter III is dedicated to other electronic trust services such as electronic signatures, seals, time stamps, documents, delivery services, certificates and website authentication. Electronic identification services are related to national identification cards and can be used in the access to digital services and in particular to e-government services; this means that an entity issuing electronic identification is acting on behalf of a Member State and that Member State is responsible for correctly establishing the correlation between a concrete individual and his/her electronic identification means. With regard to other electronic trust services, the provider/issuer is a natural or legal person which is responsible for the correct and safe provision of these services.

#### *1.4. Data protection issues raised by the proposal*

10. The processing of personal data is inherent in the use of identification schemes and to some degree also in the provision of other trust services (for instance in case of electronic signatures). Processing of personal data will be required in order to establish a trustable link between the electronic identification and authentication means used by a natural (or legal) person and that person, in order to certify that the person behind the electronic certificate is truly who he/she claims to be. For instance, electronic identifications or electronic certificates refer to natural persons and will include a set of data unambiguously representing those individuals. In other words, the creation, verification, validation and handling of the electronic means referred to in Article 3(12) of the proposal will, in many cases, involve the processing of personal data and therefore data protection becomes relevant.

11. It is, therefore, essential that the processing of data in the context of the provision of electronic identification schemes or electronic trust services is done in accordance with the EU data protection framework, in particular with national provisions implementing Directive 95/46/EC.

12. In this Opinion, the EDPS will focus his analysis on three main issues:

- (a) how data protection is addressed in the proposal;
- (b) data protection aspects of electronic identification schemes to be recognised and accepted across borders; and
- (c) data protection aspects of electronic trust services to be recognised and accepted across borders.

### **III. Conclusions**

50. The EDPS welcomes the proposal as it can contribute to mutual recognition (and acceptance) of electronic trust services and identification schemes at European level. He also welcomes the establishment of a common set of requirements that must be fulfilled by the issuers of electronic identification means and by trust service providers. Notwithstanding his general support for the proposal, the EDPS wishes to provide the following general recommendations:

- data protection provisions included in the proposal should not be restricted to trust service providers and should also be applicable to the processing of personal data in the electronic identification schemes described in Chapter II of the proposal,
- the proposed regulation should set a common set of security requirements for trust service providers and electronic identification issuers. Alternatively, it could allow the Commission to define where needed, through a selective use of delegated acts or implementing measures, the criteria, conditions and requirements for security in electronic trust services and identification schemes,
- electronic trust service providers and electronic identification issuers should be required to provide the users of their services with: (i) appropriate information on the collection, communication, and retention of their data, as well as (ii) a means to control their personal data and exercise their data protection rights,

- the EDPS recommends a more selective inclusion in the proposal of the provisions empowering the Commission to specify or detail concrete provisions after the adoption of the proposed regulation by delegated or implementing acts.

51. Some specific provisions concerning the mutual recognition of electronic identification schemes should also be improved:

- the proposed regulation should specify which data or categories of data will be processed for cross-border identification of individuals. This specification should contain at least the same level of detail as provided in annexes for other trust services and should take into account the respect of the principle of proportionality,
- the safeguards required for the provision of identification schemes should at least be compliant with the requirements set forth for the providers of qualified trust services,
- the proposal should establish appropriate mechanisms to set a framework for the interoperability of national identification schemes.

52. Finally, the EDPS also makes the following recommendations in relation to the requirements for the provision and recognition of electronic trust services:

- it should be specified with regard to all electronic services if personal data will be processed and, in the cases where personal data will be processed, the data or categories of data to be processed,
- the regulation should take appropriate safeguards to avoid any overlap between the competences of the supervisory bodies for electronic trust services and those of data protection authorities,
- the obligations imposed on electronic trust service providers concerning data breaches and security incidents should be consistent with the requirements established in the revised e-privacy Directive and in the proposed data protection regulation,
- more clarity should be provided to the definition of private or public entities that can act as third parties entitled to carry out audits under Articles 16 and 17 or that can verify electronic signature creation devices under Article 23, as well as on the criteria under which the independence of these bodies will be assessed,
- the regulation should be more precise in setting a time limit for the retention of the data referred to in Article 19(2) and (4) <sup>(1)</sup>.

Done at Brussels, 27 September 2012.

Giovanni BUTTARELLI  
*Assistant European Data Protection Supervisor*

---

<sup>(1)</sup> Under Article 19(2)(g), qualified trust service providers must record for an appropriate period of time all relevant information concerning data issued and received by them. Under Article 19(4), qualified trust service providers should provide any party relying on the certificates with information on the validity or revocation status of qualified certificates issued by them.