



EUROPEAN DATA
PROTECTION SUPERVISOR

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 EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,¹

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 28(2) thereof,²

HAS ADOPTED THE FOLLOWING OPINION:

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')³.
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 Europe⁴ 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).

¹ OJ L281, 23.11.1995, p. 31.

² OJ L8, 12.1.2001, p. 1.

³ COM (2012) 238 final.

⁴ COM (2010) 245 of 19.5.2010.

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 protections 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 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.
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.

I.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 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.

II. ANALYSIS OF THE PROPOSAL

II.1. How data protection is addressed in the Proposal

Applicability of data protection legislation to electronic identification schemes and trust services

13. As a starting point, the EDPS emphasises that electronic trust services and identification schemes provided by, on behalf or under the responsibility of Member States, to trust service providers must fulfil specific conditions. Lack of appropriate safeguards could lead to significant data protection risks. For instance, there could be a risk of identity theft or misuse of the electronic means and this could have serious adverse consequences on the individuals affected.
14. In view of the risks associated to the provision of each service, appropriate safeguards must be put in place. Furthermore, if these services are to be used for cross-border transactions, there is a clear benefit in harmonising further these safeguards at EU level. The EDPS welcomes recital 24 which acknowledges that trust service providers are data controllers of personal data and, as a consequence, have to comply with the obligations set out in Directive 95/46/EC.

The EDPS also welcomes that Article 11 lays down specific data protection and data minimisation requirements, which are in line with Directive 95/46/EC.

15. However, the EDPS notes that both recital 24 and Article 11 are only related to trust service providers and do not seem to include the processing of personal data in the electronic identification schemes described in Chapter II of the Proposal. The Explanatory Memorandum⁵ argues that such requirements cannot be imposed on identification schemes as they are a national prerogative.
16. On the other hand, the Explanatory Memorandum⁶ also states that the coordination required to remove the existing barriers (absence of legal certainty and difficulties for interoperability) can be done more effectively at the EU level.
17. In the view of the EDPS, from a data protection perspective, it would not be incompatible with EU law nor with the principle of subsidiarity to lay down in an EU Regulation a set of minimum requirements aimed at ensuring the interoperability of schemes as well as an harmonised level of data protection while at the same time leaving a margin of manoeuvre to Member States in the way in which they will implement these requirements at national level.
18. Considering that the adverse consequences of any misprocessing through identification schemes would be higher than with any other trust service, in particular because of the level of trust and reliability they are meant to provide in cross-border contexts, it appears justified to introduce a consistent set of requirements at EU level for electronic identification services.

Security provisions

19. The EDPS welcomes that the Proposal foresees in Articles 15 and 16 specific security requirements for trust service providers as well as the supervision of these requirements by competent bodies. However, the EDPS notes that there is still a certain risk of divergence in the implementation of these requirements since each trust service provider has a margin to adopt, according to its own criteria, the technical and organisational measures that it considers appropriate for the risks associated to the service, having regard to the state of the art.
20. Against this background, the EDPS considers that the proposed Regulation should establish a minimum set of requirements, in particular with respect to the circumstances, formats and procedures associated to security as well as the criteria, conditions and requirements, including the determination of what constitutes the state of the art in terms of security for electronic trust services. Articles 15(6) and 16(6) of the Proposal envisage that these minimum requirements could be further defined by the Commission at a later stage through delegated legislation. However, the EDPS underlines that the legislator should assess carefully, by applying a selective approach, the areas in which

⁵ P. 4, when referring to the necessity test.

⁶ P. 4, when referring to the effectiveness test.

these minimum requirements could be set by way of delegated legislation instead of being provided for in the proposed Regulation itself.

Additional data protection aspects to be taken into consideration

21. The EDPS is of the view that in addition to the elements referred to in Article 11 on data protection, other aspects should be taken into account. In particular, data controllers (trust service providers as well as providers of electronic identification schemes) 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) means to control their personal data and exercise their data protection rights. The need for transparency and clear information is connected to the validity of the consent obtained. From a data protection perspective, consent is a pre-requisite for processing personal data and is only valid where it is based on a free choice and on the basis of proper information⁷. The EDPS advises including in the Proposal specific references to data subjects' rights and in particular to the right of access and the right to be informed.
22. Article 11 of the Proposal provides that existing legislation in Member States allowing the use of pseudonyms shall not be affected by the Regulation. As recital 27 clarifies, pseudonyms shall be provided in such a way that the individual concerned can still be identified pursuant to Union or national law. Consequently, the data processed will be considered personal data⁸ even if pseudonyms are used. In order to avoid misconceptions, this should be stated in the proposed Regulation (preferably, in Article 11(4) or in a recital).
23. Finally, the EDPS is of the view that Privacy Enhancing Technologies ('PETs') can be enablers of a correct balance between the achievement of the objectives of the proposed Regulation and the respect of the rights of individuals in terms of data protection. The EDPS recommends that the proposed Regulation takes stock of the importance of PETs as enablers of trust by requiring that trust service providers and providers of identification services take PETs into consideration when defining an electronic service scheme. This approach will be in line with the 'data protection by design' approach foreseen in the recent proposal of the Commission on the review of the data protection framework⁹.

Use of delegated acts and implementing measures

24. In many provisions of the proposed Regulation the Commission is empowered to adopt delegated acts or implementing measures. Although such further acts and measures might contribute to the uniform application of the Regulation and may allow for further alignment of national practices based on experience gained after the Regulation applies, the EDPS has reservations as to an approach

⁷ See Article 29 Working Party Opinion 15/2011 on the definition of consent, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

⁸ As defined in Article 2(a) of Directive 95/46/EC.

⁹ Proposal for a Regulation of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final (Article 23).

that relies upon them so heavily. As mentioned in paragraph 20 above, the EDPS considers that the areas in which such delegated legislation would be useful should be carefully assessed by applying a more selective approach. The EDPS foresees the risk that such acts and measures are not yet adopted when the Regulation applies, which may affect the consistent application of the Regulation, in particular from a data protection perspective. This may be the case for example, for the security measures to be promptly respected by trust services or for the requirements for electronic signatures creation devices.

II.2. Data protection aspects in electronic identification schemes to be recognised and accepted across borders

25. The Proposal leaves very wide discretion to Member States (see in particular recitals 11 and 12) to create, define, and introduce means for electronic identification purposes and electronic identification schemes. The EDPS understands that this can be necessary to accommodate the different requirements in the different Member States and he is also aware that electronic identification schemes are already deployed in several Member States. Nevertheless, the EDPS calls for an approach that respects the different requirements in each Member State, but at the same time can set forth a common set of conditions to be applied for the use of national identification schemes across borders.

Categories of data processed

26. The processing of personal data is inherent to the electronic identification schemes of natural persons. Therefore, it is clear that the entities creating, verifying, validating, handling and preserving data will be processing personal data. However, the Regulation does not determine which data or categories of data will be processed.
27. The EDPS considers that the Regulation should identify which data or categories of data will be processed for cross border identification of individuals, at least in the same level of detail as it is done in the annexes for other trust services.
28. Furthermore, data minimisation is critical also in case of cross-border processing. Therefore, the Regulation should provide for specific goals:
 - Minimisation of the amount of data categories included in the electronic identification scheme. In particular, special attention should be given to biometric data.
 - Selective and partial disclosure of identity data, depending of the purpose for which the electronic identity is used for (for instance, a data subject that only needs to prove his/her age or that he/she lives in a specific town should not be obliged to disclose additional data).

Conditions for mutual recognition

29. The EDPS welcomes the framework for the establishment of mutual recognition as defined in Article 6. At the same time, he considers that the proposed requirements are set at a very general level and therefore do not yet provide a solid and harmonised framework for mutual recognition and acceptance of electronic identification.
30. According to the Proposal, the main requirements for an identification scheme to be recognised and accepted at European level are: (i) a Member State must notify the European Commission of the scheme, (ii) such scheme must be accepted in the jurisdiction of the country making the notification and (iii) the identification means must be issued by, on behalf of, or at least under the responsibility of the Member State notifying the scheme. However, no specific requirements are set forth for the public competent authorities or private entities issuing the identification means on behalf of the Member State. For instance, under the proposed Regulation these entities issuing identification means will not be subject to the supervision mechanisms provided for in Articles 13 and 14 or will not have to comply with the security, supervision and organisational requirements set forth in Articles 15, 16, 17 and 19. This approach can lead to heterogeneity and to different levels of data protection safeguards depending on the identification scheme being used.
31. The safeguards to be implemented by a provider should be proportionate to the potential risks of the service provided. Furthermore, mutual recognition can only work where it is based on a common minimum level of protection. Consequently, as the risks associated to the issuing of electronic identification means are important, the safeguards required should at least be compliant with the requirements set forth for the providers of qualified trust service¹⁰ in Articles 15,16 and 17. In the view of the EDPS, a competent authority issuing electronic identification means to interact with e-government services should be subject to higher security controls than a trust service provider issuing certificates to the clients of a supermarket in order to make their online shopping.
32. Consequently, the EDPS recommends that Article 6, while acknowledging that issuing identification means is a national prerogative, also takes stock that national schemes, which are to be notified for cross-border acceptance and recognition, should offer at least an equivalent level of safeguards than those required for qualified trust services. In practical terms this would mean that, in addition to the conditions already laid down in Article 6, the providers of such identification means should at least be subject to the same conditions required for the providers of qualified electronic trust services in terms of supervision (Articles 13, 14 and 16) and security, technology and organisation (Articles 15, 17 and 19).

¹⁰ Note that the risks associated to the processing of personal data in an electronic identification scheme can be higher than in case of other electronic trust services (for instance, they can lead to identity theft, affect national security and in many cases could have enormous adverse effects for the individuals affected).

Interoperability

33. Recitals 7, 15, 16 and 49 of the Proposal stress the importance of the interoperability of electronic trust services and identification schemes in order to increase their adoption and their usefulness. However, the proposed Regulation does not include specific provisions detailing the mechanisms that should ensure interoperability at European level¹¹. Further clarity is required since Article 6 is limited to making a brief reference to the need of establishing a coordination mechanism for the exchange of good practices and experiences.
34. In particular, the establishment of a framework for the interoperability of national electronic identification schemes and trust services is aimed at improving the effectiveness of the Regulation. Consequently, the EDPS recommends that the Regulation harmonises at least those aspects that are crucial for the interoperability, such as the data fields that will be used for identification of individuals, the security requirements and the data protection safeguards.

II.3. Data protection aspects in trust services to be recognised and accepted across borders

35. The EDPS welcomes the envisaged improvements compared to Directive 1999/93/EC on a Community framework for electronic signatures¹² in terms of harmonisation of the conditions for the provision of trust services. This new approach will provide better legal certainty for providers operating at European level as well as to users and third parties relying on the trust services. It will also contribute to removing barriers for the internal market that arise from divergent national interpretations of Directive 1999/93/EC and heterogeneous applications of technical solutions.
36. Notwithstanding this general support, the EDPS wishes to underline several aspects where the Proposal should provide further clarity.

Categories of data processed

37. The EDPS welcomes that specific annexes have been set forth for the different electronic services that will be provided and that these annexes include specific details on the data categories that will be processed. However, the EDPS notes that in some cases the categories of personal data to be processed are not clearly identified. For instance, for qualified certificates for electronic signatures, Annex I requires '*a set of data unambiguously representing the signatory*' in qualified certificates. This can vary a lot for electronic signatures: for example, it is not clear whether a name and address, a personal identification number or biometric data would/could be used to 'unambiguously represent' the signatory.
38. From a data protection point of view, it is crucial to understand which personal data are processed and in what circumstances, in order to assess data protection

¹¹ For instance, the European validation authorities' gateway to ensure the cross-border interoperability of electronic signatures and to increase the security of transactions carried out using the internet.

¹² OJ L 13, 19.1.2000, p. 12.

implications and provide adequate safeguards. Consequently, the EDPS recommends that the Regulation specifies with regard to all electronic services if personal data will be processed and where this is the case, which data or categories of data should be included as a minimum. Of course, a margin of manoeuvre could be left to the trust service provider for the inclusion of additional data if it is needed for the service to be provided. This approach will be in line with the data minimisation principle (as referred to in Article 11) and will also facilitate the integration and interoperability of different trust services.

Mutual recognition at international level

39. Article 10 of the Proposal provides that international agreements may be concluded in accordance with Article 218 TFEU¹³, which would allow recognition of qualified trust services and qualified certificates issued by providers in third countries as being equivalent to those issued by providers established in the EU.
40. Under such agreements, third country providers will be full competitors to EU providers, offering their services also to customers established in the EU. The EDPS welcomes that qualified trust services provided by trust service providers in third countries or international organisations have to comply with the same requirements as the ones provided by European trust service providers. It is also welcomed that protection of personal data, security and supervision are explicitly mentioned.

Supervision

41. The EDPS notes that the tasks of the supervisory bodies foreseen in Articles 13 and 14 of the Proposal may overlap with the tasks of independent data protection authorities¹⁴. Independent supervision is an essential element of the EU data protection rules. This follows from Article 8 of the Charter and Article 16 TFEU and has been underlined by the Court of Justice in the Commission/Germany ruling of March 2010¹⁵. As a consequence, the specific competences of independent data protection authorities should not be attributed to other supervisory authorities who do not have the same status and are not recognised at the same level in EU legislation. An overlap of competences might also endanger the unity of action required in terms of supervision.
42. Therefore, the EDPS recommends that the Proposal further details the definition of the role and competences of the supervisory bodies with a view to avoiding overlap with the competences of data protection authorities. A cooperation mechanism may be put in place to guarantee the consistency of the approaches taken by both trust services supervisory bodies and data protection authorities.

¹³ Article 218 sets the procedure for the adoption of international agreements and the involvement of the main parties, in particular the Council and the European Parliament.

¹⁴ For instance under Article 15(4) the competent supervisory bodies defined shall have the power to issue binding instructions to trust service providers concerning security measures.

¹⁵ CJEU, 9 March 2010, Commission/Germany, C-518/07, [2010] ECR I-1885, paras 23 and 50.

43. Finally, under Article 17(1), a qualified trust service provider may start a qualified trust service right after submitting a notification and a security audit to the supervisory body but without the need to wait for the verification from the supervisory body. In that situation, under Article 17(3), the supervisory body shall verify the compliance of the qualified trust service provider and of the qualified trust services provided with the requirements of the Regulation within one month¹⁶. The EDPS notes that in case the supervisory body makes a negative evaluation of the trust service provider or the trust service provided, this could potentially create legal uncertainty with regards to the electronic means already issued by the qualified trust service provider and also with the transactions or documents in which those means had been used. Consequently, the EDPS recommends that a positive *ex-ante* verification of the supervisory bodies is required in order to initiate the service provision.

Data breaches

44. The EDPS welcomes that provisions on data breaches have been included in the proposed Regulation considering the significant adverse impact that data breaches can have on the individuals affected. The adverse impacts of the data breach should not be merely assessed by taking into consideration only the personal data managed by the trust service provider. Instead, it should also be considered whether the data compromised could potentially be used by third parties to digitally impersonate the individuals or legal entities, and therefore multiply the adverse effects for the individuals. A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm for the individuals concerned, including identity fraud.
45. The EDPS notes that there is no definition in the proposed Regulation of the notions of '*breach of security*' or '*loss of integrity*' and there is no clarification of what '*a significant impact*' would mean. Therefore, the notion of data breach should be defined more precisely in the proposed Regulation and included in Article 3. This could be done in similar terms as the definitions provided in Article 2(i) of the revised e-privacy Directive¹⁷ or in Articles 31 and 32 of the new proposed data protection Regulation.
46. In particular, the definition should be consistent with the obligations imposed on data controllers to mandatorily notify the national competent supervisory authorities of personal data breaches, and to notify individuals in case the data breach is likely to adversely affect them. In this context, the EDPS recommends including specific provisions to ensure the alignment of the notification procedures. For instance, a cooperation mechanism could be envisaged between the supervisory body foreseen in the Proposal and other national supervisory

¹⁶ Article 17(3) allows the supervisory authority to delay the verification by informing the qualified trust service provider of the reasons of the delay and the period by which the verification shall be concluded.

¹⁷ Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services amending Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

authorities that must be notified of these data breaches, such as data protection authorities¹⁸.

Third party audit and certification

47. The EDPS notes that pursuant to Articles 16 and 17, the execution of third party audits plays a very important role in order to ensure that the trusted service providers are compliant with the requirements included in the proposed Regulation. The EDPS welcomes this approach but calls for more clarity concerning the definition of the third parties entitled to carry out such audits, as well as concerning the methodology and scope for these audits. For instance the EDPS recommends that instead of referring to these third party auditors as *recognised independent bodies*,¹⁹ the Proposal should require that these third parties are recognised as independent bodies only after supervisory bodies have verified their independence on the basis of specific criteria and have approved the methodology and scope of the audits to be carried out.
48. The same consideration should be applied to the *appropriate public or private bodies designated by Member States* in charge of verifying electronic signatures creation devices (Article 23,). The EDPS recommends that supervisory bodies should be in charge of designating these bodies. Further, Article 23 also mentions that these certification bodies will carry out evaluations on the basis of a list of standards, to be established by the Commission by means of implementing acts. The EDPS recommends that the proposed Regulation establishes a deadline for the adoption of such implementing acts. Otherwise it would be impossible to certify qualified electronic signature creation devices and therefore impossible to create qualified electronic signatures.

Recording and disclosure of data by trust service providers

49. The Proposal sets forth specific requirements for recording information that raise some concerns from a data protection point of view:
 - Under Article 19(2).g, qualified trust service providers must record all relevant information concerning data issued and received for an appropriate period of time. The EDPS notes that the Regulation should be more precise and set a time limit for the retention of this information, for instance by limiting it to the time until when the information could be required for the purpose of legal proceedings. Article 19(2) should also spell out clearly the type of information that must be recorded, instead of requiring the recording of all relevant information.
 - 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 they issue. This requirement is very open and does not impose any restriction on how long this information should be stored. The EDPS

¹⁸ As it is foreseen in the data protection reform package proposed by the Commission on 25 January 2012.

¹⁹ See Recital 49 and Articles 16 and 17 of the Proposal.

recommends that this information should only be made available until the expiry date of the certificate.

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 in Articles 19(2) and 19(4)²⁰.

Done in Brussels, on 27 September 2012

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor

²⁰ 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