

**Résumé de l'avis du Contrôleur européen de la protection des données sur la proposition de la Commission relative à un règlement du Parlement européen et du Conseil sur la confiance pour les transactions électroniques au sein du marché intérieur (règlement sur les services de confiance électroniques)**

(Le texte complet de l'avis en anglais, français et allemand est disponible sur le site internet du CEPD <http://www.edps.europa.eu>)

(2013/C 28/04)

## I. Introduction

### I.1. La proposition

1. Le 4 juin 2012, la Commission a adopté une proposition de règlement du Parlement européen et du Conseil modifiant la directive 1999/93/CE du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur («la proposition») <sup>(1)</sup>.

2. La proposition s'inscrit parmi les mesures soumises par la Commission en vue de renforcer le déploiement des transactions électroniques dans l'Union européenne. Elle fait suite aux actions prévues dans la stratégie numérique pour l'Europe <sup>(2)</sup> visant à améliorer la législation relative aux signatures électroniques (action clé 3) et à fournir un cadre cohérent pour la reconnaissance mutuelle des services d'identification et d'authentification électroniques (action clé 16).

3. La proposition vise à améliorer la confiance dans les transactions électroniques paneuropéennes et à permettre la reconnaissance juridique transnationale de l'identification, de l'authentification et de la signature électroniques ainsi que des services de confiance connexes au sein du marché intérieur, tout en garantissant un niveau élevé de protection des données et la responsabilisation des utilisateurs.

4. Un niveau élevé de protection des données est essentiel du point de vue de l'utilisation des systèmes d'identification électronique et des services de confiance. Le développement et l'utilisation de tels moyens électroniques doit s'appuyer sur le traitement adéquat des données à caractère personnel par les prestataires de services de confiance et par les entités délivrant une identité électronique. Ce point est d'autant plus important que ce traitement servira, notamment, à identifier et à authentifier des personnes physiques (ou morales) de la manière la plus fiable possible.

### I.2. Consultation du CEPD

5. Avant l'adoption de la proposition, le CEPD a eu la possibilité de formuler des observations informelles. Un grand nombre de ces observations ont été prises en considération dans la proposition, si bien que les garanties en matière de protection des données présentes dans la proposition ont été renforcées.

6. Le CEPD se réjouit d'être également consulté formellement par la Commission conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001.

### I.3. Contexte de la proposition

7. La proposition est basée sur l'article 114 du traité sur le fonctionnement de l'Union européenne et fixe les conditions et mécanismes régissant la reconnaissance et l'acceptation mutuelles de l'identification électronique et des services de confiance entre les États membres. En particulier, elle définit les principes relatifs à la fourniture de services d'identification et de confiance électronique, y compris les règles applicables à la reconnaissance et à l'acceptation. Elle fournit aussi les exigences en matière de création, vérification, validation, traitement et conservation de signatures électroniques, de cachets électroniques, d'horodatages électroniques, de documents électroniques, de services de fourniture électroniques et de certificats électroniques.

8. En outre, le règlement proposé arrête les règles relatives au contrôle de la fourniture de services de confiance et oblige les États membres à créer un organe de contrôle à cette fin. Ces organes auront notamment pour tâche d'évaluer la conformité des mesures techniques et organisationnelles mises en œuvre par les prestataires de services de confiance électroniques.

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

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

9. Le chapitre II porte sur les services d'identification électronique tandis que le chapitre III est consacré à d'autres services de confiance électroniques comme les signatures, cachets, horodateurs, documents, services de fourniture, certificats et authentification de sites internet électroniques. Les services d'identification électronique sont liés à des cartes d'identification nationales et peuvent être utilisés pour accéder à des services numériques, notamment à des services d'administration en ligne; en d'autres termes, une entité délivrant une identification électronique agit au nom d'un État membre et cet État membre est responsable de l'établissement correct de la corrélation entre un individu concret et ses moyens d'identification électronique. En ce qui concerne d'autres services de confiance électroniques, le prestataire/l'entité qui délivre l'identité est une personne physique ou morale qui est responsable de la fourniture correcte et en toute sécurité de ces services.

#### I.4. Questions relatives à la protection des données soulevées par la proposition

10. Le traitement de données à caractère personnel est inhérent à l'utilisation de systèmes d'identification et, dans une certaine mesure, à la fourniture d'autres services de confiance (par exemple, dans le cas de signatures électroniques). Le traitement de données à caractère personnel sera requis aux fins d'établir un lien fiable entre les moyens d'identification et d'authentification électroniques utilisés par une personne physique (ou morale) et la personne en question, pour certifier que la personne correspondant au certificat électronique est effectivement celle qu'elle prétend être. Par exemple, les identifications électroniques ou les certificats électroniques se rapportent à une personne physique et incluent un ensemble de données représentant ces personnes de manière non ambiguë. En d'autres termes, la création, la vérification, la validation et le traitement des moyens électroniques visés à l'article 3, paragraphe 12, de la proposition impliqueront, dans de nombreux cas, le traitement de données à caractère personnel, raison pour laquelle la protection des données devient pertinente.

11. Par conséquent, il est essentiel que le traitement des données dans le contexte de la fourniture de systèmes d'identification électronique ou de services de confiance électroniques soit réalisé dans le respect du cadre de protection des données de l'UE, en particulier des dispositions nationales qui mettent en œuvre la directive 95/46/CE.

12. Dans le présent avis, le CEPD concentrera son analyse sur trois questions principales:

- a) la façon dont la proposition aborde la question de la protection des données;
- b) les aspects de la protection des données des systèmes d'identification électronique qui doivent être reconnus et acceptés par-delà les frontières; et
- c) les aspects de la protection des données des services de confiance électroniques qui doivent être reconnus et acceptés par-delà les frontières.

### III. Conclusions

50. Le CEPD salue la proposition, qui peut contribuer à la reconnaissance (et à l'acceptation) mutuelle(s) des services de confiance électroniques et des systèmes d'identification électronique au niveau européen. Il se réjouit aussi de l'établissement d'un ensemble commun d'exigences à remplir par les organes délivrant des moyens d'identification électroniques et par les prestataires de services de confiance. En dépit de son soutien général pour la proposition, le CEPD souhaite formuler les recommandations générales suivantes:

- les dispositions en matière de protection des données contenues dans la proposition ne devraient pas être limitées aux prestataires de services de confiance, mais devraient aussi être applicables au traitement de données à caractère personnel dans les systèmes d'identification électronique décrits au chapitre II de la proposition;
- le règlement proposé devrait fixer un ensemble commun d'exigences de sécurité concernant les prestataires de services de confiance et les entités délivrant des identifications électroniques. Autre possibilité, il pourrait autoriser la Commission à définir, selon que de besoin, à travers une utilisation sélective d'actes délégués ou de mesures d'exécution, les critères, conditions et exigences pour la sécurité dans les services de confiance électroniques et les systèmes d'identification électronique;
- les prestataires de services de confiance électroniques et les entités délivrant des identifications électroniques devraient être tenus de fournir aux utilisateurs de leurs services: i) des informations appropriées sur la collecte, la communication et le stockage de leurs données ainsi que ii) les moyens de contrôler leurs données à caractère personnel et d'exercer leurs droits à la protection des données;

- le CEPD recommande une inclusion plus sélective dans la proposition des dispositions habilitant la Commission à spécifier ou à détailler des dispositions concrètes après l'adoption du règlement proposé par des actes délégués ou d'exécution.

51. Certaines dispositions spécifiques concernant la reconnaissance mutuelle des systèmes d'identification électronique devraient aussi être améliorées:

- le règlement devrait identifier les données ou les catégories de données qui seront traitées pour procéder à l'identification transnationale de personnes physiques. Cette spécification devrait avoir au minimum le même niveau de détail que celui des annexes sur les autres services de confiance et devrait prendre en considération le respect du principe de proportionnalité;
- les garanties requises pour la fourniture de systèmes d'identification devraient au minimum se conformer avec les exigences formulées à l'égard des prestataires de services de confiance qualifiés;
- la proposition devrait établir des mécanismes appropriés visant à créer un cadre pour l'interopérabilité des systèmes d'identification nationaux.

52. Enfin, le CEPD formule aussi les recommandations suivantes en ce qui concerne les exigences relatives à la fourniture et à la reconnaissance de services de confiance électroniques:

- il devrait être spécifié, pour tous les services électroniques, si des données à caractère personnel seront traitées et, dans les cas où des données à caractère personnel seront effectivement traitées, les données ou catégories de données à traiter;
- le règlement devrait prévoir des garanties appropriées pour éviter tout chevauchement entre les compétences des organes de contrôle des services de confiance électroniques et celles des autorités chargées de la protection des données;
- les obligations imposées aux prestataires de services de confiance électroniques concernant les violations de données et les incidents de sécurité doivent concorder avec les exigences établies dans la directive révisée «Vie privée» et dans le règlement proposé sur la protection des données;
- il faudrait apporter davantage de clarté à la définition des entités privées ou publiques autorisées à agir en tant que tiers habilités à effectuer les audits visés aux articles 16 et 17 ou à vérifier des dispositifs de création de signature électronique au titre de l'article 23, ainsi qu'aux critères en vertu desquels l'indépendance de ces organismes sera évaluée;
- le règlement devrait être plus précis lorsqu'il fixe un délai pour la conservation des données visées à l'article 19, paragraphes 2 et 4 <sup>(1)</sup>.

Fait à Bruxelles, le 27 septembre 2012.

Giovanni BUTTARELLI

*Contrôleur adjoint européen de la protection des données*

---

<sup>(1)</sup> En vertu de l'article 19, paragraphe 2, sous g), les prestataires de services de confiance qualifiés enregistrent pour une durée appropriée toutes les informations pertinentes concernant les données publiées et reçues par eux. En vertu de l'article 19, paragraphe 4, les prestataires de services de confiance qualifiés fournissent à toute partie utilisatrice des informations sur la validité ou la révocation des certificats qualifiés qu'ils ont délivrés.