LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

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 CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1],

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et notamment son article 28, paragraphe 2[2],

A ADOPTÉ LE PRÉSENT AVIS:

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»)[3].

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[4] visant à améliorer la législation relative aux signatures électroniques

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L8, 12.1.2001, p. 1.
[3] COM (2012) 238 final.
[4] COM (2010) 245 du 19.5.2010.

Adresse postale: rue Wiertz 60 – B-1047 Bruxelles
Bureaux: rue Montoyer 63
Courrier électronique: edps@edps.europa.eu – Site web: www.edps.europa.eu
Tél.: 02-283 19 00 – Fax : 02-283 19 50

(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 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.

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 web 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.

II. ANALYSE DE LA PROPOSITION

II.1. Comment la proposition aborde la protection des données

Applicabilité de la législation en matière de protection des données aux systèmes d'identification électronique et aux services de confiance électroniques

13. Pour commencer, le CEPD souligne que les services de confiance électroniques et les systèmes d'identification électronique fournis, au nom ou sous la responsabilité d'États membres, par des prestataires de services de confiance doivent remplir des conditions spécifiques. L'absence de garanties appropriées pourrait mener à des risques significatifs en ce qui concerne la protection des données. Par exemple, il pourrait y avoir un risque de vol d'identité ou d'abus de moyens électroniques, entraînant un grave préjudice pour les personnes concernées.

14. Compte tenu des risques associés à la fourniture de chacun de ces services, il convient de mettre en place des garanties appropriées. Qui plus est, s'il est question d'utiliser ces services dans le cadre de transactions transfrontalières, il y aurait des avantages évidents à poursuivre l'harmonisation de ces garanties au niveau de l'UE. Le CEPD se félicite de voir figurer le considérant 24 qui précise qu'un prestataire de service de confiance est un responsable du traitement de données personnelles et qu'il doit donc satisfaire aux obligations énoncées dans la directive 95/46/CE. Le CEPD se réjouit aussi du fait que l'article 11 fixe des exigences spécifiques en matière de protection des données et de limitation des données qui sont conformes à la directive 95/46/CE.

15. En revanche, le CEPD note que tant le considérant 24 que l'article 11 ne portent que sur les prestataires de services de confiance et ne semblent pas inclure le traitement de données à caractère personnel dans les systèmes d'identification électronique décrits au chapitre II de la proposition. L'exposé des motifs[5] affirme que de telles exigences ne peuvent être imposées aux systèmes d'identification étant donné qu'ils sont une prérogative nationale.

16. Par ailleurs, l'exposé des motifs[6] précise aussi que la coordination requise pour lever les obstacles existants (absence de sécurité juridique et difficultés en matière d'interopérabilité) peut être assurée avec davantage d'efficacité au niveau de l'UE.

17. Aux yeux du CEPD, du point de vue de la protection des données, il ne serait pas incompatible, ni avec la législation de l'UE, ni avec le principe de subsidiarité, de fixer dans un règlement européen un ensemble d'exigences minimales visant à garantir l'interopérabilité des systèmes ainsi qu'un niveau harmonisé de protection des données tout en laissant une marge de manœuvre aux États membres en ce qui concerne la façon dont ils mettront en œuvre ces exigences au niveau national.

[5] Page 4, lorsqu'il est fait référence au critère de nécessité.
[6] Page 4, lorsqu'il est fait référence au critère de nécessité.

18. Étant donné que les conséquences négatives de toute erreur de traitement commise dans le cadre de systèmes d'identification seraient plus graves qu'avec tout autre service de confiance, notamment eu égard au niveau de confiance et de fiabilité que ceux-ci sont censés garantir dans des contextes transnationaux, l'introduction d'un ensemble cohérent d'exigences au niveau de l'UE pour les services d'identification électronique apparaît justifiée.

Dispositions en matière de sécurité

19. Le CEPD salue le fait que la proposition prévoit, aux articles 15 et 16, des exigences de sécurité applicables aux prestataires de services de confiance ainsi que le contrôle de ces exigences par des organes compétents. Néanmoins, le CEPD remarque qu'il subsiste un certain risque de divergence dans la mise en œuvre de ces exigences puisque chaque prestataire de services de confiance dispose d'une marge de manœuvre en ce qui concerne l'adoption, selon ses propres critères, des mesures techniques et organisationnelles qu'il estime adaptées au degré de risque, compte tenu de l'état de la technique.

20. Dans ce contexte, le CEPD considère que le règlement proposé devrait instaurer un ensemble minimal d'exigences, en particulier concernant les circonstances, les formats et les procédures associés à la sécurité, ainsi que les critères, les conditions et les exigences, y compris la détermination de ce qui constitue l'état de la technique en termes de sécurité pour les services de confiance électroniques. Les articles 15, paragraphe 6, et 16, paragraphe 6, de la proposition prévoient que ces exigences minimales puissent être définies plus avant par la Commission à un stade ultérieur par des actes législatifs délégués. En revanche, le CEPD souligne que le législateur doit évaluer avec soins, au moyen d'une approche sélective, les domaines dans lesquels ces exigences minimales pourraient être établies au moyen d'actes délégués plutôt que d'être spécifiés dans le règlement proposé.

Aspects supplémentaires de la protection des données à prendre en considération

21. Le CEPD est d'avis qu'à côté des éléments visés à l'article 11 sur la protection des données, d'autres aspects devraient être pris en considération. Plus particulièrement, les responsables du traitement des données (les prestataires de services de confiance comme les systèmes d'identification électronique) 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. La nécessité de la transparence et de la clarté des informations est liée à la validité du consentement obtenu. Du point de vue de la protection des données, le consentement est une condition préalable au traitement des données à caractère personnel et n'est valide que lorsqu'il est basé sur le libre choix et des informations adéquates[7]. Le CEPD conseille d'inclure dans la proposition des

[7] Voir l'avis 15/2011 du groupe de travail «article 29» sur la définition du consentement, consultable sur: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_fr.pdf.

références spécifiques aux droits des personnes concernées et notamment au droit d'accès et au droit d'être informé.

22. L'article 11 de la proposition dispose que la législation en vigueur dans les États membres et autorisant l'utilisation de pseudonymes ne sera pas préjudiciée par le règlement. Comme le clarifie le considérant 27, les pseudonymes seront attribués de telle manière que la personne concernée pourra toujours être identifiée conformément au droit de l'Union ou au droit national. Par conséquent, les données traitées seront considérées comme des données à caractère personnel[8] même si des pseudonymes sont utilisés. Afin d'éviter tout malentendu, ce point devrait être indiqué dans le règlement proposé (de préférence à l'article 11, paragraphe 4, ou dans un considérant).

23. Enfin, le CEPD estime que les technologies renforçant la protection de la vie privée (*Privacy Enhancing Technologies,* PET) pourraient contribuer à trouver le juste équilibre entre la concrétisation des objectifs du règlement proposé et le respect des droits des personnes en matière de protection des données. Le CEPD recommande que le règlement proposé dresse le bilan de l'importance des PET en tant qu'éléments permettant de créer la confiance en exigeant des prestataires de services de confiance et des prestataires de services d'identification qu'ils prennent en considération les PET lorsqu'ils définissent un système de services électroniques. Cette approche se situera dans le prolongement de l'approche de la «protection des données dès leur conception» prévue dans la récente proposition de la Commission sur le réexamen du cadre de protection des données[9].

Utilisation d'actes délégués et de mesures d'exécution

24. Dans de nombreuses dispositions du règlement proposé, la Commission est habilitée à adopter des actes délégués ou des mesures d'exécution. Bien que de tels actes et de telles mesures puissent contribuer à l'application uniforme du règlement et permettre la poursuite de l'alignement des pratiques nationales grâce à l'expérience acquise après l'entrée en vigueur du règlement, le CEPD émet des réserves quant à une approche qui s'appuie si lourdement sur eux. Comme le précise le point 20 ci-dessus, le CEPD considère que les domaines dans lesquels cette législation déléguée serait utile doit faire l'objet d'une évaluation minutieuse, sur la base d'une approche plus sélective. Le CEPD souligne le risque que ces actes et ces mesures ne soient pas encore adoptés lorsque le règlement sera applicable, ce qui pourrait porter préjudice à l'application cohérente du règlement, notamment dans une perspective de protection des données. Cela pourrait être le cas, par exemple, des mesures de sécurité à respecter immédiatement par les services de confiance ou des exigences relatives aux services de création de signatures électroniques.

[8] Telles que définies à l'article 2, point a, de la directive 95/46/CE.

[9] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11 final (article 23).

II.2. Aspects de la protection des données des systèmes d'identification électronique qui doivent être reconnus et acceptés par-delà les frontières

25. La proposition laisse aux États membres une très grande marge de manœuvre (voir en particulier les considérants 11 et 12) concernant la création, la définition et l'introduction des moyens aux fins de l'identification électronique et des systèmes d'identification électronique. Le CEPD comprend qu'il peut être nécessaire d'adapter les différentes exigences dans les différents États membres et il est aussi conscient du fait que les systèmes d'identification électronique sont déjà déployés dans plusieurs États membres. Le CEPD préconise toutefois une approche qui respecte les exigences différentes dans chaque État membre, et qui fixe, parallèlement, un ensemble commun de conditions applicables à l'utilisation de systèmes d'identification nationaux par-delà les frontières.

Catégories de données traitées

26. Le traitement de données à caractère personnel est inhérent aux systèmes d'identification électronique des personnes physiques. Il est donc clair que les entités qui créent, vérifient, valident, traitent et conservent des données traiteront des données à caractère personnel. En revanche, le règlement ne détermine pas les données ou les catégories de données qui seront traitées.

27. Le CEPD estime que le règlement devrait identifier les données ou les catégories de données qui seront traitées pour procéder à l'identification transnationale de personnes physiques, avec au minimum le même niveau de détail que dans les annexes sur les autres services de confiance.

28. En outre, la limitation des données est critique y compris dans le cas du traitement transnational. Le règlement devrait donc fixer des objectifs spécifiques à cet égard:

- Limitation de la quantité de catégories de données incluses dans le système d'identification électronique. Il convient notamment d'accorder une attention particulière aux données biométriques.

- Divulgation sélective et partielle des données relatives à l'identité, selon la finalité pour laquelle est utilisée l'identité électronique (par exemple, une personne concernée qui ne doit donner la preuve que de son âge ou de la localité précise dans laquelle elle réside ne doit pas être obligée de divulguer des données supplémentaires).

Conditions pour la reconnaissance mutuelle

29. Le CEPD salue le cadre destiné à créer la reconnaissance mutuelle tel que défini à l'article 6. Par ailleurs, il considère que les exigences proposées sont fixées à un niveau très général et qu'elle ne fournissent donc pas encore un cadre solide et harmonisé pour la reconnaissance et l'acceptation mutuelles de l'identification électronique.

30. Selon la proposition, les exigences principales auxquelles doit répondre un système d'identification pour être reconnu et accepté au niveau européen sont les suivantes: (i) un État membre doit notifier le système à la Commission européenne, (ii) un tel système doit être accepté dans la juridiction du pays procédant à la notification et (iii) le moyen d'identification doit être délivré par l'État membre notifiant le système, en son nom ou, au moins, sous sa responsabilité. En revanche, le texte ne formule aucune exigence spécifique concernant les autorités publiques compétentes ou les entités privées délivrant un moyen d'identification au nom d'un État membre. Par exemple, selon le règlement proposé, les entités délivrant des moyens d'identification ne seront pas soumises aux mécanismes de contrôle visés aux articles 13 et 14, ou ne devront pas se conformer aux exigences de sécurité, de contrôle et d'organisation visées aux articles 15, 16, 17 et 19. Cette approche peut engendrer l'hétérogénéité et conduire à des niveaux différents de garanties en matière de protection des données, en fonction du système d'identification utilisé.

31. Les garanties à mettre en œuvre par un prestataire doivent être proportionnées aux risques potentiels du service fourni. En outre, la reconnaissance mutuelle ne peut fonctionner qu'à condition d'être basée sur un niveau minimal commun de protection. Par conséquent, puisque les risques associés à la délivrance de moyens d'identification électronique sont élevés, les garanties requises doivent au moins se conformer aux exigences prévues pour les prestataires de services de confiance qualifiés[10] aux articles 15, 16 et 17. Aux yeux du CEPD, une autorité compétente délivrant des moyens d'identification électronique pour interagir avec des services d'administration en ligne doit être soumise à des contrôles de sécurité plus stricts qu'un prestataire de services de confiance délivrant des certificats aux clients d'un supermarché pour qu'ils puissent procéder à des achats en ligne.

32. Par conséquent, le CEPD recommande que l'article 6, tout en reconnaissant que la délivrance de moyens d'identification est une prérogative nationale, fasse aussi le point sur le fait que les systèmes nationaux, qui doivent être notifiés en vue d'une acceptation et d'une reconnaissance transnationales, offrent des garanties d'un niveau au minimum équivalent à celles requises pour les services de confiance qualifiés. Sur le plan pratique, cela signifierait qu'à côté des conditions déjà prévues à l'article 6, les prestataires proposant de tels moyens d'identification devraient être soumis au moins aux mêmes conditions que celles requises des prestataires de services de confiance électroniques qualifiés en termes de contrôle (articles 13, 14 et 16) ainsi que de sécurité, de technologie et d'organisation (articles 15, 17 et 19).

[10] Notez que les risques associés au traitement de données à caractère personnel dans un système d'identification électronique peuvent être plus élevés que dans le cas d'autres services de confiance électroniques (par exemple, ils peuvent mener au vol d'identité, affecter la sécurité nationale et, dans de nombreux cas, avoir des conséquences négatives considérables pour les personnes qui en sont les victimes).

Interopérabilité

33. Les considérants 7, 15, 16 et 49 de la proposition soulignent l'importance de l'interopérabilité des services de confiance et des systèmes d'identification électroniques afin d'augmenter leur adoption et leur utilité. En revanche, le règlement proposé ne contient pas de dispositions spécifiques détaillant les mécanismes censés garantir l'interopérabilité au niveau européen[11]. Il serait souhaitable d'avoir davantage de clarté dans la mesure où l'article 6 se limite à faire une brève référence à la nécessité de créer un mécanisme de coordination pour l'échange de bonnes pratiques et d'expériences.

34. La création d'un cadre pour l'interopérabilité des systèmes d'identification et des services de confiance électroniques nationaux vise notamment à améliorer l'efficacité du règlement. Par conséquent, le CEPD recommande que le règlement harmonise au moins les aspects qui sont cruciaux pour l'interopérabilité comme les champs de données qui seront utilisés pour l'identification des personnes physiques, les exigences de sécurité et les garanties en matière de protection des données.

II.3. Aspects de la protection des données des services de confiance électroniques qui doivent être reconnus et acceptés par-delà les frontières

35. Le CEPD salue les améliorations envisagées par rapport à la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques[12] concernant l'harmonisation des conditions applicables à la fourniture de services de confiance. Cette nouvelle approche assurera une meilleure sécurité juridique aux prestataires opérant au niveau européen ainsi qu'aux utilisateurs et aux tiers qui ont besoin de services de confiance. Elle contribuera aussi à lever les obstacles au fonctionnement du marché intérieur provenant d'interprétations nationales divergentes de la directive 1999/93/CE et des applications hétérogènes de solutions techniques.

36. En dépit de ce soutien d'ordre général, le CEPD souhaite s'arrêter sur plusieurs aspects concernant lesquels la proposition devrait apporter davantage de clarté.

Catégories de données traitées

37. Le CEPD se réjouit que des annexes spécifiques aient été présentées pour les différents services électroniques qui seront fournis, et que ces annexes incluent des détails spécifiques sur les catégories de données qui seront traitées. En revanche, le CEPD note que, dans certains cas, les catégories de données à caractère personnel devant être traitées ne sont pas clairement identifiées. Par exemple, en ce qui concerne les certificats qualifiés relatifs aux signatures électroniques, l'annexe I exige *un ensemble de données représentant le signataire sans ambiguïté* dans les certificats qualifiés. Ce point peut varier dans une large mesure pour les signatures électroniques: par exemple, il n'est pas

[11] Par exemple, le portail des autorités européennes de validation afin d'assurer l'interopérabilité transnationale des signatures électroniques et d'accroître la sécurité des transactions réalisées au moyen de l'internet.
[12] JO L 13, 19.1.2000, p. 12.

possible de savoir si un nom et une adresse, un numéro personnel d'identification ou des données biométriques pourraient être utilisés pour «représenter sans ambiguïté» un signataire.

38. Du point de vue de la protection des données, il est crucial de comprendre quelles données à caractère personnel sont traitées et dans quelles circonstances afin d'évaluer les implications en matière de protection des données et de prévoir des garanties adéquates. Par conséquent, le CEPD recommande que le règlement spécifie, pour tous les services électroniques, si des données à caractère personnel seront traitées et, lorsque c'est le cas, les données ou catégories de données qu'il conviendrait, au minimum, d'inclure. Bien entendu, il pourrait être possible de laisser une marge de manœuvre au prestataire de services de confiance pour qu'il soit en mesure d'inclure des données supplémentaires dans l'hypothèse où cette inclusion serait nécessaire pour fournir le service. Cette approche serait conforme au principe de limitation des données (visé à l'article 11) et faciliterait également l'intégration et l'interopérabilité de différents services de confiance.

Reconnaissance mutuelle au niveau international

39. L'article 10 de la proposition dispose que des accords internationaux peuvent être conclus conformément à l'article 218 TFUE[13], ce qui permettrait la reconnaissance de services de confiance qualifiés et de certificats qualifiés fournis par des prestataires dans des pays tiers au même titre que ceux fournis par des prestataires de services établis dans l'UE.

40. Aux termes de ce type d'accords, les prestataires de pays tiers seront des concurrents à part entière des prestataires de l'UE puisqu'ils proposeront aussi leurs services à des clients établis dans l'UE. Le CEPD se réjouit du fait que des services de confiance qualifiés fournis par des prestataires de services de confiance dans des pays tiers ou dans des organisations internationales soient soumis aux mêmes exigences que ceux fournis par des prestataires de services de confiance européens. Il salue aussi la mention explicite de la protection des données à caractère personnel, de la sécurité et du contrôle.

Contrôle

41. Le CEPD relève que les tâches des organes de contrôle visées aux articles 13 et 14 de la proposition pourraient entraîner un chevauchement avec les tâches des autorités indépendantes chargées de la protection des données[14]. Le contrôle indépendant est un élément essentiel des règles européennes en matière de protection des données. Ce constat découle de l'article 8 de la Charte et de l'article 16 TFUE, et a été explicité par la Cour de justice dans l'arrêt Commission/Allemagne rendu en mars 2010[15]. Par voie de conséquence, les

[13] L'article 218 fixe la procédure pour l'adoption d'accords internationaux et l'implication des parties principales, notamment le Conseil et le Parlement européen.

[14] Par exemple, selon l'article 15, paragraphe 4, les organes de contrôle compétents définis ont le pouvoir de donner des instructions contraignantes aux prestataires de services de confiance concernant les mesures de sécurité.

[15] CJUE, le 9 mars 2010, Commission/Allemagne, C-518/07, [2010] ECR I-1885, paragraphes 23 et 50.

compétences spécifiques des autorités indépendantes chargées de la protection des données ne doivent pas être attribuées à d'autres autorités de contrôle qui n'ont pas le même statut et ne bénéficient pas d'une reconnaissance au même niveau dans la législation européenne. Un chevauchement des compétences peut aussi porter atteinte à l'unité d'action requise en matière de contrôle.

42. Le CEPD recommande donc que la proposition détaille plus avant la définition du rôle et des compétences des organes de contrôle en vue d'éviter un chevauchement avec les compétences des autorités chargées de la protection des données. Un mécanisme de coopération pourrait être mis en place pour garantir la cohérence des approches adoptées à la fois par les organes de contrôle des services de confiance et les autorités chargées de la protection des données.

43. Enfin, aux termes de l'article 17, paragraphe 1, un prestataire de services de confiance qualifiés peut commencer à offrir un service de confiance qualifié immédiatement après avoir soumis une notification et un audit de sécurité à l'organe de contrôle, mais sans devoir attendre la vérification de l'organe de contrôle. Dans cette situation, selon l'article 17, paragraphe 3, l'organe de contrôle vérifie la conformité du prestataire de service de confiance qualifié et des services de confiance qualifiés avec les exigences du règlement dans un délai d'un mois[16]. Le CEPD indique que dans le cas où l'organe de contrôle rend une évaluation négative du prestataire de services de confiance ou du service de confiance fourni, une telle évaluation est susceptible de créer une incertitude juridique en ce qui concerne les moyens électroniques déjà délivrés par le prestataire de services de confiance qualifiés ainsi qu'avec les transactions ou les documents dans le cadre desquels ces moyens ont été utilisés. Par conséquent, le CEPD recommande qu'une vérification positive *ex-ante* des organes de contrôle soit requise pour pouvoir débuter la fourniture du service.

Violations de données

44. Le CEPD note avec satisfaction que des dispositions relatives aux violations de données ont été incluses dans le règlement proposé, eu égard aux conséquences négatives importantes que les violations de données peuvent avoir pour les personnes concernées. Les conséquences négatives de la violation de données ne doivent pas être simplement évaluées en prenant uniquement en considération les données à caractère personnel gérées par le prestataire de services de confiance. Il convient aussi d'examiner si les données compromises sont susceptibles d'être utilisées par des tiers pour se faire passer numériquement pour des personnes physiques ou des entités juridiques et multiplier ainsi les conséquences négatives pour les personnes physiques. Une violation de données à caractère personnel peut entraîner, à défaut d'être traitée à temps et de manière adéquate, une perte économique et un tort social substantiels pour les personnes concernées, y compris le vol d'identité.

[16] L'article 17, paragraphe 3, autorise l'organe de contrôle à dépasser le délai prévu pour la vérification, auquel cas il informe le prestataire de services de confiance qualifiés en précisant les raisons du retard et le délai nécessaire pour terminer la vérification.

45. Le CEPD relève que le règlement proposé ne prévoit pas de définition des notions d'«atteinte à la sécurité» et de «perte d'intégrité» et que la notion d'«incidence importante» ne fait l'objet d'aucun éclaircissement. La notion de violation de données devrait donc être définie avec davantage de précision dans le règlement proposé et en particulier dans l'article 3. Il serait possible d'utiliser les mêmes termes que ceux repris dans les définitions figurant à l'article 2, point i, de la directive révisée «Vie privée»[17], ou aux articles 31 et 32 du nouveau règlement proposé en matière de protection des données.

46. Plus particulièrement, la définition devrait être cohérente avec les obligations imposées aux responsables du traitement qui sont tenus de notifier aux autorités de contrôle nationales compétentes les violations de données à caractère personnel, et de notifier les personnes physiques dans l'hypothèse où la violation de données est susceptible d'avoir sur elles des répercussions négatives. Dans ce contexte, le CEPD recommande l'inclusion de dispositions spécifiques pour garantir l'alignement des procédures de notification. Par exemple, un mécanisme de coopération pourrait être envisagé entre l'organe de contrôle prévu dans la proposition et d'autres autorités de contrôle nationales qui doivent être prévenues de ces violations de données, telles que les autorités chargées de la protection des données[18].

Audit et certification par des tiers

47. Le CEPD note que, conformément aux articles 16 et 17, l'exécution d'audits par des tiers joue un rôle important pour assurer la conformité des prestataires de services de confiance avec les exigences incluses dans le règlement proposé. Le CEPD se réjouit de cette approche, mais demande davantage de clarté concernant la définition des tiers habilités à effectuer de tels audits et concernant tant la méthodologie que la portée de ces audits. Par exemple, le CEPD recommande qu'au lieu de désigner ces auditeurs tiers comme étant des «organes indépendants reconnus responsables»[19], la proposition devrait exiger que ces tiers soient reconnus seulement après que des organes indépendants ont vérifié leur indépendance sur la base de critères spécifiques et ont approuvé la méthodologie et la portée des audits à effectuer.

48. La même considération s'applique aux «organismes publics ou privés compétents désignés par les États membres» chargés de vérifier les dispositifs de création de signature électronique (article 23). Le CEPD recommande que les organes de contrôle aient pour mission de désigner ces organismes. Par ailleurs, l'article 23 mentionne que ces organismes de certification effectueront des évaluations sur la base d'une liste de normes qui sera établie par la Commission au moyen d'actes d'exécution. Le CEPD recommande que le règlement proposé

[17] Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

[18] Comme le prévoit le paquet de réforme de la protection des données proposé par la Commission le 25 janvier 2012.

[19] Voir le considérant 49 et les articles 16 et 17 de la proposition.

fixe un délai relatif à l'adoption de ces actes d'exécution, faute de quoi il sera impossible de certifier des dispositifs de création de signature électronique qualifiée et, par conséquent, impossible de créer des signatures électroniques qualifiées.

Enregistrement et divulgation de données par des prestataires de services de confiance

49. La proposition indique des exigences spécifiques concernant l'enregistrement des informations qui suscitent certaines inquiétudes du point de vue de la protection des données:

- En vertu de l'article 19, paragraphe 2, point g, les prestataires de services de confiance qualifiés doivent enregistrer pour une période appropriée toutes les informations pertinentes concernant les données publiées et reçues. Le CEPD note que le règlement devrait être plus précis et fixer un délai pour la conservation de ces informations, par exemple en le limitant à la durée pendant laquelle les informations pourraient être demandées aux fins d'une procédure judiciaires. L'article 19, paragraphe 2, devrait aussi décrire clairement le type d'informations qui doit être enregistré, plutôt que d'exiger l'enregistrement de toutes les informations pertinentes.

- En vertu de l'article 19, paragraphe 4, les prestataires de services de confiance qualifiés fournissent à toute partie utilisant les certificats des informations sur la validité ou la révocation des certificats qualifiés qu'ils ont délivrés. Cette exigence est très ouverte et n'impose aucune restriction concernant la durée pendant laquelle ces informations devraient être stockées. Le CEPD recommande que ces informations ne soient mises à disposition que jusqu'à la date d'expiration du certificat.

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 identités 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[20].

Fait à Bruxelles, le 27 septembre 2012

(**signé**)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données

[20] 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.