Parlement européen
2019-2024

Commission des libertés civiles, de la justice et des affaires intérieures

2021/0136(COD)

18.5.2022

PROJET D'AVIS

de la commission des libertés civiles, de la justice et des affaires intérieures

à l'intention de la commission de l'industrie, de la recherche et de l'énergie

sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique
(COM(2021)0281 – C9-0200/2021 – 2021/0136(COD))

Rapporteur pour avis: Cristian Terheş

PA_Legam

JUSTIFICATION SUCCINCTE

Ce projet d'avis soulève plusieurs préoccupations concernant la proposition de la Commission, notamment en ce qui concerne les aspects relatifs à la protection des données et à la vie privée, qui relèvent de la compétence de la commission des libertés civiles, de la justice et des affaires intérieures (LIBE). Certaines de ces préoccupations ont déjà été partagées par le Contrôleur européen de la protection des données, ainsi que par les parties prenantes consultées lors de l'élaboration du projet d'avis. Le rapporteur pour avis tient à les souligner, sur la base des contributions écrites reçues de différents experts en la matière.

La proposition actuelle est de nature très technique et concerne des aspects essentiels des droits fondamentaux, tels que la protection des données et la vie privée. Si le Parlement ne parvient pas à élaborer un cadre cohérent et une législation techniquement éprouvée, les citoyens perdront tout contrôle sur leurs données privées, qui deviendront une marchandise. Malheureusement, les options techniques pour la mise en œuvre de la proposition doivent être adoptées par la Commission au moyen d'actes non législatifs ultérieurs. Il s'agit d'une approche dangereuse, car une option technique pourrait être plus intrusive qu'une autre, au détriment des droits fondamentaux des citoyens.

Des préoccupations plus spécifiques pourraient être exprimées en ce qui concerne le manque de clarté de la relation entre eIDAS et RGPD; le respect des éléments essentiels de la protection des données, tels que la minimisation des données et la divulgation sélective; le respect de la vie privée dès la conception et l'utilisation d'identifiants uniques; le manque d'ouverture et de transparence dans l'élaboration des spécifications de sécurité du portefeuille eIDAS et la participation de la société civile ou des universités; la dépendance à l'égard des grandes entreprises technologiques; l'affaiblissement de la sécurité du navigateur.

Par les amendements proposés, le rapporteur pour avis de la commission LIBE vise à corriger les problèmes susmentionnés, qui relèvent de la compétence de la commission LIBE. Afin de protéger la vie privée des personnes et de ne pas décourager les utilisateurs du portefeuille européen d'identité numérique, le rapporteur pour avis tient compte du fait que l'utilisation de pseudonymes doit être une possibilité dans tous les cas où l'identification complète n'est pas imposée par la loi. En outre, les références à la relation entre l'eIDAS et la législation européenne en matière de protection des données remontant au niveau de protection existant de 2014 sont réintroduites.

La nécessité de l'absence de lien et de traçabilité a été largement reconnue par les experts en la matière. Les transactions des utilisateurs révèlent de grandes quantités de données, y compris des données à caractère hautement personnel, telles que des informations sur la situation économique ou des informations sur la situation médicale, l'historique des déplacements, les modes de consommation et les interactions sociales des citoyens. Par conséquent, l'architecture envisagée devrait protéger d'une surveillance centralisée ces données relatives à un large éventail de comportements des utilisateurs en ligne et hors ligne.

Dernier point, mais non des moindres, un identifiant univoque et constant pour les personnes physiques serait illégal dans certains États membres, voire inconstitutionnel (par exemple, en Allemagne, l'utilisation d'identifiants univoques constants est interdite en vertu de l'arrêt sur la loi de recensement de 1983). Le risque d'un identifiant univoque tout au long de la vie ne peut être considéré comme la méthode la moins intrusive aux fins de l'identification univoque

d'une personne. L'article 11 bis n'est pas non plus nécessaire, étant donné que le cadre d'interopérabilité existant des systèmes d'identification conformément à l'article 12, paragraphe 4, point d), initial implique déjà une représentation univoque d'une personne pour les affaires transfrontalières et il est donc proposé de le supprimer.

Néanmoins, la proposition présente de nombreuses lacunes qui ne relèvent pas de la compétence de la commission LIBE, raison pour laquelle, afin de protéger les droits fondamentaux des Européens, l'ensemble de la proposition devrait être renvoyé à la Commission en vue d'être entièrement repensée. De la façon dont elle est envisagée, cette proposition conduirait à reproduire en Europe le modèle chinois, en permettant la création d'un système de crédit social similaire qui déterminerait la surveillance et le contrôle de masse de tous les Européens, ce qui est inacceptable. L'UE a été conçue comme un «espace de liberté» et nous devons poursuivre nos efforts pour qu'elle le demeure.

AMENDEMENTS

La commission des libertés civiles, de la justice et des affaires intérieures invite la commission de l'industrie, de la recherche et de l'énergie, compétente au fond, à prendre en considération les amendements suivants:

Amendement 1

Proposition de règlement
Considérant 6

Texte proposé par la Commission	*Amendement*
(6) Le règlement (UE) 2016/679[19] s'applique aux traitements de données à caractère personnel effectués en application du présent règlement. Par conséquent, le présent règlement devrait prévoir des garanties spécifiques pour empêcher les fournisseurs de moyens d'identification électronique et d'attestations électroniques d'attributs de combiner des données à caractère personnel provenant d'autres services avec des données à caractère personnel liées aux services relevant du champ d'application du présent règlement.	(6) ***La personne faisant l'objet de l'identité numérique est la personne physique ou morale à laquelle appartiennent les données d'identification personnelle.*** Le règlement (UE) 2016/679[19] s'applique aux traitements de données à caractère personnel effectués en application du présent règlement. Par conséquent, le présent règlement devrait prévoir des garanties spécifiques pour empêcher les fournisseurs de moyens d'identification électronique et d'attestations électroniques d'attributs de combiner des données à caractère personnel provenant d'autres services avec des données à caractère personnel liées aux services relevant du champ d'application du présent règlement.
[19] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016	[19] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

Or. en

Amendement 2

Proposition de règlement
Considérant 11

Texte proposé par la Commission	*Amendement*
(11) Les portefeuilles européens d'identité numérique devraient garantir le niveau de sécurité le plus élevé possible pour les données à caractère personnel utilisées pour l'authentification, que ces données soient stockées localement ou à l'aide de solutions en nuage, en tenant compte des différents niveaux de risque. Le recours à l'authentification biométrique ***est l'une des méthodes d'identification offrant un niveau*** de ***confiance élevé, en particulier lorsqu'elle est utilisée en combinaison avec d'autres éléments d'authentification***. Étant donné que les données biométriques représentent une caractéristique univoque d'une personne, leur utilisation exige des mesures organisationnelles et de sécurité proportionnées au risque que le traitement de ces données peut entraîner pour les droits et libertés des personnes physiques et conformément au règlement (UE) 2016/679.	(11) Les portefeuilles européens d'identité numérique devraient garantir le niveau de sécurité le plus élevé possible pour les données à caractère personnel utilisées pour l'authentification, que ces données soient stockées localement ou à l'aide de solutions en nuage, en tenant compte des différents niveaux de risque. Le recours à l'authentification biométrique ***ne devrait pas être une condition préalable à l'utilisation du portefeuille européen d'identité numérique, nonobstant l'exigence d'une authentification forte de l'utilisateur. Les données biométriques aux fins*** de ***l'identification univoque d'une personne physique dans le cadre du présent règlement ne devraient pas être stockées dans le nuage***. Étant donné que les données biométriques représentent une caractéristique univoque d'une personne, leur utilisation exige des mesures organisationnelles et de sécurité proportionnées au risque que le traitement de ces données peut entraîner pour les droits et libertés des personnes physiques et conformément au règlement (UE) 2016/679.

Or. en

Justification

Afin de garantir que les utilisateurs aient le contrôle de leurs données dans les portefeuilles européens d'identité numérique, le système envisagé ne devrait pas dépendre d'une infrastructure en nuage.

Amendement 3

Proposition de règlement
Considérant 29

Texte proposé par la Commission	*Amendement*
(29) Les portefeuilles européens d'identité numérique devraient permettre, sur le plan technique, la divulgation sélective des attributs aux parties utilisatrices. Cette fonctionnalité devrait devenir un élément de conception de base, renforçant ainsi la commodité du service et la protection des données à caractère personnel, notamment s'agissant de la minimisation du traitement des données à caractère personnel.	(29) Les portefeuilles européens d'identité numérique devraient permettre, sur le plan technique, la divulgation sélective des attributs aux parties utilisatrices. Cette fonctionnalité devrait devenir un élément de conception de base, renforçant ainsi la commodité du service et la protection des données à caractère personnel, notamment s'agissant de la minimisation du traitement des données à caractère personnel. ***Les mécanismes de validation du portefeuille européen d'identité numérique, les divulgations sélectives et l'authentification des utilisateurs pour accéder aux services en ligne devraient préserver la vie privée, en empêchant le suivi de l'utilisateur et en respectant le droit à l'anonymat et au pseudonymat.***

Or. en

Justification

Les fonctions essentielles du portefeuille doivent être mises en œuvre de manière à préserver la vie privée afin de limiter le potentiel de suivi automatisé de l'utilisateur dans les cas où celui-ci choisit d'annuler une demande de partage d'informations déjà lancée par une partie utilisatrice, en choisissant uniquement de divulguer de manière sélective les attributs individuels le concernant (par exemple, vérification de l'âge dans un débit d'alcool) ou en utilisant le portefeuille pour se connecter à un service sans possibilité de suivi ultérieur. Cette dernière caractéristique est proposée par Apple avec sa fonctionnalité «Sign in with Apple», que le portefeuille cherche à remplacer.

Amendement 4

Proposition de règlement
Article 1 – paragraphe 1 – point 3 – point i
Règlement (UE) n° 910/2014
Article 3 – paragraphe 1 – point 47

Texte proposé par la Commission	*Amendement*
47. "archivage électronique", un service assurant la réception, le stockage, la suppression et la transmission de données ou documents électroniques afin ***de garantir leur intégrité, l'exactitude*** de leur ***origine*** et ***leurs particularités juridiques*** pendant toute la durée de leur ***conservation***;	47. "archivage électronique", un service assurant la réception, le stockage, la suppression et la transmission de données ou documents électroniques afin ***d'apporter la preuve*** de leur ***authenticité*** et ***de leur intégrité*** pendant toute la durée de leur ***stockage***;

Or. en

Amendement 5

Proposition de règlement
Article 1 – paragraphe 1 – point 4
Règlement (UE) n° 910/2014
Article 5 – paragraphe 1

Texte proposé par la Commission	*Amendement*
Sans préjudice de l'effet juridique donné aux pseudonymes en droit national, l'utilisation de pseudonymes dans les transactions électroniques n'est pas interdite.;	Sans préjudice de l'effet juridique donné aux pseudonymes en droit national, l'utilisation de pseudonymes ***et d'identités souveraines*** dans les transactions électroniques n'est pas interdite.***»; l'utilisation de pseudonymes est toujours possible pour remplacer un identifiant univoque ou s'authentifier après de parties utilisatrices privées;*** ***Le traitement des données à caractère personnel est effectué conformément au règlement (UE) 2016/679, notamment en mettant en œuvre le principe de la protection des données dès la conception et par défaut;***

Or. en

Justification

Afin de protéger la vie privée des personnes et de ne pas décourager les utilisateurs du portefeuille européen d'identité numérique, l'utilisation de pseudonymes doit être une possibilité dans tous les cas où l'identification complète n'est pas imposée par la loi. En outre, les références à la relation entre l'eIDAS et la législation européenne en matière de protection des données remontant au niveau de protection existant de 2014 sont réintroduites. Le règlement eIDAS initial offrait un niveau de protection des données plus élevé que celui prévu par la directive 95/46/CE en imposant, à l'article 12, paragraphe 3, point c), de faciliter la mise en œuvre du principe du respect de la vie privée dès la conception.

Amendement 6

Proposition de règlement
Article 1 – paragraphe 1 – point 7
Règlement (UE) n° 910/2014
Article 6 bis – paragraphe 4 – point a – point 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(2 bis) pour que les parties utilisatrices soient identifiées de manière univoque et que leurs demandes d'informations soient limitées sur la base de l'approbation d'un État membre conformément à l'article 6 ter, paragraphe 1;

Or. en

Justification

L'interface commune devrait inclure cette garantie afin d'empêcher les parties utilisatrices non approuvées ou non identifiées de demander des informations allant au-delà de leur cas d'utilisation. Le groupe d'experts eIDAS organisé par la Commission européenne a reconnu la nécessité de «politiques de partage» qui restreignent les informations qu'une partie utilisatrice peut demander à l'utilisateur et empêchent les demandes d'informations excessives (voir le chapitre 4.6.1 et la note de bas de page 22 du document final du 17 février 2022).

Amendement 7

Proposition de règlement
Article 1 – paragraphe 1 – point 7
Règlement (UE) n° 910/2014
Article 6 bis – paragraphe 4 – point a – point 2 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(2 ter) veiller à ce que les intermédiaires entre les parties utilisatrices et les portefeuilles européens d'identité numérique n'obtiennent pas d'informations sur le contenu de la transaction;

Or. en

Justification

L'interface commune devrait garantir que les intermédiaires entre les parties utilisatrices et les utilisateurs du portefeuille européen d'identité numérique ne puissent pas avoir accès au contenu de la transaction qu'ils transmettent. Ces protections techniques sont habituelles et ne limitent pas le fonctionnement du système. L'existence de ces intermédiaires a été reconnue par le groupe d'experts eIDAS (voir le chapitre 4.8.3 du document final du 17 février 2022).

Amendement 8

Proposition de règlement
Article 1 – paragraphe 1 – point 7
Règlement (UE) n° 910/2014
Article 6 bis – paragraphe 4 – point a – point 3

Texte proposé par la Commission	*Amendement*
(3) pour la présentation aux parties utilisatrices de données d'identification personnelle, ***de l'attestation électronique*** d'attributs ou d'autres données ***telles que des justificatifs***, en mode local ne nécessitant pas d'accès à l'internet pour le portefeuille***;***	(3) pour la présentation aux parties utilisatrices de données d'identification personnelle ***telles que des justificatifs***, ***des attestations électroniques*** d'attributs ou d'autres données, en mode local ne nécessitant pas d'accès à l'internet pour le portefeuille***, et pour que l'utilisateur prenne une décision en connaissance de cause quant au partage d'informations à caractère personnel avec les parties utilisatrices. Cela inclut l'identification de la partie utilisatrice, le refus total ou partiel des demandes de renseignements des parties utilisatrices, un historique complet des transactions et des informations sur l'exercice des droits de la personne concernée.***

Or. en

Justification

Le succès du portefeuille européen d'identité numérique dépend de la prise de décisions éclairées par les citoyens sur les informations qu'ils partagent avec les parties utilisatrices. Le groupe d'experts eIDAS, qui élabore actuellement la boîte à outils, a donné des orientations similaires concernant les informations obligatoires sur la finalité du traitement par la partie utilisatrice, ainsi que sur la possibilité de refuser des demandes d'informations (voir chapitre 4.6.1 du document final du 17 février 2022).

Amendement 9

Proposition de règlement
Article 1 – paragraphe 1 – point 7
Règlement (UE) n° 910/2014
Article 6 bis – paragraphe 4 – point b

Texte proposé par la Commission	*Amendement*
(b) font en sorte que les prestataires de services de confiance d'attestations qualifiées d'attributs ne puissent pas recevoir d'informations concernant l'utilisation de ces attributs;	(b) font en sorte que les prestataires de services de confiance d'attestations qualifiées ***et non qualifiées*** d'attributs ne puissent pas recevoir d'informations concernant l'utilisation de ces attributs;

Or. en

Justification

Cet amendement étend les garanties visant à protéger le comportement des utilisateurs contre tout pistage. Des exemples de fournisseurs d'attestations d'attributs non qualifiés sont des entreprises privées, des clubs ou des universités. Avec cette modification du texte, une garantie technique existante du portefeuille européen d'identité numérique est simplement étendue à un plus grand nombre de parties prenantes.

Amendement 10

Proposition de règlement
Article 1 – paragraphe 1 – point 7
Règlement (UE) n° 910/2014
Article 6 bis – paragraphe 4 – point e

Texte proposé par la Commission	*Amendement*
(e) font en sorte que les données	(e) font en sorte que les données

d'identification personnelle visées à l'article 12, paragraphe 4, point d), ***représentent*** de manière univoque et constante la personne physique ou morale qui ***y est associée.***	d'identification personnelle visées à l'article 12, paragraphe 4, point d), ***représentant*** de manière univoque et constante la personne physique ou morale***, ne soient partagées que de manière pseudonymique, de sorte qu'elles soient différentes pour les différentes parties utilisatrices afin d'empêcher l'association ou le suivi de l'utilisateur entre les parties utilisatrices et d'empêcher l'émetteur du portefeuille européen d'identité numérique, les services tiers*** qui ***lui sont liés ou l'État membre de recevoir toute information sur l'utilisation du portefeuille européen d'identité numérique;***

Or. en

Justification

Le groupe d'experts eIDAS a reconnu la nécessité de l'absence de lien et de traçabilité (voir page 26 au chapitre 5 du document final du 17 février 2022). Les transactions des utilisateurs révèlent de grandes quantités de données, y compris des données à caractère hautement personnel, telles que des informations sur la situation économique ou des informations sur la situation médicale, l'historique des déplacements, les modes de consommation et les interactions sociales des citoyens.

Amendement 11

Proposition de règlement
Article 1 – paragraphe 1 – point 7
Règlement (UE) n° 910/2014
Article 6 bis – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. L'utilisateur exerce un contrôle total sur le portefeuille européen d'identité numérique. L'entité qui délivre le portefeuille européen d'identité numérique ***ne collecte pas*** les ***informations sur l'utilisation du portefeuille*** qui ***ne*** sont ***pas nécessaires à la fourniture des services qui y sont attachés; elle ne combine pas non plus*** des ***données d'identification personnelle et d'autres données à***	7. L'utilisateur exerce un contrôle total sur le portefeuille européen d'identité numérique ***et ses données***. ***L'architecture technique empêche*** l'entité qui délivre le portefeuille européen d'identité numérique ***ou*** les ***services tiers*** qui ***lui*** sont ***liés ou l'État membre de recueillir ou d'obtenir*** des ***informations sur l'utilisation du portefeuille par l'utilisateur. L'échange d'informations par l'intermédiaire*** du

caractère personnel stockées ou relatives à l'utilisation du portefeuille européen d'identité numérique ***avec des données à caractère personnel provenant de tout autre service offert par cette entité ou*** de ***services tiers qui ne sont pas nécessaires à*** la ***fourniture*** des ***services attachés au portefeuille, à moins que l'utilisateur n'en ait fait expressément la demande***. Les données à caractère personnel relatives à la fourniture des portefeuilles européens d'identité numérique sont maintenues séparées, de manière physique et logique, de toute autre donnée détenue. Si le portefeuille européen d'identité numérique est fourni par des parties privées conformément au paragraphe 1, points b) et c), les dispositions de l'article 45 septies, paragraphe 4, s'appliquent mutatis mutandis.

portefeuille européen d'identité numérique ***ne permet pas que d'autres parties utilisatrices ou fournisseurs d'attestation électronique d'attributs soient en mesure de suivre,*** de ***relier, de corréler ou d'acquérir d'une autre manière*** la ***connaissance*** des ***transactions ou du comportement des utilisateurs***. Les données à caractère personnel relatives à la fourniture des portefeuilles européens d'identité numérique sont maintenues séparées, de manière physique et logique, de toute autre donnée détenue. Si le portefeuille européen d'identité numérique est fourni par des parties privées conformément au paragraphe 1, points b) et c), les dispositions de l'article 45 septies, paragraphe 4, s'appliquent mutatis mutandis. ***L'entité qui délivre le portefeuille européen d'identité numérique est le responsable du traitement conformément au règlement (UE) 2016/679 concernant le traitement des données à caractère personnel dans le portefeuille européen d'identité numérique.***

Or. en

Justification

Un système d'identité électronique qui mérite la confiance des citoyens ne peut se concevoir que comme une architecture qui protège d'une surveillance centralisée les données telles que la situation médicale, l'historique des voyages, les modes de consommation et les interactions sociales des citoyens, concernant un large éventail de comportements des utilisateurs en ligne et hors ligne. L'émetteur est le responsable du traitement car il détermine les moyens de traitement des données à caractère personnel en déterminant le système concret, c'est-à-dire les moyens de traitement, que ce système soit exécuté ou non sur un dispositif placé sous son contrôle (voir C-40/17 et C-25/17).

Amendement 12

Proposition de règlement
Article 1 – paragraphe 1 – point 12
Règlement (UE) n° 910/2014
Article 11 bis

Texte proposé par la Commission	*Amendement*
(12) L'article 11 bis suivant est inséré:	***supprimé***
«Article 11 bis	
Identification univoque	
1. Lorsque des moyens d'identification électronique notifiés et les portefeuilles européens d'identité numérique sont utilisés en vue de l'authentification, les États membres garantissent une identification univoque.	
2. Aux fins du présent règlement, les États membres incluent, dans l'ensemble minimal de données d'identification personnelle mentionné à l'article 12, paragraphe 4, point d), un identifiant univoque et constant en conformité avec le droit de l'Union, afin d'identifier l'utilisateur à leur demande dans les cas où l'identification de l'utilisateur est exigée par la loi.	
3. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission précise davantage les mesures visées aux paragraphes 1 et 2 au moyen d'un acte d'exécution relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi que cela est indiqué à l'article 6 bis, paragraphe 10.»	

Or. en

Justification

Un identifiant univoque et constant pour les personnes physiques serait illégal dans certains États membres, voire inconstitutionnel (en Allemagne, l'utilisation d'identifiants univoques constants est interdite en vertu de l'arrêt sur la loi de recensement de 1983). Le risque d'un identifiant univoque tout au long de la vie ne peut être considéré comme la méthode la moins intrusive aux fins de l'identification univoque d'une personne. L'article 11 bis n'est pas non plus nécessaire, étant donné que le cadre d'interopérabilité existant des systèmes d'identification conformément à l'article 12, paragraphe 4, point d), initial implique déjà une représentation univoque d'une personne pour les affaires transfrontalières.

Amendement 13

Proposition de règlement
Article 1 – paragraphe 1 – point 13 – point b
Règlement (UE) n° 910/2014
Article 12 – paragraphe 4 – point d

Texte proposé par la Commission	*Amendement*
«d) d'une référence à un ensemble minimal de données d'identification personnelle ***nécessaires pour représenter*** de manière univoque ***et constante*** une personne physique ou morale***;»***;	«d) d'une référence à un ensemble minimal de données d'identification personnelle ***représentant*** de manière univoque une personne physique ou morale***, qui est disponible dans les schémas d'identification électronique***;

Or. en

Justification

La proposition de la Commission exigerait une identification univoque et constante, indépendante d'un système particulier d'identification électronique. Dans les faits, cette modification apparemment technique du cadre d'interopérabilité aurait le même effet que l'article 11 bis.

Amendement 14

Proposition de règlement
Article 1 – paragraphe 1 – point 22 – point b
Règlement (UE) n° 910/2014
Article 20 – paragraphe 2

Texte proposé par la Commission	*Amendement*
«Lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées, l'organe de contrôle informe les autorités de contrôle instituées en vertu du règlement (UE) 2016/679 des résultats de ses audits.»;	«Lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées, l'organe de contrôle informe les autorités de contrôle instituées en vertu du règlement (UE) 2016/679 ***et le responsable du portefeuille européen d'identité numérique*** des résultats de ses audits.»;

Or. en

Justification

Conformément aux articles 33 et 34 du RGPD, le responsable a certaines obligations en cas de violation des données. Pour s'acquitter de ces obligations, il doit être informé d'une

éventuelle violation des données dans son système.

Amendement 15

Proposition de règlement
Article 1 – paragraphe 1 – point 22 – point b
Règlement (UE) n° 910/2014
Article 20 – paragraphe 2 – alinéa 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Une partie prenante qui utilise des services de confiance qualifiés, tels que des certificats qualifiés ou une attestation électronique qualifiée d'attributs, dans une entreprise, peut introduire auprès de l'autorité de contrôle une réclamation concernant la sécurité ou la fiabilité du service de confiance qualifié.

Or. en

Amendement 16

Proposition de règlement
Article 1 – paragraphe 1 – point 25 – point c – point 2
Règlement (UE) n° 910/2014
Article 24 – paragraphe 2 – point f ter bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(f ter bis) veille au traitement licite des données à caractère personnel conformément au règlement (UE) 2016/679;

Or. en

ANNEXE: LISTE DES ENTITÉS OU PERSONNES AYANT APPORTÉ LEUR CONTRIBUTION AU RAPPORTEUR

La liste suivante est établie sur une base purement volontaire, sous la responsabilité exclusive du rapporteur. Le rapporteur a reçu des contributions des entités ou personnes suivantes pour l'élaboration du projet d'avis:

Entité et/ou personne

1. European Commission DG CNECT

2. The European Data Protection Supervisor
3. Brussels Privacy Hub, *THE EUROPEAN COMMISSION PROPOSAL AMENDING THE eIDAS REGULATION (EU) No 910/2014: A PERSONAL DATA PROTECTION PERSPECTIVE*
4. Professor Ricardo Genghini, Chairman of the European Standardization Committee E-Signature and Infrastructures (ESI) within the European Telecommunications Standards Institute (ETSI) - *Notes on the current draft of eIDAS Revision Proposal*
5. epicenter.works & European Digital Rights (EDRI)
6. Luukas Ilves, Deputy Secretary General of the Estonian Ministry of Economic Affairs and Communications for Digital Development
7. European Consumer Organisation (BEUC) - *Making European Digital Identity as Safe as It Is needed - BEUC Position Paper*
8. Jaap-Henk Hoepman, Associate Professor of privacy enhancing protocols and privacy by design in the Digital Security group at the Institute for Computing and Information Sciences of the Radboud University Nijmegen, *Civil liberties aspects of the commission proposal to amend the eIDAS regulation*
9. Eric Verheul, professor in the Digital Security Group of the Radboud University Nijmegen - *Issues and recommendations on the eIDAS wallet as proposed in the eIDAS update*
10. Manuel Atug expert in IT Security and engineering Chaos Computer Club & Christian Kahlo eID expert - *written input*
11. Lukasz Olejnik, PhD, https://lukaszolejnik.com, *written contribution*
12. Carmela Troncoso - Professor on Security and Privacy at Swiss Federal Institute of Technology Lausanne - *written input*
13. Dr. F. S. Gürses, Associat Professor at the Faculty of Technology, Policy and Management, TU Delft - *written input*
14. Eurosmart - The Voice Of The Digital Security Industry - Feedback on the revision of eIDAS
15. Mozzila
16. Google
17. Apple
18. The International Association for Trusted Blockchain Applications (INATBA) - Establishing a Framework for a European Digital Identity (eIDAS) - Policy Position
19. TWG Trusted Information of the EU Observatory for ICT Standardisation - report on "Trust in the European digital space in the age of automated bots and fakes"
20. Rule of Law Defense Coalition, Bucharest Romania
21. American Chamber of Commerce to the European Union, Brussels - *written input*