LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du Contrôleur européen de la protection des données

sur une proposition de directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2006/48/CE et 2009/110/CE et abrogeant la directive 2007/64/CE, ainsi qu'une proposition de règlement du Parlement européen et du Conseil relatif aux commissions d'interchange pour les opérations de paiement liées à une carte

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) nº 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[2], et notamment son article 28, paragraphe 2.

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION

1.1. Consultation du CEPD

1. Le 27 juillet 2013, la Commission a adopté un projet de proposition de directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2006/48/CE et 2009/110/CE et abrogeant la directive 2007/64/CE (la «proposition de directive»), ainsi qu'une proposition de règlement du Parlement européen et du Conseil relatif aux commissions d'interchange pour les opérations de paiement liées à une carte.[3] Ces propositions ont été envoyées au CEPD pour consultation le 28 juillet 2013.

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] COM (2013) 547 final et COM (2013) 550 final.

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 30
E-mail: edps@edps.europa.eu - Site Internet: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax: 02-283 19 50

2. Le CEPD se félicite du fait qu'il soit consulté par la Commission et se réjouit qu'une référence au présent avis ait été incluse dans le préambule des actes.

3. Le CEPD a eu la possibilité de faire part d'observations informelles à la Commission avant l'adoption de la proposition de règlement. Certaines de ces observations ont été prises en compte. Par conséquent, les garde-fous en matière de protection des données prévus par la proposition de règlement ont été renforcés.

4. Étant donné que la proposition de règlement ne soulève aucun problème du point de vue de la protection des données, le CEPD concentrera ses observations sur la proposition de directive.

1.2. Objectifs et portée de la proposition de directive

5. La proposition de directive a pour objet de favoriser un développement plus poussé d'un marché des paiements électroniques à l'échelle de l'UE qui permette aux consommateurs, aux détaillants et aux autres acteurs du marché de profiter pleinement des avantages offerts par le marché intérieur de l'UE, conformément à ce que prévoient la stratégie Europe 2020 et la stratégie numérique pour l'Europe. Pour atteindre cet objectif et pour promouvoir davantage de concurrence, d'efficience et d'innovation dans le secteur des paiements électroniques, la Commission affirme que la sécurité juridique et l'égalité des conditions de concurrence sont un préalable indispensable et qu'il en résultera une convergence à la baisse des coûts et des prix pour les utilisateurs de services de paiement, ainsi qu'un plus large choix et une plus grande transparence de ces services, ce qui facilitera l'offre de services de paiement innovants et permettra de garantir des services de paiement sûrs et transparents.

6. La Commission fait valoir que ces objectifs seront atteints en actualisant et en complétant le cadre régissant actuellement les services de paiement, en prévoyant des règles pour renforcer la transparence, l'innovation et la sécurité dans le domaine des paiements de détail et pour améliorer la cohérence des réglementations nationales, eu égard, tout particulièrement, aux besoins légitimes des consommateurs.

2. OBSERVATIONS SPÉCIFIQUES SUR LA PROPOSITION DE DIRECTIVE

2.1. Référence générale à la législation relative à la protection des données

7. Le CEPD relève que la fourniture de services de paiement requiert le traitement, par différentes parties prenantes, de données à caractère personnel: les nom, numéro de compte bancaire et contenu des contrats doivent être échangés entre les payeurs et les bénéficiaires et communiqués à leurs prestataires de services de paiement respectifs, afin de garantir le bon fonctionnement des transferts.

8. Le CEPD se réjouit de l'introduction dans l'article 84 d'une disposition de fond prévoyant que *tout* traitement de données à caractère personnel aux fins de la proposition de directive doit être effectué conformément aux règles nationales transposant la directive 95/46/CE et la directive 2002/58/CE, ainsi qu'au règlement (CE) n° 45/2001.

9. Toutefois, le CEPD rappelle que le fait de clarifier la législation applicable en matière de protection des données est essentiel mais pas suffisant. Les références à la législation applicable en matière de protection des données devraient être spécifiées dans des garde-fous concrets qui s'appliqueront à toute situation dans laquelle le traitement de données à caractère personnel est envisagé.

10. Dans sa lettre en réponse à la consultation publique de la Commission sur le livre vert intitulé «Vers un marché européen intégré des paiements par carte, par internet et par téléphone mobile»[4], le CEPD a souligné que le respect total des règles de l'UE en matière de protection des données requiert l'application de garde-fous spécifiques. En particulier, il a indiqué que l'échange et le traitement de données à caractère personnel liées aux payeurs et aux bénéficiaires et avec les divers prestataires de services de paiement doivent respecter les principes de nécessité, de proportionnalité et de limitation des finalités, ainsi que l'obligation de ne pas conserver les données pendant une durée excédant celle nécessaire. Le CEPD a également insisté sur l'importance cruciale de la transparence comme moyen de garantir l'exercice effectif des droits des personnes en matière de protection des données. Le CEPD recommande dès lors que des garde-fous spécifiques soient explicitement introduits dans le texte de la proposition de directive, ainsi qu'il est détaillé plus avant ci-dessous.

2.2. La base juridique du traitement de données à caractère personnel

11. En ce qui concerne le traitement de données à caractère personnel par les systèmes de paiement et les prestataires de services de paiement, il convient de préciser dans la proposition de directive que la fourniture de services de paiement entraîne le traitement de données à caractère personnel. À l'heure actuelle, la proposition de directive n'envisage le traitement de données à caractère personnel qu'aux fins de la prévention, des enquêtes et de la détection de la fraude en matière de paiement aux termes du considérant 71, sans prendre en compte le fait que la prestation de services de paiement peut elle-même impliquer le traitement de données à caractère personnel. S'agissant de la base juridique justifiant un tel traitement, il convient de préciser expressément dans la proposition de directive que le traitement de données à caractère personnel peut être effectué dès lors qu'il est nécessaire à la prestation de services de paiement.

[4] Voir la lettre du CEPD du 11 avril 2012 en réponse à la consultation publique de DG MARKT sur le livre vert intitulé «Vers un marché européen intégré des paiements par carte, par internet et par téléphone mobile», consultable sur: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2012/12-04-11_Mobile_Payments_EN.pdf

12. En ce qui concerne le traitement de données à caractère personnel aux fins de la prévention, des enquêtes et de la détection de la fraude en matière de paiement, le CEPD estime que l'article 84 de la proposition de directive n'est pas suffisamment précis pour pouvoir être considéré comme un fondement juridique valable pour un tel traitement. Les dispositions régissant la prévention de la fraude devraient, tout au moins dans les grandes lignes, définir plus précisément la (les) finalité(s) du traitement, les données à caractère personnel concernées et les modalités du traitement. Au moment de définir ces éléments liés au traitement de données à caractère personnel, il convient de tenir dûment compte du principe de proportionnalité (selon lequel seules les données à caractère personnel qui sont nécessaires aux fins du traitement peuvent être traitées). Le CEPD recommande dès lors d'insérer une disposition plus précise dans la proposition de directive.

2.3. Proportionnalité du traitement

13. Il convient de veiller à ce que les différents acteurs n'aient accès aux, et ne traitent que les données qui sont nécessaires pour la prestation de leurs services (voir notamment le considérant 26). À titre d'illustration, les opérateurs mobiles responsables de la transmission de l'ordre de transaction ne doivent pas, en principe, avoir accès aux informations relatives au contenu sur le détail des paiements. Cela devrait être expressément indiqué dans une disposition de fond de la proposition de directive.

14. De la même manière, les dispositions sur l'accès des tiers (voir ci-dessous au point 2.7.) des articles 58 et 59 de la proposition de directive devraient préciser que les informations sur la «disponibilité des fonds nécessaires» devraient consister en une simple réponse «oui» ou «non» à la question de savoir s'il y a suffisamment de fonds disponibles, et non en un relevé indiquant le solde du compte, par exemple.

15. Le CEPD souligne l'importance de la mise en œuvre des principes de «respect de la vie privée dès la conception» et de «respect de la vie privée par défaut» dans tous les systèmes de traitement de données développés et utilisés dans le cadre de la proposition de directive. Ces concepts sont apparus dans le cadre de l'actuelle directive 95/46/CE relative à la protection des données et devraient bénéficier d'une reconnaissance juridique dans la proposition de règlement général relatif à la protection des données (voir l'article 23)[5]. Le «respect de la vie privée dès la conception» fait référence à l'intégration de la protection des données et du respect de la vie privée dès les toutes premières étapes de la conception de nouveaux produits, services et procédures impliquant le traitement de données à caractère personnel, tandis que le «respect de la vie privée par défaut» se rapporte à la sélection de la configuration la plus favorable par défaut au respect de la vie privée.

[5] COM (2012) 11 final.

16. Le «respect de la vie privée dès la conception» implique, entre autres, de veiller à ce que les systèmes de traitement des données soient conçus pour traiter le moins de données à caractère personnel possible (minimisation des données), de mettre en œuvre un paramétrage «par défaut» favorable au respect de la vie privée; de limiter l'accès aux renseignements personnels à ce qui est strictement nécessaire pour fournir le service; et de mettre en œuvre des outils permettant aux utilisateurs de mieux protéger leurs données à caractère personnel (par exemple, contrôles de l'accès, cryptage) et exercer leurs droits.

17. Le CEPD a souligné à maintes reprises l'importance de tenir compte de façon adéquate de ces concepts dans la mise en œuvre de la stratégie numérique[6], en prévision de l'adoption de la proposition de règlement général relatif à la protection des données. Il recommande donc d'ajouter une disposition de fond dans la proposition de directive prévoyant l'obligation d'intégrer le «respect de la vie privée dès la conception/respect de la vie privée par défaut» dans tous les systèmes de traitement de données développés et utilisés dans le cadre de la proposition de directive.

2.4. Supervision par les autorités compétentes

18. Le CEPD se réjouit du fait que la proposition de directive instaure, au considérant 32, l'obligation pour les autorités compétentes d'exercer leurs compétences «dans le respect des droits fondamentaux, notamment du droit au respect de la vie privée» dans le cadre de la surveillance de la conformité des établissements de paiement. Ce considérant dispose également que, pour l'exercice des compétences pouvant conduire à de graves atteintes au droit au respect de la vie privée et familiale, du domicile et des communications, les États membres devraient mettre en place des garde-fous adéquats et efficaces contre toute pratique abusive ou arbitraire, par exemple, le cas échéant, au moyen d'une autorisation préalable donnée par les autorités judiciaires de l'État membre concerné. Le CEPD rappelle que ces exigences s'appliquent sans préjudice du contrôle d'une autorité indépendante (autorité nationale de protection des données) au titre de l'article 8, paragraphe 3, de la charte des droits fondamentaux de l'Union européenne.

19. Le CEPD souhaiterait néanmoins voir ces exigences se concrétiser en une disposition de fond dans la proposition de directive. Il recommande donc d'introduire dans l'article 22 l'obligation pour les autorités compétentes de demander des documents et des informations par une décision formelle, en spécifiant la base juridique et la finalité de la demande, les informations requises ainsi que le délai dans lequel ces informations doivent être communiquées.

[6] Voir l'avis du CEPD du 18 mars 2010 sur la «Promotion de la confiance dans la société d'information par des mesures d'encouragement de la protection des données et de la vie privée» et l'avis du CEPD du 10 avril 2013 sur la Communication de la Commission sur «Une stratégie numérique pour l'Europe: faire du numérique un moteur de la croissance européenne», disponible dans la rubrique Consultation du site Internet du CEPD: www.edps.europa.eu.

2.5. Échange d'informations

20. L'article 25 de la proposition de directive exige des autorités compétentes qu'elles échangent des informations entre elles et avec la Banque centrale européenne, les banques centrales nationales des États membres, l'ABE et d'autres autorités compétentes désignées au titre des législations de l'Union ou nationales applicables aux prestataires de services de paiement.

21. L'article 26, paragraphe 3, dispose que les autorités compétentes se communiquent mutuellement toute information essentielle et/ou pertinente, notamment en cas d'infraction ou d'infraction présumée de la part d'un agent, d'une succursale ou d'une entité vers laquelle des activités sont externalisées. Dans certains cas, ces échanges d'informations concerneront assurément des personnes identifiées ou identifiables, par exemple un agent, un utilisateur de services de paiement ou un consommateur.

22. Le CEPD considère que ces deux dispositions sont trop vagues et que, par conséquent, elles ne fournissent pas une base juridique adéquate pour le traitement de données à caractère personnel requis. S'agissant de la limitation des finalités, la proposition de directive ne spécifie ni les finalités de l'échange d'informations, ni le type de données qui seront échangées, notamment les données à caractère personnel. En outre, le CEPD constate que la proposition de directive ne prévoit aucune limitation concrète de la période de conservation des données à caractère personnel potentiellement traitées. Cela pourrait être source d'incertitude et conduire à une diversité excessive dans la mise en œuvre et/ou la pratique nationale.

23. Au vu des éléments qui précèdent, le CEPD recommande (i) de mentionner les finalités pour lesquelles les données à caractère personnel peuvent être traitées par les autorités nationales compétentes, la Banque centrale européenne, les banques centrales nationales et les autres autorités visées à l'article 25, (ii) de spécifier le type d'informations personnelles qui peuvent être traitées dans le cadre de la proposition de directive, et (iii) de fixer une période de conservation des données proportionnelle au traitement précité (ou tout au moins d'instaurer des critères précis pour son établissement au niveau national).

2.6. Transparence et information des personnes

24. Le CEPD remarque que plusieurs dispositions[7] prévoient un certain nombre d'obligations visant à renforcer la transparence à l'égard des utilisateurs. Il estime que l'obligation de transparence concernant les services de paiement devrait également recouvrir l'obligation de transparence à l'égard du traitement de données à caractère personnel. Les personnes concernées devraient savoir qui traite quelles données et à

[7] Par exemple, les articles 37 à 42, 44 à 46, 49 à 51 et les considérants 32, 35 et 39 à 42.

quelle fin, pendant combien de temps et de quelle façon elles peuvent exercer leurs droits, y compris ceux relatifs à l'accès à leurs données ainsi qu'à leur rectification ou à leur effacement.

25. Dès lors, le CEPD recommande d'inclure, dans une disposition de fond de la proposition de directive, une référence spécifique à l'obligation de communiquer aux personnes des informations appropriées sur le traitement de données à caractère personnel, conformément aux dispositions nationales mettant en œuvre les articles 10 et 11 de la directive 95/46/CE et à l'article 11 du règlement CE nº 45/2001.

26. En outre, le considérant 35 devrait aussi être modifié de façon à exiger la communication de toutes les informations requises au titre de la directive «*ainsi qu'au titre de la directive 95/46/CE et du règlement CE nº 45/2001*» (de même, le mot «*seul*» devrait être supprimé car les obligations d'information prévues dans la directive ne sont pas les seules qui doivent être respectées).

27. La communication d'informations sur le traitement de données à caractère personnel en temps utile avant de recourir au service de paiement est d'autant plus importante que le consentement de l'utilisateur est destiné à jouer un rôle central et que l'autorisation des opérations de paiement ne peut être considérée comme donnée que si le payeur a donné son consentement. Avant de donner son consentement à l'opération, le payeur doit être informé non seulement du prix et du calcul des frais, mais aussi des modalités du traitement de ses données à caractère personnel, afin qu'il puisse prendre une décision éclairée quant à ce paiement et aux implications sur le traitement de ses données à caractère personnel.

28. Le CEPD se réjouit que les dispositions sur la transparence instaurent des règles claires sur les modalités de la communication d'informations aux utilisateurs et sur la nécessité que ces informations soient consultables à tout moment. Il recommande qu'il soit expressément indiqué dans les dispositions relatives à la transparence que les modalités prévues concernant la communication d'informations aux utilisateurs s'appliquent également à la communication d'informations sur le traitement de données à caractère personnel, en application des articles 10 et 11 de la directive 95/46/CE.

2.7. Accès des tiers

29. Les articles 58 et 59 de la proposition de directive instaurent des règles régissant l'accès aux données des comptes de paiement et l'utilisation de ces données par des prestataires de services de paiement tiers et des émetteurs tiers d'instruments de paiement.

30. Le CEPD constate que la Commission a tenu compte de la protection des données lors de la rédaction de ces articles, notamment du principe de minimisation des données. Toutefois, le CEPD est d'avis que les dispositions pertinentes laissent une trop grande marge d'interprétation. Ainsi, par exemple, les termes «disponibilité des fonds nécessaires» et «données sensibles en matière de paiements» ne sont définis nulle part dans le texte de la proposition de directive. Si ces termes non définis se voyaient accorder une interprétation large dans le droit national, cela pourrait conduire à une transposition divergente dans les États membres, avec la possibilité de risques en matière de protection des données liés à l'accès des tiers.

31. Dans le cas de la «disponibilité des fonds nécessaires», le CEPD recommande de préciser que les informations transmises aux tiers devraient consister en une simple réponse «oui» ou «non» à la question de savoir s'il y a suffisamment de fonds disponibles, et non en un relevé indiquant le solde du compte, par exemple.

32. Le terme «données sensibles en matière de paiements» n'existe pas dans la législation relative à la protection des données. L'article 8 de la directive 95/46/CE répertorie les catégories particulières de données sensibles bénéficiant d'un niveau de protection accru. Les données en matière de paiements ne font pas partie des catégories répertoriées. Cela ne signifie pas que les données à caractère personnel en matière de paiements ne sont pas protégées par la législation relative à la protection des données, mais simplement qu'elles ne sont pas qualifiées de «données sensibles». Le CEPD recommande donc de supprimer le mot «sensible» et de le remplacer par le terme «données en matière de paiements».

2.8. Exigences en matière de sécurité

33. Le CEPD se félicite de l'obligation faite par l'article 5, point j), aux établissements de paiement de fournir aux autorités compétentes un document relatif à la politique de sécurité, une analyse détaillée des risques en ce qui concerne les services de paiement proposés et une description des mesures de maîtrise et d'atténuation prises pour protéger les utilisateurs de services de paiement de façon adéquate contre les risques décelés en matière de sécurité, y compris la fraude et l'utilisation illicite de données sensibles ou à caractère personnel.

34. Compte tenu de l'importance cruciale de la sécurité dans le domaine des services de paiement, il convient de garantir que le traitement de données à caractère personnel et leur communication aux différents intermédiaires respectent les principes de confidentialité et de sécurité prévus aux articles 16 et 17 de la directive 95/46/CE. Le CEPD recommande d'ajouter au considérant 6 et à l'article 85 que le traitement de données à caractère personnel doit respecter les exigences de sécurité prévues aux articles 16 et 17 de la directive 95/46/CE.

35. Le considérant 6 et l'article 85 instaurent l'obligation de signaler sans délai à l'Autorité bancaire européenne les incidents de sécurité majeurs. Le CEPD souhaite souligner que des exigences de notification similaires sont également prévues par la directive 2002/58/CE, telle que modifiée par la directive 2009/136/CE, pour le secteur des télécommunications lorsque des données à caractère personnel sont compromises; aux termes de la directive, l'entité responsable doit signaler cette violation à l'autorité compétente (c'est-à-dire l'autorité de protection des données ou le régulateur des télécommunications) ainsi qu'aux personnes concernées, le cas échéant.

36. Il convient donc de garantir la cohérence avec les exigences en matière de violation de données à caractère personnel qui sont déjà applicables aux fournisseurs de télécommunications en vertu de la directive 2002/58/CE, telle que modifiée par la directive 2009/136/CE, mais aussi avec les dispositions relatives aux violations de données à caractère personnel envisagées par la proposition de règlement général relatif à la protection des données, dispositions qui s'appliqueraient à l'ensemble des responsables du traitement (articles 31 et 32). Il convient de préciser dans un considérant de la proposition de directive que les obligations de signalement des incidents de sécurité s'appliquent sans préjudice des autres obligations de signalement d'incidents prévues par d'autres législations, en particulier les exigences relatives aux violations de données à caractère personnel prévues par la loi sur la protection des données (dans la directive 2002/58/CE et dans la proposition de règlement général relatif à la protection des données) et les exigences de notification d'incidents de sécurité envisagées dans le cadre de la proposition de directive sur la sécurité des réseaux et de l'information[8], proposition sur laquelle le CEPD a publié un avis[9] le 14 juin 2013. Le CEPD aimerait également souligner que le fait que la proposition de directive se réfère, à l'article 85, à la proposition de directive sur la sécurité des réseaux et de l'information, toujours en cours de négociation, donne lieu à une situation ambiguë qui renforce encore la nécessité de clarification.

37. L'article 87 de la proposition de directive dispose que les États membres doivent veiller à ce qu'un prestataire de services de paiement applique l'authentification des tiers. Cet article dispose également que l'Autorité bancaire européenne (ABE), en coopération étroite avec la Banque centrale européenne (BCE), doit publier des orientations adressées aux prestataires de services de paiement concernant les techniques les plus avancées d'authentification des clients et les cas éventuels d'inapplication de l'authentification forte des clients. Le CEPD recommande d'inclure dans la proposition de directive des références à la

[8] Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, COM(2013) 48 final.

[9] Avis du CEPD du 14 juin 2013 sur la «stratégie de l'Union européenne en matière de cybersécurité», disponible dans la rubrique Consultation du site Internet du CEPD: www.edps.europa.eu

nécessité de consulter le CEPD pour autant que les orientations concernent le traitement de données à caractère personnel.

2.9. Normalisation et interopérabilité

38. La proposition de directive insiste sur la nécessité de développer et de renforcer la normalisation et l'interopérabilité. Comme nous l'avons souligné dans notre réponse à la consultation publique, nous considérons que le développement de ces normes devrait être précédé par des analyses d'impact sur le respect de la vie privée visant à analyser les implications des nouvelles technologies disponibles sur le respect de la vie privée et la protection des données des personnes. Ce processus devrait permettre d'identifier les risques associés à chacune des options techniques disponibles ainsi que les remèdes qui pourraient être mis en place pour minimiser les risques liés à la protection des données. Nous suggérons donc d'ajouter, dans une disposition de fond de la proposition de directive, l'obligation de développer ces normes sur la base – et après réalisation – d'analyses d'impact sur le respect de la vie privée.

3. CONCLUSIONS

Le CEPD se réjouit de l'introduction dans l'article 84 d'une disposition de fond prévoyant que *tout* traitement de données à caractère personnel aux fins de la proposition de directive doit être effectué conformément aux règles nationales transposant la directive 95/46/CE et la directive 2002/58/CE, ainsi qu'au règlement (CE) n° 45/2001.

Le CEPD recommande ce qui suit:

- les références à la législation applicable en matière de protection des données devraient être spécifiées dans des garde-fous concrets qui s'appliqueront à toute situation dans laquelle le traitement de données à caractère personnel est envisagé;

- le projet de directive devrait préciser que la fourniture de services de paiement peut impliquer le traitement de données à caractère personnel;

- la proposition de directive devrait clarifier expressément que le traitement de données à caractère personnel peut être effectué dès lors qu'il est nécessaire à la prestation de services de paiement;

- une disposition de fond devrait être ajoutée prévoyant l'obligation d'intégrer le «respect de la vie privée dès la conception/respect de la vie privée par défaut» dans tous les systèmes de traitement de données développés et utilisés dans le cadre de la proposition de directive;

- en ce qui concerne les échanges d'informations: (i) mentionner les finalités pour lesquelles les données à caractère personnel peuvent être traitées par les autorités nationales compétentes, la Banque centrale européenne, les banques centrales nationales et les autres autorités visées à l'article 25, (ii) spécifier le type d'informations personnelles qui peuvent être traitées dans le cadre de la proposition de directive, et (iii) fixer une période de conservation des données proportionnelle au traitement ou, tout au moins, instaurer des critères précis pour son établissement;

- une exigence devrait être introduite dans l'article 22 contraignant les autorités compétentes à demander des documents et des informations par une décision formelle, en spécifiant la base juridique et la finalité de la demande, les informations requises ainsi que le délai dans lequel ces informations doivent être communiquées;

- l'article 31 devrait indiquer que les modalités prévues concernant la communication d'informations aux utilisateurs s'appliquent également à la communication d'informations sur le traitement de données à caractère personnel, en application des articles 10 et 11 de la directive 95/46/CE;

- dans le cas du terme «disponibilité des fonds nécessaires» prévu aux articles 58 et 59, il devrait être précisé que les informations transmises aux tiers devraient consister en une simple réponse «oui» ou «non» à la question de savoir s'il y a suffisamment de fonds disponibles, et non en un relevé indiquant le solde du compte, par exemple;

- dans le cas du terme «données sensibles en matière de paiements» à l'article 58, le mot «sensible» devrait être supprimé et remplacé par le terme «données en matière de paiements»;

- il convient de clarifier dans un considérant que les obligations de signalement des incidents de sécurité s'appliquent sans préjudice des autres obligations de signalement d'incidents prévues par d'autres législations, en particulier les exigences relatives aux violations de données à caractère personnel prévues par la loi sur la protection des données (dans la directive 2002/58/CE et dans la proposition de règlement général relatif à la protection des données) et les exigences de notification d'incidents de sécurité envisagées dans le cadre de la proposition de directive sur la sécurité des réseaux et de l'information;

- il convient de garantir que le traitement de données à caractère personnel et leur communication aux différents intermédiaires respectent les principes de confidentialité et de sécurité prévus aux articles 16 et 17 de la directive 95/46/CE;

- une disposition de fond devrait être ajoutée à la proposition de directive prévoyant l'obligation de développer des normes sur la base – et après réalisation – d'analyses d'impact sur le respect de la vie privée;

- il convient d'inclure dans la proposition de directive une référence à la nécessité de consulter le CEPD dans la mesure où les orientations de l'ABE concernant les techniques les plus avancées d'authentification des clients et les cas éventuels d'inapplication de l'authentification forte des clients portent sur le traitement de données à caractère personnel.

Bruxelles, le 5 décembre 2013

(signé)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données