Avis du Contrôleur européen de la protection des données

sur le règlement de la Commission établissant le registre de l'Union pour la période d'échanges débutant le 1er janvier 2013 et pour les périodes d'échanges suivantes du système d'échanges de quotas d'émission de l'Union

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[2],

vu la demande d'avis formulée conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001,

A ADOPTÉ L'AVIS SUIVANT:

1. Introduction:

1.1. Contexte

1. Le 18 novembre 2011, la Commission a adopté le règlement (UE) n° 1193/2011 de la Commission établissant le registre de l'Union pour la période d'échanges débutant le 1er janvier 2013 et pour les périodes d'échanges suivantes du système d'échange de quotas d'émission de l'Union conformément à la directive 2003/87/CE du Parlement européen et du Conseil et à la décision n° 280/2004/CE du Parlement européen et du Conseil et modifiant les règlements de la Commission(CE) n° 2216/2004 et (UE) n° 920/2010 (ci après le «règlement»)[3]. Le même jour, le règlement a été communiqué au CEPD pour consultation.

[1] JO L 281 du 23.11.1995, p. 31
[2] JO L 8 du 12.1.2001, p. 1
[3] JO L315 du 29.11.2011, p. 1.

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 63
E-mail : edps@edps.europa.eu - Site internet: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax : 02-283 19 50

2. Avant l'adoption du règlement, le CEPD a eu l'occasion de formuler des observations informelles, dont certaines ont été prises en compte dans le règlement, et le CEPD observe que, de ce fait, les garanties en matière de protection des données ont été renforcées.

3. Le CEPD salue le fait d'être consulté de manière formelle par la Commission et qu'il soit fait référence au présent avis dans le préambule de l'instrument adopté.

1.2. Objectifs et champ d'application du règlement

4. Le système communautaire d'échange de quotas d'émission (SCEQE) figure parmi les politiques mises en place à l'échelle de l'Union européenne (UE) pour contribuer à la réalisation des objectifs de l'UE en matière de réduction des émissions de gaz à effet de serre conformément au protocole de Kyoto. Le SCEQE instaure un régime de mise en conformité pour les opérateurs et vise à garantir le plafonnement effectif des émissions dans l'ensemble de l'UE[4].

5. Le présent règlement modifie et remplacera, à partir du 1er janvier 2013, les précédents règlements de la Commission en la matière, notamment le règlement (CE) n° 2216/2004 et le règlement (UE) n° 920/2010[5] fixant les règles d'un «système de registres normalisé et sécurisé».

6. Une des principales nouveautés introduites par le présent règlement est l'établissement, à partir de 2012, d'un registre de l'Union centralisé en lieu et place du précédent système de combinaison des registres nationaux.

7. Le registre de l'Union et le journal des transactions de l'Union européenne (ou «EUTL»), déjà opérationnel au niveau de l'UE, sont deux sous-systèmes hébergés et gérés par la Commission européenne. Leurs fonctions sont différentes, mais ce sont des systèmes complémentaires.

8. Le registre de l'Union contient les comptes des acteurs intervenant dans le SCEQE (par exemple, les comptes de dépôt d'exploitant, les comptes de dépôt d'exploitant d'aéronef, les comptes de négociation, les comptes Enchères) et enregistre les transactions entre les comptes. Le registre de l'Union est donc un registre électronique central établi au niveau de l'UE pour soutenir les échanges de quotas d'émission par les titulaires de comptes au sein et entre les États membres.

9. L'EUTL permet quant à lui de consigner les allocations, transferts et annulations de quotas d'émission de CO2 dans l'UE et de vérifier la cohérence de certaines opérations.

2. Objectifs et structure de l'avis du CEPD

10. Bien que ce ne soit pas son objectif principal, le règlement requiert le traitement de données à caractère personnel, notamment les informations issues du casier judiciaire et les informations relatives aux suspicions d'activités criminelles. Le

[4] Pour plus d'informations sur le SCEQE, voir le document http://ec.europa.eu/clima/publications/docs/ets_fr.pdf.
[5] JO L 386 du 29.12.2004, p. 1 et JO L 270 du 14.10.2010, p. 1.

traitement de ces données vise à s'assurer que les comptes ne seront pas utilisés abusivement à des fins criminelles.

11. Les données à caractère personnel peuvent concerner les personnes agissant au nom des titulaires de compte, par exemple, les «directeurs» et représentants autorisés de ces titulaires. En outre, les titulaires de compte peuvent également être des personnes physiques, ce qui peut impliquer le traitement de leurs données à caractère personnel. Par ailleurs, des données sont également collectées au sujet des bénéficiaires effectifs des titulaires de compte, qui peuvent aussi être des personnes[6].

12. Compte tenu du caractère personnel — souvent sensible — des données à traiter en vertu du règlement, le CEPD recommande de prévoir dans le règlement des garanties adéquates en matière de protection des données.

13. Le règlement ayant déjà été adopté, l'objectif premier du présent avis est de s'assurer que les recommandations du CEPD seront prises en compte lors de la modification du règlement, prévue fin 2012.

14. Les présentes recommandations peuvent en outre guider la Commission et les administrateurs nationaux dans la mise en œuvre, au niveau pratique, des garanties nécessaires en matière de protection des données. Pour plus de détails sur la mise en œuvre au niveau pratique, voir les points 41 à 43 appelant à l'élaboration d'une politique complète de protection des données, le point 36 relatif à d'autres mesures pratiques telles que les menus d'aide, messages d'avertissement dans le registre de l'Union et documents de formation, et le point 40 concernant la documentation relative au système et la publication d'informations sur le site web du registre de l'Union.

15. La section 3 du présent avis fournit une brève description des données à caractère personnel — en se focalisant sur les données sensibles — à traiter en application du règlement. Cette description est nécessaire pour la mise en contexte des recommandations formulées dans les sections 4 à 12 du présent avis. La section 4 réclame davantage de précisions sur les données à caractère personnel traitées en vertu du règlement, sur les personnes appelées à traiter ces données ainsi que sur le stockage des données, toujours en se focalisant sur les données sensibles. Les autres recommandations du CEPD sont formulées aux sections 5 à 12. La section 13 contient les conclusions du CEPD.

3. Données à caractère personnel à traiter en vertu du règlement

Informations traitées par les administrateurs nationaux en relation avec l'ouverture et la gestion d'un compte

16. Une large part des données à caractère personnel à traiter en vertu du règlement est recueillie par les administrateurs nationaux de chaque État membre auprès des demandeurs lorsqu'ils sollicitent l'ouverture d'un compte dans le registre de l'Union (voir articles 12 à 24, renvoyant à diverses annexes). Lesdits «administrateurs nationaux» sont les entités chargées de gérer, au nom d'un État membre, une série

[6] Voir la section 3 pour plus de détails sur les catégories de données traitées en vertu du règlement, y compris les données sensibles.

de comptes d'utilisateur du registre de l'Union qui relèvent de la juridiction de cet État.

17. Pour l'ouverture d'un compte, le règlement exige des demandeurs qu'ils fournissent des informations, dont des données à caractère personnel, à l'administrateur national. Les informations requises dépendent du type de compte (voir, en particulier, les annexes II, III, IV, V et VII).

18. Les données à communiquer sont le code d'identification personnelle, le nom, la désignation de la fonction, l'adresse, les numéros de téléphone fixe et de téléphone portable, la date et le lieu de naissance ainsi que la langue préférée. Les demandeurs doivent parfois également fournir une copie de la carte d'identité, du passeport, de la preuve de la résidence permanente et du contenu du casier judiciaire.

19. En outre, certaines informations sur le bénéficiaire effectif de la personne morale doivent être communiquées aux administrateurs nationaux dans le cadre de la prévention de l'utilisation du système financier à des fins de blanchiment de capitaux et de financement du terrorisme (voir annexe III, point 5(d)).

20. Par ailleurs, l'article 20 impose aux administrateurs nationaux de refuser l'ouverture d'un compte dans certaines circonstances, notamment s'ils ont de bonnes raisons de suspecter que les comptes sont utilisés pour commettre des fraudes concernant des quotas ou des unités de Kyoto, pour des opérations de blanchiment de capitaux ou de financement du terrorisme, ou pour d'autres délits graves. Les informations supplémentaires (au-delà des documents à fournir précisés par le règlement) auxquelles un administrateur national peut accéder pour conclure à l'existence de tels «doutes raisonnables» ne sont pas spécifiées, leur définition étant probablement laissée à la charge du droit national.

21. À l'instar de l'article 20, d'autres dispositions relatives à la gestion de compte requièrent aussi le traitement par l'administrateur national de données sensibles en rapport avec les suspicions d'activité criminelle. Ces dispositions sont:

- l'article 22 concernant le refus d'agréer des représentants autorisés;
- l'article 31 relatif à la suspension de l'accès aux comptes;
- l'article 30 concernant la clôture de comptes et la révocation de représentants autorisés «à l'initiative de l'administrateur»; et
- l'article 71 relatif à la «suspension de l'accès à des quotas ou à des unités de Kyoto en cas de suspicion de transaction frauduleuse».

Échanges d'informations entre administrateurs nationaux, Commission et tiers, dont les services de répression

22. L'article 71 et diverses autres dispositions du règlement (dont l'article 36, paragraphe 4, et les articles 70, 72, 73 et 83) appellent à un échange des données — notamment celles concernant des suspicions d'activité criminelle — entre les administrateurs nationaux, la Commission et des tiers, dont les services de répression.

23. L'article 71, paragraphe 3, du règlement prévoit que l'administrateur national (ou la Commission) «informe immédiatement l'autorité compétente chargée de faire appliquer la loi de [la] suspension [de l'accès à un compte]». L'article 72 exige que

les administrateurs nationaux coopèrent avec les autorités compétentes et notifient toute constatation ou suspicion d'opérations de blanchiment de capitaux, de financement du terrorisme ou d'activités criminelles. L'article 36, paragraphe 4, impose d'autres exigences de notification spécifiques. Par ailleurs, l'article 83, paragraphe 8, autorise spécifiquement — sans toutefois l'exiger — la notification aux autorités chargées de faire appliquer la loi et aux autorités fiscales de certains types de transaction suspects spécifiques.

24. L'article 70, paragraphes 2 et 3, du règlement demande que les atteintes ou risques d'atteinte à la sécurité susceptibles d'aboutir à la suspension de l'accès au registre de l'Union soient notifiés aux administrateurs nationaux et à la Commission.

25. En outre, l'article 73, paragraphe 1, du règlement dispose que «[l]a Commission peut donner instruction à l'administrateur central de suspendre temporairement l'acceptation par l'EUTL de certains ou de la totalité des processus ayant pour origine le registre de l'Union, si celui-ci n'est pas géré et tenu conformément aux dispositions du présent règlement. Elle en informe immédiatement les administrateurs nationaux concernés».

26. L'article 83, paragraphe 7, du règlement prévoit que les administrateurs nationaux «communiquent à tous les autres administrateurs nationaux et à l'administrateur central[7], par des moyens sécurisés», le nom et l'identité des personnes auxquelles ils ont refusé l'ouverture d'un compte, ou qu'ils ont refusé de désigner comme représentants autorisés, ainsi que le nom et l'identité des titulaires et des représentants autorisés des comptes auxquels l'accès a été suspendu ou qui ont été clôturés en raison (entre autres) de certaines activités criminelles constatées ou présumées. Bien que le texte du règlement ne l'indique pas explicitement, selon les explications fournies par la Commission, cette disposition vise à réduire le risque que les titulaires de comptes (et leurs représentants) auxquels l'ouverture d'un compte a été refusée ou auxquels l'accès aux comptes a été suspendu ou clôturé en raison d'activités criminelles présumées puissent ultérieurement réintroduire avec succès une demande d'ouverture de compte dans un autre État membre. L'introduction d'une nouvelle demande dans un autre État membre après un refus ou une suspension n'est en soi pas interdite par le règlement. De même, le refus d'une demande précédente dans un État membre n'exclut pas la possibilité de l'acceptation d'une demande ultérieure dans un autre État membre. Toutefois, pour décourager toute forme de forum shopping et garantir une coopération efficace, le règlement a mis en place un mécanisme d'échange d'informations qui, en fait, fonctionne comme une liste noire et alerte les administrateurs nationaux sur l'éventuelle nécessité d'un examen plus minutieux de toute demande provenant des personnes ou organisations concernées[8].

27. L'article 83, paragraphes 2 à 6, du règlement octroie à Europol un accès direct au registre de l'Union et à l'EUTL. Certains autres tiers, dont les autorités répressives et fiscales, disposent d'un accès sur demande (pour plus de détails, voir section 7).

[7] En ce qui concerne l'administrateur central, voir section 5.
[8] Voir la section 10 contenant une recommandation spécifique par rapport à cette liste noire.

4. Précisions requises sur les données à caractère personnel traitées en vertu du règlement

Les données à caractère personnel sont-elle archivées et échangées dans ou hors du cadre du registre de l'Union?

28. Le règlement ne spécifie pas si une partie des données à caractère personnel traitées en relation avec la gestion de compte sera également enregistrée dans le registre de l'Union. Il ne précise pas non plus si les échanges d'informations entre les administrateurs nationaux et la Commission se font dans ou hors du cadre du registre de l'Union et de l'EUTL. Sur la seule base du texte du règlement, il n'est donc pas clairement établi si des données sensibles sont enregistrées et archivées dans le registre de l'Union et l'EUTL.

29. Cette précision revêt une importance cruciale, étant donné que l'article 81, paragraphe 1, du règlement prévoit que les données enregistrées dans le registre de l'Union sont conservées pendant quinze ans. Il s'agit d'une longue période de conservation, susceptible de ne pas être appropriée pour le stockage de plusieurs catégories de données sensibles[9].

30. Sur la base des informations complémentaires fournies par la Commission, il apparaît qu'un grand nombre de données collectées lors de l'ouverture d'un compte — par exemple les copies récentes des extraits de casier judiciaire ou les copies des passeports, cartes d'identité et documents apportant la preuve de résidence — ne sont pas téléchargées dans le registre de l'Union mais traitées et archivées au niveau local par les administrateurs nationaux, dans le respect des lois nationales régissant la protection des données.

31. En ce qui concerne les contenus de casiers judiciaires, il semble qu'aucune information ne soit systématiquement téléchargée dans le registre de l'Union. Toutefois, la possibilité qu'un administrateur national puisse introduire, par exemple, dans le champ «commentaire» de la base de données une note indiquant les raisons du refus de l'ouverture d'un compte, ne peut être exclue. En ce qui concerne les documents d'identité, il apparaît que les dates d'expiration et les numéros de carte d'identité ou de passeport sont téléchargés dans le registre de l'Union, mais pas les copies des documents eux-mêmes.

32. Il apparaît également que le refus de l'ouverture d'un compte ou la suspension d'un compte peut être enregistré dans le registre de l'Union[10].

Éclaircissements sur le fait que le registre de l'Union et l'EUTL puissent contenir des données sensibles

33. Sur la base de ce qui précède, le CEPD recommande de revoir le texte du règlement afin d'y préciser clairement quelles sont les données traitées dans et hors du cadre du registre de l'Union et de l'EUTL. À cet effet, le CEPD accueillerait très favorablement l'introduction dans le règlement d'une disposition générale indiquant qu'aucune catégorie particulière de données à caractère personnel[11] — et, en

[9] Voir la section 9 concernant les délais de conservation.
[10] La Commission a expliqué qu'en tout état de cause, cette information n'est pas «transmise au niveau international» (voir la section 11 concernant les transmissions internationales de données).
[11] Voir l'article 8 de la directive 95/46/CE.

particulier, aucune donnée issue du casier judiciaire ou information concernant des activités de fraude ou autres activités criminelles constatées ou présumées — n'est enregistrée dans l'EUTL ou dans le registre de l'Union[12].

34. Toute exception à cette règle générale doit être spécifiquement indiquée et être nécessaire et proportionnée. Par exemple, comme indiqué au point 27, il semble que le refus de l'ouverture d'un compte ou la suspension d'un compte puisse être enregistré dans le registre de l'Union. Combinée au nom du titulaire du compte, qui peut être une personne physique, ou aux noms de ses représentants (par exemple, les directeurs), cette information peut constituer une donnée sensible. Cette exception et toute autre exception similaire devraient être dûment justifiées et spécifiquement mentionnées dans le règlement.

Utilisation de champs ouverts aux fins de commentaires

35. Comme indiqué au point 30, il apparaît que les informations concernant le casier judiciaire ne sont pas systématiquement téléchargées dans la base de données. Toutefois, comme expliqué au point 31, la possibilité qu'un administrateur national puisse introduire, par exemple, un commentaire dans la base de données indiquant les raisons du refus de l'ouverture d'un compte ne peut être exclue. Pour éviter cela, le CEPD recommande que le règlement interdise clairement l'utilisation de champs ouverts pour la saisie de données sensibles, sauf si nécessaire et proportionné aux fins de la gestion du registre de l'Union et spécifiquement autorisé par le règlement (voir point 34).

36. Au niveau pratique, le CEPD recommande que des instructions claires soient fournies aux utilisateurs du registre de l'Union (par le biais d'un menu d'aide, d'un message d'avertissement, de documents de formation et/ou d'une autre manière) pour indiquer qu'aucune information de ce type ne peut être saisie dans les champs prévus pour les commentaires.

Informations concernant les bénéficiaires effectifs

37. Le CEPD recommande également que le règlement précise clairement quelles seront les informations traitées en ce qui concerne les bénéficiaires effectifs (voir point 19).

5. L'administrateur central

38. Les articles 4 et 5 (lus en combinaison avec l'article 3, paragraphe 2, du règlement et l'article 20 de la directive 2003/87/CE) disposent qu'un administrateur central, désigné par la Commission, gère et tient à jour le registre de l'Union et l'EUTL.

39. Le règlement n'indique pas clairement si l'administrateur central proviendra de la Commission européenne, d'une autre institution/agence ou d'un autre organe de l'UE, ou encore, d'une entité organisée conformément à la législation d'un des États membres. Dans l'hypothèse où il s'agirait de deux entités différentes, les obligations respectives de la Commission et de l'administrateur central désigné par la Commission ne sont pas non plus clairement indiquées. Des éclaircissements sur ces points seraient nécessaires. En particulier, si l'intention est que la Commission agisse en tant qu'administrateur central, comme expliqué par la Commission au

[12] Ceci devrait également figurer clairement dans la politique de protection des données mentionnée aux points 41 à 43.

CEPD, cette information devrait aussi être précisée clairement dans le texte même du règlement.

40. Le CEPD recommande en outre qu'au niveau pratique, cette information figure clairement dans la documentation relative au système, y compris dans la politique de protection des données mentionnée aux points 41 à 43, ainsi que dans la partie accessible au public du site web du registre de l'Union.

6. Répartition des tâches et responsabilités: adoption d'une politique de protection des données

41. Des précisions, en termes de protection des données, seraient également bienvenues au sujet de la répartition des tâches et responsabilités entre les administrateurs nationaux et l'administrateur central.

42. Le CEPD recommande de préciser, dans un document de politique globale de protection des données relative au SCEQE ou dans un document similaire élaboré conjointement par la Commission et les administrateurs nationaux, les responsabilités de chaque entité, en mentionnant le régime de protection des données applicable dans chaque cas. Ce document pourrait indiquer, par exemple, qui est chargé d'informer les personnes concernées, qui a la responsabilité d'agir lorsqu'un accès, une rectification, un verrouillage ou un effacement est demandé par les personnes concernées, qui porte la responsabilité de la sécurité du registre de l'Union et de l'EUTL, et qui prend les décisions concernant leur conception.

43. L'obligation d'adopter un tel document pourrait être spécifiquement prévue par le règlement, de même que les principaux éléments de ce cadre.

7. Accès aux données octroyé à Europol et à d'autres tiers

44. L'article 83 du règlement traite de la confidentialité des informations contenues dans l'EUTL et dans le registre de l'Union. Il précise à qui et dans quelles circonstances les données peuvent être transmises. La règle par défaut, énoncée au paragraphe 1 dudit article, est que toutes les informations contenues dans l'EUTL et dans le registre de l'Union sont considérées comme confidentielles, «sauf disposition contraire du droit de l'Union ou de la législation nationale qui poursuit un objectif légitime compatible avec le présent règlement et qui est proportionnée».

45. Le reste de la disposition prévoit que certaines entités spécifiquement citées (entre autres, les services chargés de faire appliquer la loi et les autorités fiscales des États membres, l'Office européen de lutte antifraude, la Cour des comptes européenne et Eurojust) peuvent obtenir, sur demande, les données conservées dans le registre de l'Union et dans l'EUTL si ces données sont nécessaires à l'exécution de leurs tâches. L'article 83, paragraphe 5, mentionne spécifiquement que cette autorisation peut inclure l'accès «à des données de transaction anonymes afin de rechercher des types de transaction suspects». L'article 83, paragraphe 5, indique par ailleurs que ces entités elles-mêmes «peuvent signaler les types de transaction suspects aux autres entités énumérées» ci-dessus.

46. En outre, Europol bénéficie d'un accès permanent aux fins de l'exécution de ses tâches conformément à la décision 2009/371/JAI du Conseil portant création de l'Office européen de police. Europol doit tenir la Commission informée de l'utilisation qu'il fait des données.

47. Le CEPD recommande, premièrement, que les finalités de l'accès aux données par les entités énumérées, y compris Europol, soient définies plus en détail. La simple énumération des entités auxquelles des données peuvent être transmises ne constitue pas une «définition de la finalité» suffisante aux termes de la législation en matière de protection des données. Au lieu de fournir simplement une liste des entités, il serait peut-être approprié de préciser que l'accès aux données prévu par l'article 83 est limité aux cas où cela s'avère nécessaire et proportionné pour des finalités précisément définies et énoncées dans le règlement.

48. Le CEPD rappelle également que, en principe, toutes les finalités autorisées des transmissions de données à caractère personnel doivent être précisées et compatibles avec la finalité initiale pour laquelle les données ont été collectées. Toute extension à des éléments ne relevant pas du champ d'application du registre de l'Union (par exemple, le blanchiment de capitaux, le financement du terrorisme ou d'autres délits graves) devrait être assortie d'une justification complète et d'un cadre clair.

49. À cet égard, le CEPD relève que le règlement (UE) n° 920/2010, aujourd'hui modifié par le présent règlement, comportait une description plus spécifique des finalités dans la mesure où il mentionnait à l'article 75, paragraphe 3, la possibilité d'une transmission de données «si la demande est fondée et répond à des besoins d'enquête, de détection et de répression des fraudes, à des exigences de l'administration fiscale ou de recouvrement de l'impôt, de lutte contre le blanchiment de capitaux, le financement du terrorisme ou d'autres délits graves». Une formulation similaire, mais plus restrictive, serait en tout cas préférable à une simple liste des entités auxquelles des données peuvent être transmises, comme dans le règlement actuel. Par exemple, la formulation utilisée dans le règlement en relation avec les refus d'ouverture de comptes pourrait être reprise ici et laisserait suffisamment de flexibilité pour les autorités répressives et fiscales: les transferts de données pourraient donc être limités aux cas où ils sont nécessaires et proportionnés pour répondre à des besoins d'enquête, de détection et de répression des «fraudes concernant des quotas ou des unités de Kyoto, pour des opérations de blanchiment de capitaux ou de financement du terrorisme, ou pour d'autres délits graves pour lesquels le compte pourrait servir d'instrument».

50. Par ailleurs, en ce qui concerne l'accès à des «données de transaction anonymes afin de rechercher des types de transaction suspects», il importe de souligner que les données continueront d'être considérées comme des «données à caractère personnel» et seront par conséquent soumises à la législation en matière de protection des données aussi longtemps que les personnes pourront être indirectement identifiées. L'utilisation de «techniques d'anonymisation» ne signifie pas que les données sont considérées comme «rendues anonymes» au sens du considérant 26 de la directive 95/46/CE[13]. Une série de données peut contenir des données à caractère personnel et conduire à l'identification d'une personne, même après la suppression des identifiants directs et l'utilisation de diverses autres

[13] Considérant 26: «pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne».

«techniques d'anonymisation»[14]. Dans la mesure où les données concernant les titulaires de comptes sont enregistrées et conservées quinze ans dans le registre de l'Union et dans l'EUTL, il est peu probable qu'au cours de cette période de conservation, toute donnée relative aux transactions puisse être considérée comme strictement anonyme en ce sens qu'elle ne permet pas la réidentification des personnes à l'origine de ces transactions. En outre, si l'objectif de cette disposition est de permettre aux services répressifs — après avoir détecté un «type de transaction suspect» — d'identifier les titulaires de compte concernés pour pouvoir enquêter et engager des poursuites contre eux ou les personnes ayant agi en leur nom, cet objectif nécessite alors en soi l'identification ultérieure des personnes concernées.

51. Le CEPD recommande une formulation plus claire du règlement, de manière à éviter tout malentendu sur ce point. Il conviendrait également d'ajouter des garanties, dans le règlement et en tout cas au niveau pratique, prévoyant l'application de techniques d'anonymisation adéquates avant le transfert en masse de données relatives aux transactions, pour ce qui constitue essentiellement une exploration des données. En plus de la pseudonymisation (par exemple, par le codage des données des titulaires de comptes), d'autres techniques d'anonymisation peuvent s'avérer nécessaires si la pseudonymisation seule n'est pas suffisamment efficace, par exemple parce qu'il existe un risque que malgré la pseudonymisation, il demeure possible de rattacher des transactions à une même personne[15].

52. En ce qui concerne l'anonymisation, le CEPD estime que compte tenu de l'accès direct au registre de l'Union et à l'EUTL dont bénéficie Europol, il conviendrait également de prévoir des dispositions spécifiques garantissant qu'Europol ne pourra accéder aux données à caractère personnel qu'après l'application de techniques d'anonymisation adéquates.

53. Enfin, le CEPD souligne que l'obligation de confidentialité énoncée au paragraphe 1 de l'article 83 du règlement devrait s'appliquer aux données à caractère personnel contenues dans le registre de l'Union et dans l'EUTL, mais aussi à toutes les données à caractère personnel détenues en dehors de ces bases de données et nécessitant un traitement en vertu du règlement. La confidentialité est importante vis-à-vis des données à caractère personnel traitées au niveau local par les administrateurs nationaux ainsi que vis-à-vis des données échangées entre les administrateurs nationaux et la Commission, notamment — mais pas uniquement — dans le contexte de la liste noire mentionnée au point 26 et abordée de manière plus approfondie à la section 10.

8. Publication de données à caractère personnel sur l'Internet

54. Dans un but de transparence, la partie accessible au public du site web du registre de l'Union affiche certaines informations, dont un nombre limité de données à caractère personnel (par exemple, les informations de contact) concernant les titulaires de comptes et leurs représentants. Certaines de ces informations sont obligatoires, d'autres facultatives. L'article 83, paragraphes 8 et 10, dispose que les

[14] Voir pages 15 à 20 de l'avis du groupe de travail «article 29» sur le concept de données à caractère personnel (WP 136). Voir également les points pertinents de plusieurs avis du CEPD, par exemple, la section 3.1 de l'avis du CEPD du 3 septembre 2010 sur la notification d'un contrôle préalable concernant le système européen de surveillance (TESSy).

[15] Voir page 18 de l'avis du groupe de travail «article 29», précité à la note de bas de page 14.

titulaires de comptes peuvent accepter ou s'opposer à la publication de certaines données à caractère personnel les concernant ou concernant leurs directeurs.

55. En effet, chacune des annexes II, IV, VI, VII et XII spécifie, pour chaque information, i) ce qui est publié sur le site web, ii) ce qui ne l'est pas, iii) ce qui est publié uniquement sur demande expresse (opt-in) et iv) ce qui est publié sauf opposition expresse (opt-out).

56. Le CEPD se réjouit de ces clarifications et n'a pas d'autres commentaires à formuler en ce qui concerne les catégories de données qui devraient être publiées et celles qui ne devraient pas l'être, ou en ce qui concerne le type de consentement requis dans chaque cas.

57. LE CEPD serait toutefois favorable à l'insertion dans le règlement d'une disposition générale indiquant qu'aucune donnée à caractère personnel autre que celles spécifiquement prévues dans le règlement ne sera accessible au public par le biais du site web.

9. Délai de conservation

Introduction et remarques générales

58. L'article 81, paragraphe 1, du règlement, prévoit que «[l]e registre de l'Union et tous les autres registres PK [protocole de Kyoto] conservent les archives relatives à tous les processus, aux données du journal et aux titulaires de comptes pendant quinze ans ou aussi longtemps que des questions de mise en œuvre y ayant trait restent pendantes».

59. Le CEPD a constaté que les exigences en matière de stockage des données ont été établies conformément aux normes d'échange de données de la convention-cadre des Nations unies sur les changements climatiques, adoptée par toutes les parties au protocole de Kyoto, y compris l'Union européenne et tous ses États membres[16].

60. Le CEPD recommande néanmoins de clarifier davantage l'article 81, paragraphe 1, en rappelant que les exigences en matière de conservation des données sont conformes à la législation de l'UE en matière de protection des données, qui prévoit que les données à caractère personnel doivent être conservées «pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement»[17].

61. Compte tenu des exigences de protection des données, mais aussi des obligations internationales au titre du protocole de Kyoto, le CEPD recommande que le règlement définisse plus clairement les catégories de données à caractère personnel qui doivent être conservées pendant quinze ans et celles auxquelles ce délai de conservation ne s'applique pas.

[16] Voir les normes d'échange de données entre les systèmes de registres au titre du protocole de Kyoto, spécifications techniques (version 1.1.8), en particulier la section 7 relative aux «normes d'archivage des données» (page 66), accessibles en ligne à l'adresse - http://unfccc.int/files/kyoto_mechanisms/registry_systems/application/pdf/des_full_ver_1.1.8.pdf.
[17] Voir l'article 6, paragraphe 1, point e), de la directive 95/46/CE.

62. En outre, pour les catégories de données à caractère personnel auxquelles ce délai de conservation ne s'applique pas (par exemple, parce qu'elles sont traitées en dehors du registre de l'Union), il conviendrait que le règlement fixe des délais de conservation spécifiques appropriés ou — si cela est suffisant — exige au moins la fixation de délais de conservation adéquats selon les lois nationales, conformément aux règles nationales qui transposent la directive 95/46/CE.

Principales préoccupations concernant la conservation des données: données sensibles, notamment les données issues du casier judiciaire et les données concernant des infractions présumées

63. Après analyse, le CEPD recommande particulièrement à la Commission de se pencher spécifiquement sur la question des informations issues du casier judiciaire (y compris toute information ou «commentaire» figurant dans la base de données au sujet du contenu de ce casier judiciaire, par exemple, en cas de refus d'ouverture de compte ou de suspension de l'accès à un compte). En vertu du droit national, à l'expiration de délais déterminés, les données issues du casier judiciaire sont systématiquement effacées des bases de données relatives aux casiers judiciaires gérées par les États membres. Dès lors, une règle générale imposant le stockage des informations issues du casier judiciaire d'un titulaire de compte ou d'un directeur pendant quinze ans — ce qui peut être longtemps après la suppression de ces informations dans la base de données de l'État membre concerné — serait excessive.

64. Le CEPD est également préoccupé par le délai de conservation des données relatives aux titulaires de comptes, représentants ou directeurs faisant l'objet d'enquêtes, surtout si ceux-ci ont été innocentés par la suite. Un tel cas pourrait se produire, par exemple, si la demande d'ouverture d'un compte introduite par une entité a été refusée alors que cette entité faisait l'objet d'une enquête pour fraude concernant des quotas ou des unités de Kyoto. Pour ne citer qu'un exemple, l'article 20, paragraphe 2, point b), du règlement dispose qu'un administrateur peut refuser d'ouvrir un compte «si le titulaire de compte potentiel ou, s'il s'agit d'une personne morale, l'un des directeurs, fait l'objet d'une enquête ou a été condamné au cours des cinq dernières années pour fraude concernant des quotas ou des unités de Kyoto, pour blanchiment de capitaux, financement du terrorisme ou pour d'autres délits graves pour lesquels le compte pourrait servir d'instrument». Cette disposition est complétée par l'article 83, paragraphe 7, qui exige que «[l]es administrateurs nationaux communiquent à tous les autres administrateurs nationaux et à l'administrateur central, par des moyens sécurisés, le nom et l'identité des personnes auxquelles ils ont refusé l'ouverture d'un compte conformément à l'article 20, paragraphe 2, [...]».

65. Par rapport à de telles données, la fixation de délais de conservation adéquats et non excessifs est clairement nécessaire, que ces données soient traitées dans ou hors du cadre du registre de l'Union.

66. Pour répondre à ces préoccupations, le CEPD recommande que le règlement précise clairement les délais de conservation des données relatives aux titulaires de comptes et à leurs représentants, et en particulier le délai de conservation des données issues du casier judiciaire ou des informations concernant des enquêtes ou suspicions. Les règles suivantes seraient éventuellement appropriées:

- pour les données collectées et traitées en dehors de l'EUTL et du registre de l'Union, le règlement pourrait préciser que ces données seront soumises à l'application de délais de conservation proportionnés, spécifiés conformément aux règles nationales qui transposent la directive 95/46/CE;
- si des données sensibles sont traitées dans le cadre du registre de l'Union ou de l'EUTL, ou si des données sensibles sont échangées par l'intermédiaire d'un autre mécanisme formalisé d'échange de données entre les administrateurs nationaux et l'administrateur central, le règlement devrait fixer spécifiquement des délais de conservation adéquats et non excessifs, après consultation avec les États membres. La définition d'un cadre complet et cohérent pour la conservation des données est particulièrement importante pour les listes noires périodiquement mises à jour des titulaires de comptes ou représentants suspectés d'activités criminelles, dont l'établissement est prévu par l'article 83, paragraphe 7, du règlement.

Préoccupations d'ordre secondaire

67. Le CEPD juge douteuse la nécessité de conserver pendant quinze ans des adresses depuis longtemps invalides ainsi que des numéros de téléphone, numéros de passeport ou dates de naissance de directeurs qui ne sont plus en fonction dans les entreprises concernées. Pour ces catégories de données, des délais de conservation plus courts pourraient sans doute être fixés.

Début du délai de conservation

68. Le CEPD recommande également que la Commission indique clairement le début des délais de conservation et précise, par exemple, s'il s'agit de la date de téléchargement des informations dans la base de données électronique.

10. Garanties supplémentaires pour les échanges de données prévus par l'article 83, paragraphe 7: établissement d'une liste noire des titulaires de comptes et des représentants pour activités criminelles constatées ou présumées

69. Les listes noires prévues par l'article 83, paragraphe 7, du règlement[18] requièrent l'application, au niveau pratique, de garanties adéquates en matière de protection des données. Dans le règlement lui-même, il conviendrait en outre de préciser que:
- les personnes concernées doivent être dûment averties de leur mise sur liste noire;
- un mécanisme doit être prévu pour accéder aux demandes des personnes concernées concernant l'accès, la rectification, le verrouillage ou l'effacement de données;
- un mécanisme doit être prévu pour garantir que les informations figurant dans la liste noire sont exactes et à jour;
- toutes les données à caractère personnel doivent être supprimées dès que leur conservation n'est plus nécessaire (voir également le point 66 ci-dessus);
- l'accès à la liste noire doit être clairement limité aux administrateurs nationaux et à l'administrateur central et réservé à des finalités spécifiques liées à la gestion du compte, telles que la prévention du forum shopping (toute exception, si autorisée, doit être clairement mentionnée dans le règlement et dûment justifiée).

[18] Voir point 26 ci-dessus.

11. Transferts de données dans le relevé international des transactions

70. L'article 6, paragraphe 1, du règlement dispose que le registre de l'Union est relié au relevé international des transactions («ITL») de la convention-cadre des Nations unies sur les changements climatiques (CCNUCC) par un lien de communication qui permet de transmettre les transactions consistant en transferts d'unités de Kyoto.

71. L'article 6, paragraphe 2, prévoit également que l'EUTL est également relié à l'ITL par un lien de communication qui permet d'enregistrer et de contrôler les transferts visés au paragraphe 1.

72. Compte tenu de ces liens de communication et, partant, de l'échange de données résultant de ces arrangements, le CEPD recommande que le règlement précise quelles sont, le cas échéant, les données à caractère personnel transférées dans l'ITL. Le CEPD recommande en tout cas que le règlement indique spécifiquement qu'aucune catégorie particulière de données ne sera transférée dans l'ITL.

73. Par exemple, comme indiqué au point 32, il semble que le refus de l'ouverture d'un compte ou la suspension d'un compte soit enregistré dans le registre de l'Union. Combinée au nom du titulaire du compte, qui peut être une personne physique, ou aux noms de ses représentants (par exemple, les directeurs), cette information peut constituer une donnée sensible. Dans de tels cas et dans des situations similaires, l'interdiction de transfert pourrait s'appliquer.

12. Sécurité des données

74. En matière de sécurité, l'article 4, paragraphe 4, du règlement dispose que «[l]e registre de l'Union est conforme aux spécifications fonctionnelles et techniques des normes d'échange de données entre les systèmes de registres au titre du protocole de Kyoto, élaborées conformément à la décision 12/CMP 1, et il répond aux exigences en matière de matériel informatique, de réseau, de logiciel et de sécurité définies dans les spécifications techniques pour l'échange des données prévues à l'article 79».

    L'article 79, paragraphe 2, du règlement prévoit quant à lui que «[l]es spécifications techniques pour l'échange des données sont élaborées en concertation avec le groupe de travail des administrateurs du comité des changements climatiques et sont compatibles avec les spécifications fonctionnelles et techniques des normes d'échange de données entre les systèmes de registres au titre du protocole de Kyoto, élaborées conformément à la décision 12/CMP 1».

75. Dans l'hypothèse où l'administrateur central proviendrait de la Commission ou d'une autre institution, agence ou d'un autre organe de l'UE, le CEPD recommande qu'il soit également fait référence aux dispositions pertinentes du règlement (CE) n° 45/2001 (articles 22 et 23).

76. En outre, le CEPD recommande que le règlement lui-même contienne un ensemble minimal de garanties en termes de sécurité. Il pourrait notamment être précisé que:

- le registre de l'Union et l'EUTL sont gérés conformément à un plan de sécurité spécifique au système, élaboré après une évaluation complète des risques et en

tenant compte des normes internationales et des meilleures pratiques dans les États membres; et que

- le plan de sécurité et son application font périodiquement l'objet d'un audit par un tiers indépendant.

13. Conclusions

77. Le CEPD formule les recommandations suivantes en vue de la modification du règlement, prévue en 2012, et suggère que le règlement:

- indique plus clairement les données à caractère personnel qui seront traitées en vertu du règlement ainsi que les données à caractère personnel qui seront stockées et traitées dans le registre de l'Union et l'EUTL. En particulier, le CEPD accueillerait favorablement l'introduction dans le règlement d'une disposition générale indiquant qu'aucune catégorie particulière de données à caractère personnel ne sera enregistrée dans l'EUTL et dans le registre de l'Union (section 4);
- indique clairement si l'administrateur central proviendra de la Commission européenne, d'une autre institution/agence ou d'un autre organe de l'UE, ou encore, d'une entité organisée conformément à la législation d'un des États membres (section 5).
- exige l'adoption d'une politique de protection des données pour l'attribution des tâches et responsabilités (section 6);
- définisse plus spécifiquement les finalités de l'accès aux données par les tiers, y compris Europol, et prévoie des garanties adéquates pour l'anonymisation en cas d'exploration des données (section 7);
- interdise la publication des données sensibles (section 8);
- modifie les délais de conservation afin de garantir que les exigences en matière de conservation des données soient conformes à la législation de l'UE en matière de protection des données (section 9);
- impose que les personnes concernées soient dûment averties de leur mise sur liste noire et qu'un mécanisme soit mis en place pour garantir les droits d'accès des personnes concernées et vérifier que les informations figurant dans la liste noire sont exactes et à jour; fixe des délais de conservation adéquats, des restrictions à l'accès et aux finalités pour lesquelles la liste noire peut être utilisée (section 10);
- interdise les transmissions de données sensibles à l'extérieur de l'Union européenne et en particulier dans le relevé international des transactions (section 11);
- apporte des éclaircissements supplémentaires sur la sécurité et la responsabilité (audits) (section 12).

78. Le CEPD invite en outre la Commission et les États membres à tenir compte de ses commentaires dans la mise en œuvre, au niveau pratique, des garanties nécessaires en matière de protection des données. Cela pourrait se concrétiser par l'adoption d'une politique de protection des données, par la publication d'informations sur le site web du registre de l'Union, ainsi que par d'autres mesures pratiques, telles que la production de menus d'aide, de messages d'avertissement dans le registre de l'Union et de documents de formation.

Fait à Bruxelles, le 11 mai 2012

(**signé**)

Giovanni BUTTARELLI
Contrôleur adjoint européen de la protection des données