

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du Contrôleur européen de la protection des données sur une proposition de règlement du Parlement européen et du Conseil portant création d'une ordonnance européenne de saisie conservatoire des comptes bancaires, destinée à faciliter le recouvrement transfrontalier de créances en matière civile et commerciale

(2011/C 373/03)

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

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

1. Le 25 juillet 2011, la Commission a adopté une proposition de règlement du Parlement européen et du Conseil portant création d'une ordonnance européenne de saisie conservatoire des comptes bancaires (ci-après «OESC»), destinée à faciliter le recouvrement transfrontalier de créances en matière civile et commerciale ⁽³⁾.
2. La proposition a été envoyée au CEPD conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001 le jour même de son adoption. Le CEPD a été consulté de manière informelle avant l'adoption de la proposition. Il s'est félicité de cette consultation informelle et il note avec satisfaction que la quasi-totalité de ses observations ont été prises en considération dans la proposition finale.
3. Dans le présent avis, le CEPD expliquera et analysera brièvement les aspects de protection des données contenus dans la proposition.

II. LES ASPECTS DE PROTECTION DES DONNÉES CONTENUS DANS LA PROPOSITION

II.1. Les activités de traitement des données entreprises dans le cadre de la proposition de règlement

4. La proposition de règlement instituera une procédure européenne de mesures conservatoires qui permettra à un créancier («le demandeur») d'obtenir une ordonnance européenne de saisie conservatoire des comptes bancaires (ci-après «OESC») pour empêcher le retrait ou le transfert de fonds détenus par le débiteur («le défendeur») sur un compte bancaire situé dans l'Union européenne. La proposition vise à améliorer la situation actuelle dans laquelle, en raison de procédures «lourdes, longues et onéreuses», les débiteurs peuvent aisément échapper aux mesures d'exécution en transférant rapidement leurs fonds d'un compte bancaire dans un État membre à un autre ⁽⁴⁾.
5. Les données à caractère personnel sont traitées de diverses manières et transférées entre différents acteurs au titre de la proposition de règlement. Une distinction importante est établie entre deux situations. En premier lieu, la situation dans laquelle une OESC est sollicitée avant l'engagement d'une procédure judiciaire ou dans laquelle une décision, une transaction judiciaire ou un acte authentique n'a pas encore été déclaré exécutoire dans l'État membre d'exécution ⁽⁵⁾. En second lieu, la situation dans laquelle une OESC est sollicitée après l'obtention d'une décision, d'une transaction judiciaire ou d'un acte authentique exécutoires.
6. Dans la première situation, les données à caractère personnel du demandeur et du défendeur (informations d'identification, détails du compte bancaire du défendeur, description des circonstances pertinentes et preuves du comportement) sont communiquées par le demandeur à la juridiction nationale devant laquelle la procédure au fond de l'affaire a été introduite conformément aux règles applicables sur la compétence. La demande est présentée au moyen du formulaire dont le modèle figure à l'annexe I de la proposition (voir article 8 de la proposition).

⁽⁴⁾ Voir l'exposé des motifs de la proposition, p. 4.

⁽⁵⁾ La notion d'«acte authentique» est définie à l'article 4, paragraphe 11, de la proposition comme étant «un acte dressé ou enregistré officiellement en tant qu'acte authentique dans un État membre et dont l'authenticité: a) porte sur la signature et le contenu de l'acte, et b) a été établie par une autorité publique ou toute autre autorité habilitée à cet effet.»

⁽¹⁾ JO L 281 du 23.11.1995, p. 31.

⁽²⁾ JO L 8 du 12.1.2001, p. 1.

⁽³⁾ Voir COM(2011) 445 final.

7. Dans la seconde situation, le demandeur envoie les données à caractère personnel du défendeur (informations d'identification, détails du compte bancaire du défendeur et copie de la décision, de la transaction judiciaire ou de l'acte authentique) soit à la juridiction qui a prononcé la décision ou la transaction judiciaire soit, lorsqu'il s'agit d'un acte authentique, à l'autorité compétente de l'État membre dans lequel l'acte authentique a été dressé, ou directement à l'autorité compétente de l'État membre d'exécution. La demande est présentée au moyen du formulaire dont le modèle figure à l'annexe I de la proposition (voir article 15 de la proposition).
 8. Dans les deux situations, le demandeur doit fournir toutes les informations relatives au défendeur et au(x) compte(s) bancaire(s) de ce dernier nécessaires pour permettre à la banque ou aux banques d'identifier ce défendeur et son/ses compte(s) (voir article 16 de la proposition). Pour les personnes physiques, ces informations comprennent le nom complet du défendeur, le nom de la banque, le ou les numéros de compte, l'adresse complète du défendeur et sa date de naissance ou son numéro de carte nationale d'identité ou de passeport. Ces informations figurent sur le formulaire dont le modèle figure à l'annexe I (voir point 4.7 de l'annexe I). Les champs de données indiqués comme étant facultatifs dans le formulaire sont le numéro de téléphone et l'adresse électronique du défendeur (voir point 3 de l'annexe I).
 9. Lorsque le demandeur ne dispose pas de toutes les informations concernant un compte bancaire, il peut demander à l'autorité compétente de l'État membre d'exécution qu'elle obtienne les informations nécessaires, conformément à l'article 17 de la proposition. Cette demande est formulée dans la demande d'OESC et comprend «toutes les informations dont dispose le demandeur», relatives au défendeur et aux comptes bancaires de ce dernier (voir article 17, paragraphes 1 et 2). La juridiction ou l'autorité d'émission délivre l'OESC et le transmet à l'autorité compétente de l'État membre d'exécution qui utilise «tous les moyens appropriés et raisonnables existant dans l'État membre d'exécution pour obtenir les informations» (article 17, paragraphes 3 et 4). Les méthodes d'obtention d'informations sont l'une des suivantes: la possibilité d'obliger toutes les banques établies sur leur territoire de déclarer si le défendeur détient un compte auprès d'elles et l'accès par l'autorité compétente aux informations lorsque celles-ci sont détenues par des autorités ou administrations publiques et sont consignées dans des registres ou sous une autre forme (article 17, paragraphe 5).
 10. À l'article 17, paragraphe 6, il est souligné que les informations visées à l'article 17, paragraphe 4, doivent être «adéquates aux fins d'identification du ou des comptes du défendeur, pertinentes et non excessives et être limitées a) à l'adresse du défendeur, b) à la ou aux banques gérant le ou les comptes du défendeur, c) à ou aux numéros de compte du défendeur».
 11. Plusieurs dispositions de la proposition comprennent l'échange transfrontalier d'informations, y compris de données à caractère personnel. En ce qui concerne la transmission de l'OESC de la juridiction ou de l'autorité d'émission à l'autorité compétente de l'État membre d'exécution, elle est effectuée au moyen du formulaire dont le modèle figure à l'annexe II de la proposition (voir articles 21 et 24 de la proposition). Ce formulaire contient moins d'informations sur le défendeur étant donné qu'il n'est fait aucune mention de la date de naissance du défendeur, de son numéro de carte nationale d'identité ou de passeport, de son numéro de téléphone ou de son adresse électronique. Il semble découler de différentes étapes décrites dans la proposition de règlement que cela est dû au fait, soit que le ou les numéros de compte du défendeur ont déjà été établis avec certitude, soit que cette information n'a pas encore été recueillie par l'autorité compétente de l'État membre d'exécution sur la base de l'article 17 de la proposition.
 12. L'article 20 porte sur la communication et la coopération interjuridictionnelles. Les informations relatives à l'ensemble des circonstances pertinentes peuvent être demandées directement ou par l'intermédiaire des points de contact du réseau judiciaire européen en matière civile et commerciale créé par la décision 2001/470/CE ⁽¹⁾.
 13. Dans les trois jours ouvrables suivant la réception de l'OESC, la banque informe l'autorité compétente de l'État membre d'exécution et le demandeur au moyen du formulaire dont le modèle figure à l'annexe III de la proposition (voir article 27). Ce formulaire demande les mêmes informations sur le défendeur que le formulaire exposé à l'annexe II. À l'article 27, paragraphe 3, il est indiqué que la banque peut transmettre sa déclaration par des moyens électroniques de communication sécurisés.
- ## II.2. Exigences relatives à la protection des données
14. Les diverses activités de traitement de données à caractère personnel couvertes par la proposition de règlement doivent être réalisées dans le respect des règles relatives à la protection des données visées dans la directive 95/46/CE et la législation nationale qui la transpose. Le CEPD note avec satisfaction que cette exigence a été rappelée au considérant 21 ainsi qu'à l'article 46, paragraphe 3, de la proposition. Le CEPD se félicite également que les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne soient mentionnés au considérant 20 de la proposition.
 15. Certaines informations relatives au demandeur et au défendeur sont indispensables au bon fonctionnement de l'OESC. Selon les règles relatives à la protection des données, seules des informations proportionnées et réellement nécessaires doivent être utilisées. Le CEPD note avec satisfaction que la Commission a sérieusement examiné la question de la proportionnalité et de la nécessité du traitement de données à caractère personnel aux fins de la proposition actuelle.

⁽¹⁾ JO L 174 du 27.6.2001, p. 25.

16. La liste restreinte de détails personnels requis aux articles 8, 15 et 16, ainsi que dans les annexes de la proposition, en est la première illustration. Le CEPD note avec satisfaction que le volume de données à caractère personnel diminue dans les différentes annexes qui suivent les différentes étapes de la procédure d'OESC. Dans l'ensemble, le CEPD n'a aucune raison de penser que les informations requises vont au-delà de ce qui est nécessaire aux fins de la proposition de règlement. À cet égard, le CEPD n'a que deux autres observations à formuler.
17. La première concerne les détails de l'adresse du demandeur dans les annexes de la proposition de règlement. Selon l'article 25 de la proposition, l'OESC est signifiée ou notifiée au défendeur, à l'instar de tous les documents soumis à la juridiction ou à l'autorité compétente en vue de l'obtention de l'ordonnance, ce qui semble inclure les informations visées aux annexes I, II et III. Aucune mention n'est faite de la possibilité pour le demandeur de demander le retrait des détails de son adresse des différents documents avant qu'ils ne soient envoyés au défendeur. Étant donné qu'il peut exister des situations dans lesquelles la divulgation des détails de l'adresse du demandeur au défendeur est susceptible d'entraîner le risque de faire subir au demandeur des pressions extrajudiciaires de la part du défendeur, le CEPD suggère au législateur d'inclure à l'article 25, la possibilité pour le demandeur de demander le retrait de ces détails des informations communiquées au défendeur.
18. La seconde observation porte sur les champs de données facultatives à l'annexe I concernant le numéro de téléphone et l'adresse électronique. Si ces informations sont incluses dans des champs de données qui peuvent être utilisés si d'autres informations de contact du défendeur sont manquantes, ce point mérite d'être clarifié. Dans le cas contraire, il semble n'y avoir aucune raison de conserver ces champs de données.
19. La référence explicite au principe de nécessité visé à l'article 16 et à l'article 17, paragraphes 1 et 6, de la proposition traduit également l'importance donnée par la Commission à la proportionnalité et à la nécessité du traitement de données à caractère personnel aux fins de la présente proposition. L'article 16 mentionne toutes les informations «nécessaires» à l'identification du défendeur, l'article 17, paragraphe 1, les informations «nécessaires» et l'article 17, paragraphe 6, reprend le libellé de l'article 6, paragraphe 1, point c), de la directive 95/46/CE qui dispose que les données doivent être adéquates, pertinentes et non excessives. Le CEPD est satisfait de ces dispositions étant donné qu'elles indiquent clairement que les données à caractère personnel doivent être collectées conformément au principe de nécessité. L'article 17 soulève néanmoins certaines questions.
20. L'article 17, paragraphe 2, exige du demandeur qu'il communique «toutes les informations dont dispose le demandeur», relatives au défendeur et aux comptes bancaires de ce dernier. Cette formulation large pourrait comprendre la transmission de tous types d'informations relatives au défendeur. Cette disposition ne précise pas que ces informations doivent être limitées aux informations nécessaires à l'identification du défendeur et à la détermination de ses comptes bancaires. Le CEPD recommande d'inclure cette limitation à l'article 17, paragraphe 2.
21. La mention à l'article 17, paragraphe 4, de «tous les moyens appropriés et raisonnables» pourrait comprendre des méthodes d'investigation portant gravement atteinte à la vie privée du défendeur. Cependant, lu en conjonction avec l'article 17, paragraphe 5, il devient évident que ces moyens sont limités aux deux méthodes décrites au point 9 du présent avis. Toutefois, afin d'éviter toute interprétation erronée de la portée des moyens dont dispose l'autorité compétente, le législateur pourrait envisager de remplacer la mention de «tous les moyens appropriés et raisonnables» par «une des deux méthodes visées au paragraphe 5».
22. Quant aux deux méthodes mentionnées à l'article 17, paragraphe 5, point b), le CEPD a des questions concernant la seconde. Cette méthode concerne l'accès par l'autorité compétente aux informations qui sont détenues par des autorités ou administrations publiques et qui sont consignées dans des registres ou sous une autre forme. À l'annexe I de la proposition, il est fait mention de «registres publics existants» (voir point 4 de l'annexe I). Dans un souci de clarté, il conviendrait d'expliquer la véritable signification de l'article 17, paragraphe 5, point b), de la proposition. Il conviendrait de souligner que non seulement les informations collectées devraient être nécessaires aux fins de la proposition de règlement mais également que les méthodes de collecte des informations devraient se conformer aux principes de nécessité et de proportionnalité.
23. En ce qui concerne la transmission transfrontalière des données entre les différentes entités concernées, le CEPD ne voit aucun problème particulier du point de vue de la protection des données. Seul l'article 27, paragraphe 3, de la proposition mérite une réflexion plus approfondie. Aux termes de ce dernier, les banques peuvent transmettre leur déclaration (au moyen du formulaire dont le modèle figure à l'annexe III) par des moyens électroniques de communication sécurisés. Le verbe «pouvoir» est utilisé étant donné que le recours à des moyens électroniques est une alternative à l'envoi de la déclaration par courrier ordinaire. Cette déduction résulte de l'annexe III. L'article 27, paragraphe 3, vise à permettre aux banques d'utiliser des moyens électroniques de communication, mais uniquement si ces moyens sont sécurisés. Le CEPD recommande au législateur de clarifier cette disposition, étant donné que le texte actuel pourrait être interprété comme rendant l'utilisation de moyens sécurisés facultative. L'article 27, paragraphe 3, pourrait être remplacé par: «La banque peut transmettre sa déclaration par des moyens électroniques de communication, à condition que ces moyens soient sécurisés conformément aux articles 16 et 17 de la directive 95/46/CE».

III. CONCLUSION

24. Le CEPD note avec satisfaction les efforts entrepris pour tenir compte des différents aspects de protection des données qui sont soulevés par la proposition d'instrument d'une OESC. Plus particulièrement, il apprécie l'application du principe de nécessité et les références qui y sont faites. Cependant, le CEPD estime que la proposition de règlement nécessite des améliorations et des clarifications supplémentaires. Le CEPD recommande:

- d'envisager d'inclure à l'article 25 la possibilité pour le demandeur de demander le retrait des détails de son adresse, des informations communiquées au défendeur;
- de retirer les champs de données facultatives de l'annexe I (le numéro de téléphone et l'adresse électronique du défendeur) si le véritable besoin de ces données n'est pas démontré;
- de limiter les informations fournies par le demandeur au titre de l'article 17, paragraphe 2, aux informations nécessaires à l'identification du défendeur et à la détermination de ses comptes bancaires;

- d'envisager de remplacer la mention à l'article 17, paragraphe 4, de «tous les moyens appropriés et raisonnables» par «une des deux méthodes visées au paragraphe 5»;
- d'expliquer ce que signifie «registres publics existants» à l'article 17, paragraphe 5, point b);
- de reformuler l'article 27, paragraphe 3, de la manière suivante: «La banque peut transmettre sa déclaration par des moyens électroniques de communication, à condition que ces moyens soient sécurisés conformément aux articles 16 et 17 de la directive 95/46/CE».

Fait à Bruxelles, le 13 octobre 2011.

Giovanni BUTTARELLI
Contrôleur adjoint européen de la protection des données