LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

PETER HUSTINX
CONTRÔLEUR

Président du Conseil de
l'Union européenne
Secrétariat général
Conseil de l'Union européenne
Rue de la Loi 175
1048 Bruxelles, Belgique

Bruxelles, le 14 février 2014
PH/ABu/mk/ D(2014)0375 **C2011-1104**

Objet: avancée sur le paquet de mesures pour une réforme de la protection des données

Monsieur,

Compte tenu des négociations en cours autour du paquet de mesures pour une réforme de la protection des données, et en particulier de la prochaine réunion du Conseil JAI les 3 et 4 mars, nous souhaitons attirer votre attention sur un certain nombre de points en suspens.

Il est nécessaire de moderniser le cadre européen actuel de la protection des données à caractère personnel pour remplir l'obligation qui incombe au législateur européen en vertu de l'article 16 du TFUE. Cette modernisation est également un élément essentiel de la garantie d'une protection efficace des droits fondamentaux des citoyens européens à la vie privée et à la protection des données à caractère personnel, énoncés aux articles 7 et 8 de la Charge des droits fondamentaux de l'UE[1].

Nous considérons que les règles européennes en matière de protection des données doivent être réformées de toute urgence afin d'apporter une plus grande cohérence et uniformité à la protection des données au sein de l'Union européenne, créant ainsi des conditions équitables, tant pour les acteurs du marché en ligne que pour les acteurs traditionnels. Les citoyens, quant à eux, méritent une protection plus efficace de leurs droits fondamentaux à la vie privée et à la

[1] Voir, entre autres, l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données du 7 mars 2012.

Adresse postale: rue Wiertz 60 – B-1047 Bruxelles, Belgique
Bureaux: rue Montoyer 30
Courriel: edps@edps.europa.eu – Site Internet: www.edps.europa.eu
Tél.: +32 (0) 2-283 19 00 – Fax: +32 (0) 2-283 19 50

protection des données, qui ne peut être garantie que si le cadre légal applicable est cohérent (c'est-à-dire couvre l'éventail le plus large possible d'entités et d'activités de traitement de données) et consistant (c'est-à-dire appliqué de façon aussi uniforme que possible dans l'ensemble des 28 États membres).
Nous notons avec satisfaction les efforts actuels de la présidence grecque du Conseil visant à progresser sur un certain nombre de points en suspens. Nous soutenons et nous réjouissons également de l'objectif qui consiste à obtenir un accord sur un mandat de négociation avec le Parlement européen avant la fin de la présidence grecque, et à conclure le processus de négociation avant fin 2014.

Toutefois, s'agissant d'un certain nombre d'éléments importants du paquet de mesures concernant la protection des données, il est clair qu'aucun compromis n'est encore en vue. Il semble même que l'acquis existant puisse être affaibli à certains égards (notamment le champ d'application de la proposition de règlement général sur la protection des données, désigné ci-après «le règlement général»), ce qui est encore plus préoccupant.

Compte tenu des discussions en cours, il nous semble utile de présenter la position du CEPD sur trois points fondamentaux en suspens liés à la proposition de règlement général. Il s'agit selon nous d'un élément essentiel de notre rôle de conseiller des institutions communautaires sur toutes les affaires liées au traitement de données à caractère personnel.

1. <u>Le champ d'application de la proposition de règlement général</u>

Nous avons compris que l'option d'exclure le secteur public du champ d'application du règlement général (ou au moins l'introduction d'exceptions et de dérogations étendues) était toujours à l'étude. À cet égard, nous tenons à souligner que ni la directive 95/46/CE relative à la protection des données, actuellement en vigueur, ni la Convention 108 du Conseil de l'Europe (à laquelle tous les États membres ont adhéré) ne fait de distinction entre les secteurs «privé» et «public».

Exclure le secteur public aurait donc pour effet de retarder considérablement le processus législatif, mais cela signifierait aussi un grand pas en arrière par rapport au cadre actuel de la protection des données. De plus, exclure le secteur public, ou prévoir de larges exonérations, ne semble ni justifié, ni nécessaire. Aujourd'hui, déjà, les règles en vigueur en matière de protection des données prévoient de vastes possibilités permettant aux organes du secteur public de traiter des données à caractère personnel, si nécessaire pour se conformer à une obligation légale ou pour des missions exécutées dans l'intérêt public, et ces possibilités seront maintenues en vertu de la proposition de règlement général.

De surcroît, les frontières entre les secteurs «public» et «privé» sont bien moins claires qu'il n'y paraît. Par exemple, le même type d'activités (telles que la fourniture de services de santé) peut être exercé par des entités privées dans un État membre et des organes publics dans un autre État membre, ou il peut exister un mélange des deux dans un seul et même État membre. **Des entités très similaires**, traitant les mêmes catégories de données à caractère personnel (telles que des hôpitaux ou universités), **peuvent être soumises au même ensemble de règles, peu importe qu'il s'agisse d'organes publics ou d'entités privées**.

Par ailleurs, les échanges de données entre des organes publics et des entités privées (qui sont la ligne de vie d'une économie moderne et se déroulent quotidiennement dans le contexte de l'externalisation ou de partenariats public/privé) ne peuvent fonctionner parfaitement que si le

même cadre légal s'applique. Dans de nombreux cas, des organes publics exercent des activités de marché. Les soumettre à des règles en matière de protection des données différentes de celles applicables aux opérateurs privés modifierait inévitablement les conditions équitables du marché intérieur.

Enfin, un tel vaste découpage du cadre européen en matière de protection des données à caractère personnel affaiblirait la position de force de l'Union européenne dans ses négociations avec des pays tiers, en particulier dans les cas où l'Union européenne a milité pour l'adoption d'un cadre juridique global en matière de protection des données. Il en serait de même si de vastes exemptions étaient prévues pour le secteur public, à moins qu'elles ne soient strictement nécessaires et restent limitées à des situations très spécifiques qui ne sont pas encore couvertes par les exceptions existantes.

2. Le principe du guichet unique

En termes simples, le principe du guichet unique signifie que, lorsque des données à caractère personnel sont traitées dans plusieurs États membres, une seule et unique autorité de contrôle doit être responsable du suivi des activités du responsable du traitement ou du sous-traitant dans l'ensemble de l'Union européenne, ainsi que de la prise des décisions afférentes. Aux termes de la proposition de règlement général, il devrait normalement s'agir de l'autorité nationale chargée de la protection des données de l'État membre dans lequel est situé l'«établissement principal» de l'entité traitant les données, également appelée «autorité chef de file». Selon nous, le rôle d'une autorité chef de file *ne* doit *pas* être perçu comme une compétence *exclusive*, mais plutôt comme un mode structuré de coopération avec d'autres autorités de contrôle compétentes, étant donné que l'«autorité chef de file» dépendra fortement de la contribution et du soutien des autres autorités de protection des données à différentes étapes du processus[2].

Le principe du guichet unique est un élément important de la proposition d'harmonisation du cadre légal de la protection des données. Il a été proposé par la Commission pour assurer une application cohérente, garantir la sécurité juridique et réduire la charge administrative pour les responsables du traitement et les sous-traitants qui agissent dans plusieurs États membres[3]. En outre, il réduit la fragmentation du paysage de la protection des données. Il est important pour les entreprises de pouvoir traiter (idéalement) avec un seul et même interlocuteur au lieu de (potentiellement) 28 autorités nationales de protection des données. Nous rappelons que le Conseil JAI a approuvé le principe en octobre 2013, précisant qu'il s'agissait (avec le mécanisme de contrôle de la cohérence) de «l'un des aspects essentiels de la proposition de la Commission».

En décembre dernier, le service juridique du Conseil a soulevé un certain nombre d'objections légales au principe du guichet unique, remettant en question sa compatibilité avec la Charte des droits fondamentaux de l'Union européenne, et en particulier avec l'article 47 de cette dernière qui prévoit le droit à une voie de recours effective devant un tribunal et un droit à un procès équitable, correspondant en substance aux articles 13 et 6, paragraphe 1, de la CEDH. La préoccupation principale semble être la question de la «proximité» entre l'autorité nationale chargée de la protection des données prenant une décision dans une affaire particulière et le citoyen individuel, qui est perçue comme «un aspect important de la protection des droits individuels».

[2] Voir l'avis du CEPD du 7 mars 2012, point 237.
[3] Préambule 97 de la proposition de la Commission.

Nous considérons que l'interprétation par le service juridique du Conseil du principe du guichet unique dépeint une **image injustement négative** des propositions actuellement étudiées. En effet, il nous semble possible de réconcilier le principe avec un niveau élevé de protection des droits fondamentaux des citoyens, y compris ceux protégés par l'article 47 de la Charte. Cette position repose sur un certain nombre de considérations, dont nous souhaiterions partager avec vous les plus importantes.

D'abord et avant tout, il est important de souligner qu'à ce jour, conformément à l'article 28, paragraphe 6, de la directive 95/46/CE, une autorité nationale chargée de la protection des données a toujours compétence pour exercer les pouvoirs dont elle est investie (notamment enquête sur des réclamations) sur le territoire de l'État membre dont elle relève. Toutefois, à moins que la plainte ne concerne un responsable du traitement (ou un sous-traitant) disposant d'un établissement ou d'un équipement dans ledit État membre[4], les pouvoirs réels de cette autorité nationale chargée de la protection des données en matière d'exécution de la législation afférente peuvent être limités en pratique. En effet, la nécessité d'appliquer, dans un cas particulier, le droit national d'un autre État membre et l'absence de possibilités d'enquêter ou d'imposer des sanctions lorsque le responsable du traitement / sous-traitant n'est pas physiquement présent rend le recours à l'autorité nationale chargée de la protection des données purement théorique et largement inefficace.

Par opposition, la proposition de règlement général assurerait un cadre juridique uniforme et mettrait en place un mécanisme garantissant une exécution efficace dans la pratique par les autorités nationales chargées de la protection des données. Tout d'abord, les citoyens bénéficieraient explicitement du droit de déposer une réclamation auprès de l'autorité locale chargée de la protection des données (ou devant toute autre autorité nationale) pour exercer leurs droits[5]. Mais plus fondamentalement, dans des affaires dans lesquelles une autorité de protection des données aurait actuellement des possibilités limitées, le nouveau règlement garantirait l'application effective par l'autorité chef de file dans le contexte du guichet unique (et en tirant profit du mécanisme de contrôle de la cohérence[6]), si nécessaire avec le soutien d'une autorité de protection des données à compétence locale. En outre, une personne aura toujours la possibilité de former un recours contre une entreprise établie dans son pays, devant ses juridictions nationales, en cas de violation présumée du règlement[7].

De ce point de vue, la proposition de règlement général aura un **impact très positif** sur les possibilités offertes aux individus pour faire exécuter leurs droits à la protection des données et constituera donc une **amélioration importante** dans la protection du droit à une voie de recours effective, tel que garanti à l'article 47 de la Charte.

La proposition de règlement général prévoit également le contrôle juridictionnel de décisions prises par des autorités de protection des données[8]. Lorsque le principe du guichet unique s'applique, une personne souhaitant contester une décision prise par l'autorité chef de file devra le faire devant une juridiction de l'État membre de l'autorité chef de file, ce qui, dans de nombreux cas, signifierait en pratique la nécessité de former un recours dans un autre État membre.

[4] C'est ce qui découle des règles relatives au droit applicable énoncées à l'article 4, paragraphe 1, point a), b) et c).
[5] Article 73, paragraphe 1, de la proposition.
[6] Chapitre VII de la proposition.
[7] Article 75 de la proposition.
[8] Article 73 de la proposition.

Dans ce contexte, nous considérons que le seul fait que les juridictions d'un État membre autre que le pays de résidence d'un citoyen puissent être saisies ne prive pas en soi le citoyen d'une protection juridictionnelle effective. En réalité, conformément à la directive 95/46/CE actuellement applicable, il est également possible que des citoyens souhaitant contester le traitement de données à caractère personnel par une entreprise exerçant dans de nombreux États membres soient contraints de s'adresser à une autorité spécifique et, s'ils souhaitent contester ses décisions, doivent former un recours dans ce même État membre[9]. À notre connaissance, il n'existe aucune raison de remettre en question cette spécificité du système actuel par rapport à la Charte des droits fondamentaux.

Il est également reproché au principe du guichet unique proposé de créer des obstacles excessifs pour les citoyens cherchant des remèdes juridiques du fait de la distance géographique, de la méconnaissance d'un système juridique étranger, du besoin d'engager et de mener une procédure dans une langue étrangère ou des coûts d'une telle procédure.

L'alternative proposée à cet égard semble être la création d'un organe communautaire doté d'une personnalité juridique qui jouerait le rôle du guichet unique. La mise en place d'une telle «agence de protection des données» au niveau européen pourrait effectivement être tentante sur le plan conceptuel. Mais elle nécessiterait une centralisation fondamentale de la structure décentralisée actuelle du contrôle de la protection des données, ce qui, à tout le moins, ne faciliterait pas le processus décisionnel dans un délai raisonnable.

Plus important encore, il ne semble pas nécessaire de garantir une meilleure protection des droits fondamentaux des citoyens.

Il est important de garder à l'esprit que, dans la plupart des cas, tous les acteurs impliqués (personnes concernées, responsable du traitement et autorité de protection des données) resteront domiciliés dans un seul et même pays. Par conséquent, le principe du guichet unique ne s'appliquerait que dans un nombre de cas relativement limité. En d'autres termes, bien que certains de ces cas puissent avoir un impact majeur, les cas dans lesquels des citoyens sont affectés par des décisions d'une autorité chef de file située dans un État membre autre que leur propre pays de résidence seraient en pratique **bien moins nombreux** que les cas «ordinaires» dans lesquels des décisions sont prises par l'autorité «nationale» chargée de la protection des données.

Enfin, le principe du guichet unique doit être considéré dans son propre contexte comme un élément important contribuant à l'efficacité globale et à la cohérence du futur cadre de la protection des données. Il ne fait aucun doute qu'un système bien plus uniforme de protection des données et une baisse des frais de procédure (la procédure serait en principe limitée à la juridiction de l'autorité chef de file, à savoir celle du principal établissement) seraient avantageux pour les entreprises au sein de l'Union européenne. Toutefois, une application plus cohérente d'un ensemble uniforme de règles de protection des données, comme cela serait le cas dans le cadre de la proposition de règlement général, **profiterait aussi aux citoyens**.

Par exemple, lorsqu'un citoyen est concerné par un traitement de données par un établissement (subsidiaire) dans son pays de résidence (et, éventuellement, par d'autres établissements), mais que toutes les décisions sont en réalité prises par l'établissement

[9] Voir, par exemple, l'affaire de Facebook et de l'autorité irlandaise chargée de la protection des données.

principal du responsable du traitement dans un autre État membre, la possibilité d'obtenir une décision unique d'une autorité de protection des données ou une décision de justice qui serait valable et exécutable dans tous ces différents États membres constituerait une amélioration considérable par rapport à la situation actuelle.

Sur le même principe, le guichet unique réduit aussi le risque de procédures parallèles et les conflits de juridiction en résultant, dans la mesure où une procédure dans l'État membre de l'autorité chef de file serait normalement suffisante pour exécuter les droits d'une personne dans l'ensemble de l'Union européenne.

Néanmoins, certaines questions liées au futur fonctionnement du guichet unique nécessitent de poursuivre la réflexion, et des détails importants doivent encore être élaborés ou définis plus précisément. Nous restons à votre disposition pour vous apporter toute assistance que vous jugerez utile dans le cadre de ce processus.

3. L'approche basée sur les risques et la responsabilité

Nous avons régulièrement soutenu et nous sommes réjouis de l'introduction du principe de la responsabilité[10] dans la proposition de règlement général, en vertu duquel le responsable du traitement doit adopter des politiques et mettre en œuvre des mesures appropriées pour garantir et être en mesure de démontrer la conformité aux règles en matière de protection des données, ainsi que veiller à l'efficacité des mesures[11]. Ce principe doit encourager les responsables du traitement à se concentrer sur la garantie d'une protection effective des citoyens, plutôt que sur l'application d'une approche consistant à «cocher des cases» dans le but de satisfaire à des exigences bureaucratiques.

La responsabilité signifie également que les efforts de conformité devraient principalement concerner les domaines dans lesquels ils sont le plus nécessaires, s'agissant, par exemple, de la sensibilité des données et des risques associés à un traitement spécifique. À cet égard, nous apprécions les efforts des différentes présidences du Conseil pour décrire de façon appropriée la notion de «risque», qui implique nécessairement une mesure de jugement. Dans l'intérêt de la sécurité juridique, la proposition de règlement général devrait fournir des critères suffisamment clairs encadrant la réalisation d'une telle évaluation des risques par les responsables du traitement, notamment des facteurs objectifs (tels que le nombre de personnes affectées par un traitement spécifique) et des notions plus subjectives (par exemple les effets potentiellement négatifs sur la vie privée d'une personne). Sur la base de ces critères généraux énoncés dans la proposition de règlement général, d'autres conseils devraient être donnés par le comité européen de la protection des données ou dans des actes délégués, le cas échéant. Une telle approche garantirait une plus grande sécurité juridique pour les responsables du traitement, une protection plus efficace pour les citoyens européens et une flexibilité suffisante à l'épreuve du temps.

[10] Voir l'avis n°3/2010 du groupe de travail «Article 29» du 13 juillet 2010 sur le principe de la responsabilité (WP 173).
[11] Article 22 de la proposition.

Nous restons à votre disposition pour vous apporter tous conseils supplémentaires sur les points susvisés, ainsi que sur d'autres éléments en discussion/à l'étude, si vous le jugez utile pour faire avancer le processus de réforme.

Une copie du présent courrier/de la présente lettre a été envoyée à la représentation permanente des États membres, à M. Juan Fernando LÓPEZ AGUILAR, président du comité LIBE du Parlement européen, et à Mme Viviane REDING, vice-présidente de la Commission européenne.

Veuillez croire, cher Monsieur, à l'assurance de ma considération distinguée.,

(**signé**)

Peter HUSTINX