GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

01574/12/FR

WP199

Avis 08/2012 apportant des contributions supplémentaires au débat sur la réforme de la protection des données

adopté le 5 octobre 2012

Introduction

Depuis l'adoption des instruments relatifs à la réforme de la protection des données, le 25 janvier 2012, le Conseil et le Parlement européen ont lancé leurs procédures respectives dans le cadre du processus législatif.

Le Parlement européen

Le Parlement européen a confié à la commission LIBE la responsabilité principale pour les deux propositions examinées et a nommé deux rapporteurs, MM. Jan Albrecht et Dimitrios Droutsas. Les autres commissions parlementaires concernées sont les commissions IMCO, ITRE, ECON, JURI et EMPL.

Le paquet de réforme a déjà fait l'objet de plusieurs débats au sein de la commission LIBE et avec les rapporteurs fictifs (membres des autres groupes politiques chargés de suivre ce projet de réforme). Le 29 mai 2012, les rapporteurs ont également organisé une réunion des parties prenantes portante sur la proposition de règlement. La commission LIBE a organisé, les 9 et 10 octobre 2012, une réunion interparlementaire avec des membres des parlements nationaux, afin de débattre des instruments législatifs proposés dans le cadre de cette réforme. La commission LIBE prévoit de présenter ses projets de rapports sur la réforme avant la fin de l'année 2012. De même, les autres commissions concernées seraient alors tenues de présenter aussi leurs propres projets d'avis avant la fin de l'année.

Lors de la réunion de la commission LIBE de juin 2012, les rapporteurs ont présenté un premier document de travail soulignant les principaux éléments de la réforme, préconisant une approche globale (pour «*mettre en place deux instruments juridiques bien ordonnés et cohérents de haut niveau en adoptant, pour les deux textes, une procédure globale, parallèle, équilibrée et coordonnée*») et mettant en évidence plusieurs thèmes nécessitant de plus amples débats et clarifications.

1. le rôle conféré à la Commission dans le cadre des actes délégués et des actes d'exécution ainsi que du mécanisme de contrôle de la cohérence;
2. le fait que, pour l'heure, les institutions et agences de l'Union soient exclues du champ d'application de la réforme de la protection des données;
3. la façon dont sont liés le droit général de l'Union et les droits nationaux spécifiques;
4. le partage exact des rôles et des responsabilités entre les autorités de protection des données en ce qui concerne les flux transfrontières;
5. les éclaircissements concernant le profilage, exigés par le Parlement, notamment en ce qui concerne le facteur humain et le droit à être informé de la logique présidant au traitement des données;
6. les notions d'«intérêt légitime», d'«intérêt général» et de «sécurité publique»;

7. la corrélation entre les deux instruments législatifs, notamment en ce qui concerne l'accès des autorités répressives aux données à caractère personnel détenues par des entités privées;
8. des demandes ou injonctions d'accès par des autorités publiques de pays tiers, aux données à caractère personnel conservées au sein des pays de l'Union, notamment lorsque le responsable du traitement des données dispose également d'un établissement dans ce pays tiers;
9. des incitations accrues à la protection des données dès le stade conceptuel et qui s'appliqueraient par défaut.

Le Conseil

Plusieurs réunions du groupe de travail du Conseil (DAPIX) ont eu lieu, d'abord sous la présidence danoise et maintenant sous la présidence chypriote du Conseil. Les discussions au sein du groupe DAPIX ont principalement porté sur la proposition de règlement, dont les articles ont été examinés un à un.

Selon le Conseil, les discussions menées au sein du groupe de travail ont révélé un large consensus entre les États membres sur la nécessité de réformer le cadre juridique existant en matière de protection des données et de renforcer les droits des personnes à la protection de leurs données à caractère personnel. En outre, une convergence de vues est apparue entre les États membres sur la nécessité d'harmoniser davantage et de rendre plus cohérente l'application de la réglementation de l'UE sur la protection des données. Toutefois, un document ayant circulé de manière non autorisée montre qu'un certain nombre de notions essentielles et établies depuis longtemps concernant la protection des données à caractère personnel sont remises en question par plusieurs délégations nationales.

Lors d'une réunion informelle des ministres de la justice et des affaires intérieures organisée à Nicosie les 23 et 24 juillet 2012, les ministres ont discuté de l'opportunité de concevoir, dans certains cas, des exigences formelles plus ciblées (la charge administrative), en particulier en ce qui concerne les micro, petites et moyennes entreprises – sur la base de critères établis, tels que les risques liés à l'activité de traitement des données, la taille de l'entité responsable du traitement, le volume des données à caractère personnel traitées et/ou le nombre de personnes concernées par ces données. Les ministres ont en outre convenu qu'aucune distinction ne devait être faite en tant que telle dans la réglementation concernant les secteurs privé et public, même si un certain degré de souplesse est nécessaire dans le domaine du secteur public. Les ministres sont également convenus d'examiner au cas par cas le bien-fondé, l'horizon temporel et les solutions alternatives en ce qui concerne les très nombreuses propositions d'actes délégués et d'exécution. À cette fin, les États membres ont reçu un questionnaire (qu'ils doivent soumettre avant le 4 octobre) portant sur les charges administratives, les actes délégués et les actes d'exécution ainsi que le niveau de souplesse jugé nécessaire pour la réglementation sur la protection des données dans le secteur public.

Contributions supplémentaires du groupe de travail «Article 29»

Dans son avis du 23 mars 2012, le groupe de travail «Article 29» a présenté sa première réaction générale face aux propositions de la Commission et mis en évidence des sujets de préoccupation ainsi qu'un certain nombre de suggestions en vue d'améliorer ces propositions.

Le groupe de travail «Article 29» accueille avec satisfaction l'approche globale adoptée par les rapporteurs du Parlement européen et est convaincu que toutes les commissions parlementaires associées examineront avec la plus grande attention tous les éléments du paquet afin d'apporter de nouvelles améliorations aux deux propositions de la Commission.

Le groupe de travail se félicite également des mesures prises par la présidence chypriote du Conseil, mentionnées ci-dessus, visant à relancer les discussions au sein du groupe de travail du Conseil chargé d'examiner cette réforme.

En vue des discussions actuelles et à venir au Parlement européen et au Conseil, le groupe de travail a décidé d'adopter le présent avis qui fournit des indications supplémentaires, notamment sur certains concepts clés en matière de protection des données, et analyse la nécessité et les effets de la proposition d'actes délégués, en proposant, là où cela s'avère nécessaire, des alternatives plus appropriées[1].

Le groupe de travail observe que parmi les préoccupations formulées au sujet des incidences du règlement proposé, certaines se sont focalisées sur les aspects clés des données à caractère personnel et de la notion de consentement. Le groupe de travail estime qu'il s'agit là d'une erreur. Afin de mieux protéger la confidentialité des informations à caractère personnel et de garantir la pérennité du règlement, il est nécessaire d'adopter une définition des données à caractère personnel qui soit large et de veiller à ce que toute procédure fondée sur un consentement soit une procédure de qualité. Au cas où l'adoption de ces concepts clés produirait des effets disproportionnés pour l'application des dispositions du règlement relatives au traitement et à la fixation des droits individuels, ce sont ces dispositions et leurs dérogations que l'on devrait examiner de plus près, et non les concepts clés eux-mêmes.

[1] En outre, le groupe de travail a entamé l'examen de la notion de limitation des motifs et a l'intention de publier un avis à cet égard au début de l'an prochain. Le groupe de travail participera également aux discussions en cours portant sur la portée du règlement proposé, notamment en ce qui concerne les dérogations pour les ménages et l'utilisation personnelle.

Sur la définition des données à caractère personnel

Dans son avis du 23 mars[2], le groupe de travail se félicite de la définition du concept de «personne concernée» figurant à l'article 4, paragraphe 1, de la proposition de règlement, qui énonce qu'on entend par «*personne concernée: une personne physique identifiée ou une personne physique qui peut être identifiée*...».

Le groupe de travail observe que cette définition ne change pas fondamentalement la notion de données à caractère personnel telles que définie dans la directive 95/46/CE, mais qu'elle se limite à réorganiser ses différents éléments[3]. Dans son avis sur la notion de données à caractère personnel[4], le groupe de travail a déjà observé que la présente définition offre suffisamment de continuité et de souplesse dans la manière dont elle s'applique aux données dans divers contextes, tels que la recherche pharmaceutique ou les adresses IP.

L'une des principales conclusions de cette analyse est qu'une personne physique peut être considérée comme susceptible d'être identifiée lorsqu'elle peut être distinguée des autres membres d'un groupe de personnes, et, de ce fait, être traitée de manière différente.

Il est donc suggéré de préciser, au considérant 23 et à l'article 4, que la notion de personne «identifiable» comprend également le fait de singulariser une personne de la sorte.

Aux termes du considérant 23: *«Il y a lieu d'appliquer les principes de protection à toute information concernant une personne identifiée ou identifiable* ***et à toute information permettant de repérer une personne et de la traiter différemment****. 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. Il n'y a pas lieu d'appliquer les principes de protection aux données qui ont été rendues suffisamment anonymes pour que la personne concernée ne soit plus identifiable.»*[5]

Aux termes de l'article 4, paragraphe 2: *une «personne concernée» désigne une personne physique identifiée ou une personne physique qui peut être identifiée, directement ou indirectement,* ***ou singularisée et traitée différemment,*** *par des moyens raisonnablement*

---

2 Avis 1/2012 sur les propositions de réforme de la protection des données (WP 191).

3 L'article 2, point a), de la directive 95/46/CE dispose actuellement que par «données à caractère personnel», il faut entendre « toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.» Le considérant 26 établit actuellement que «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». Le règlement proposé introduit par conséquent une définition de «personnes concernée» qui se fonde uniquement sur les éléments existants.

4 Avis 4/2007 sur le concept de données à caractère personnel (WP 136).

5 Les mots **en caractères gras** ont été ajoutés au texte. Il est proposé d'effacer les mots figurant entre crochets. [….].

susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale, notamment par référence à un numéro d'identification, à des données de localisation, à des identifiants en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;»

En outre, le considérant 24, qui se rapporte à la définition des données à caractère personnel, prévoit que les numéros d'identification, données de localisation, identifiants en ligne ou autres éléments spécifiques, ne doivent pas forcément être considérés comme des données à caractère personnel en toutes circonstances. Dans sa formulation actuelle, la dernière phrase pourrait conduire à une interprétation trop restrictive de la notion de données à caractère personnel en ce qui concerne, par exemple, les adresses IP ou des témoins de connexion («cookies») d'identification. Le groupe de travail rappelle que les données à caractère personnel sont toutes les données relatives à une personne qui est identifiable. *«(Des) données concernent une personne si elles font référence à l'identité, aux caractéristiques ou au comportement d'une personne ou si de telles informations sont utilisées pour déterminer ou influencer la manière dont cette personne est traitée ou évaluée»*.

Le groupe de travail a déjà développé dans l'avis 4/2007 différents scénarios qui justifient la nécessité de considérer les adresses IP comme se rapportant à des personnes identifiables, *«en particulier dans les cas où le traitement des adresses IP est effectué dans le but d'identifier les utilisateurs de l'ordinateur (par exemple, par les titulaires de droits d'auteur, afin d'engager des poursuites à l'encontre d'utilisateurs d'ordinateurs pour violation des droits de propriété intellectuelle) (...)»*. Dans ce cas, ainsi que dans celui de témoins de connexion («cookies»), le responsable du traitement prévoit que des «moyens susceptibles d'être raisonnablement mis en œuvre» soient disponibles en vue d'identifier une personne et de lui associer un traitement spécifique[6].

C'est pourquoi le groupe de travail suggère de modifier le considérant 24 comme suit.

Considérant 24: *«Lorsqu'elles utilisent des services en ligne, les personnes physiques se voient associer des identifiants en ligne tels que des adresses IP ou des témoins de connexion ("cookies") par les appareils, applications, outils et protocoles utilisés. Ces identifiants peuvent laisser des traces qui, combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils et à identifier les personnes* ***ou à les singulariser****. Il en découle que des numéros d'identification, des données de localisation, des identifiants en ligne ou d'autres éléments spécifiques* ***doivent d'une manière générale*** *[supprimer: ne doivent pas nécessairement]* ***être considérés,*** *en soi, comme des données à caractère personnel [supprimer: dans tous les cas de figure].»*

[6] Voir également le rapport préliminaire de la Federal Trade Commission intitulé «*Protecting Consumer Privacy in an Era of Rapid Change*» (La protection de la vie privée des consommateurs à l'ère des changements rapides), de décembre 2010 et le rapport de la FTC intitulé «Protecting Consumer Privacy in an Era of Rapid Change», de mars 2012.

Sur la notion de consentement

Le consentement de la personne concernée constitue le premier fondement juridique, cité à l'article 6, paragraphe 1, du traitement des données à caractère personnel, pour autant que certaines conditions soient remplies. Ces conditions sont précisées à l'article 4, paragraphe 8, et à l'article 7 de la proposition de règlement.

Toutefois, le consentement, lorsqu'il est d'application nécessaire, joue un rôle en tant qu'élément dans un contexte plus vaste, dans lequel d'autres motifs peuvent également être invoqués pour légitimer le traitement de données à caractère personnel.

Dans son avis sur le consentement[7] publié récemment, le groupe de travail «Article 29» insiste sur la nécessité d'assurer que le consentement est utilisé dans un contexte approprié, et qu'il n'en soit pas fait un usage abusif. Lorsque le consentement est utilisé, celui-ci doit être exprimé de manière suffisamment claire. Il peut être exprimé de diverses façons, par exemple par le biais d'une déclaration ou d'une action de confirmation, puisqu'une telle notion est définie de façon suffisamment souple. L'exigence essentielle est qu'une telle déclaration ou action signifie clairement que la personne concernée consent au traitement des données à caractère personnel la concernant.

S'appuyant sur l'avis du groupe de travail, l'article 7 de la proposition de règlement apporte également des éléments positifs supplémentaires, en particulier en imposant la charge de la preuve au responsable du traitement, en introduisant des garanties dans le cadre d'une déclaration écrite et en invalidant le consentement lorsqu'il existe un déséquilibre significatif entre la situation de la personne concernée et celle du responsable du traitement. Le groupe de travail se félicite réellement de ces clarifications importantes et du renforcement des droits des particuliers.

Le groupe de travail a connaissance de ce que des doutes ont été émis quant au réalisme du mot «explicite» dans le contexte du consentement à l'article 4, paragraphe 8. Le groupe de travail est d'avis que l'inclusion du mot «explicite» constitue une importante clarification du texte, qui est nécessaire pour permettre aux personnes concernées d'exercer véritablement leurs droits, en particulier en ce qui concerne l'internet, où l'usage actuel du consentement est trop souvent abusif. Il serait très peu souhaitable que cette importante clarification du texte soit supprimée de celui-ci.

Enfin, le groupe de travail souligne que la notion d'autorisation a un sens général dans un large éventail de situations. Il estime que les conditions énoncées à l'article 4, paragraphe 8, et à l'article 7 sont tout à fait appropriées pour assurer une utilisation adéquate du consentement dans toutes ces situations. En ce qui concerne le cas particulier des témoins de connexion

[7] Avis 15/2011 sur la notion de consentement (WP 187).

(«cookies»), le groupe de travail a récemment souligné la souplesse supplémentaire qui a été consentie dans ce contexte[8].

Sur la proposition d'actes délégués

La proposition de la Commission relative à un nouveau règlement sur la protection des données prévoit un volume considérable d'actes délégués et d'actes d'exécution. Même si, dans certains cas, ces actes supplémentaires peuvent être un instrument précieux pour apporter un plus haut niveau d'harmonisation et d'orientation, le groupe de travail Article 29 émet certaines réserves en ce qui concerne la mesure dans laquelle la Commission serait habilitée à adopter de tels actes, comme il l'a déjà mentionné dans son avis concernant les propositions de réforme de la protection des données (WP 191). Comme mentionné ci-dessus, la commission LIBE du Parlement européen et le Conseil ont tous deux exprimé des inquiétudes similaires et ont annoncé qu'ils allaient examiner la proposition d'actes délégués et d'actes d'exécution article par article, pour s'assurer de leur réelle nécessité.

Dans son avis sur les propositions de réforme de la protection des données, le groupe de travail a indiqué que le comité européen de la protection des données, successeur du présent groupe de travail, devrait en tout état de cause être consulté dans le cadre du processus d'élaboration des actes délégués ou d'exécution. En outre, actuellement, l'une des tâches principales du groupe de travail est de fournir une orientation interprétative. Les orientations fournies ces dernières années, principalement sous la forme d'avis, ont apporté la preuve de la valeur ajoutée qui est la sienne. À l'avenir, il sera encore plus important que le comité européen de la protection des données fournisse de telles orientations interprétatives. Comme ce comité se compose de toutes les autorités nationales de protection des données, il peut, dans certains cas, être mieux à même de fournir des orientations.

Les différences entre les actes délégués et les actes d'exécution

Depuis l'entrée en vigueur du traité de Lisbonne, la Commission peut être habilitée à adopter des actes délégués et des actes d'exécution. Les actes délégués reposent sur l'article 290 du TFUE et ils peuvent être adoptés pour compléter ou modifier certains éléments non essentiels d'un acte législatif (dans le cas présent, le règlement proposé). Les actes d'exécution reposent sur l'article 291 du TFUE et sont utilisés lorsque des conditions uniformes d'exécution des actes juridiquement contraignants de l'Union, comme une directive ou un règlement, sont nécessaires.

En ce qui concerne les actes délégués, la délégation de pouvoirs proposée signifie qu'une part substantielle de la réglementation ne fait pas partie du règlement proposé et n'est pas adoptée dans le cadre de la procédure législative normale. Cela ne signifie pas pour autant que le Parlement européen et le Conseil ne participent pas à l'adoption des actes délégués. Un acte délégué n'entre en vigueur que si le Parlement européen et le Conseil n'ont pas exprimé

[8] Avis 4/2012 sur l'exemption du consentement pour les cookies (WP 194).

d'objection dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil, comme il découle également de l'article 86 de la proposition de règlement.

Si le Parlement européen ou le Conseil formulent une objection à l'égard d'un acte délégué, celui-ci n'entrera pas en vigueur. La Commission peut alors décider de proposer un nouvel acte délégué en tenant compte des objections exprimées, ou élaborer une nouvelle proposition législative au cas où l'objection reposerait sur le fait que la Commission aurait outrepassé les pouvoirs qui lui ont été délégués. Une autre possibilité est bien sûr que la Commission décide de ne pas faire de nouvelle proposition d'acte ou de texte législatif.

L'article 290 du TFUE ne prévoit pas la possibilité pour le Parlement européen ou le Conseil de proposer des amendements; ils peuvent uniquement s'opposer à l'entrée en vigueur d'un acte délégué.

Les articles 290 et 291 du TFUE n'établissent pas de critères clairs pour le choix entre un acte délégué et un acte d'exécution. La proposition de règlement montre clairement que la Commission prévoit des actes d'exécution afin d'assurer des conditions uniformes et plus techniques pour la mise en œuvre du règlement, telles que les formulaires types et les procédures standards.

Le fait de conférer à la Commission le pouvoir d'adopter des actes délégués et des actes d'exécution ne signifie pas nécessairement qu'elle soit tenue d'adopter tous les actes proposés dans le règlement. La plupart des actes ne seront adoptés que lorsque cela sera nécessaire.

Le groupe de travail insiste sur le fait que pour pouvoir adopter des actes délégués et des actes d'exécution, la Commission devrait préalablement en établir la nécessité. Le fait qu'une telle nécessité ne puisse pas toujours être appréciée au moment de l'adoption du règlement ne suffit pas à justifier l'octroi à la Commission du pouvoir d'adopter des actes délégués ou d'exécution, simplement pour le cas où cela s'avérerait utile par la suite.

Il résulte de ce qui précède qu'il existe plusieurs manières de réglementer la protection des données au niveau de l'UE:

- dans la proposition de règlement lui-même;
- dans un acte délégué;
- dans un acte d'exécution;
- dans les considérants du règlement proposé.

Toutefois, dans certains cas, le recours aux orientations interprétatives fournies par le comité européen de la protection des données (qui peuvent inclure l'approbation de codes de conduite) permet d'obtenir une approche plus cohérente et plus harmonisée au niveau de l'UE.

Comme la Commission semble envisager la mise en œuvre de ces actes principalement pour assurer des conditions uniformes, plus techniques de mise en œuvre du règlement, telles que les formulaires types et les procédures standards, et non pas tant pour la poursuite de la mise en œuvre et de l'application des normes (substantielles), ces actes ont pour le moment été supprimés de l'évaluation ci-après. Ils devront néanmoins peut-être également faire l'objet d'une analyse.

Évaluation de la proposition d'actes délégués

La Commission a précisé d'emblée que l'objectif de la réforme était d'assurer l'harmonisation et de veiller à ce que ces instruments restent neutres sur le plan de la technologie. Cet objectif a donc été pris en compte pour l'analyse de la proposition d'actes délégués.

Un autre critère clair (découlant de l'article 290 du TFUE) est que les éléments essentiels devraient être inclus dans l'acte de base, c'est-à-dire dans le règlement proposé, et non dans un acte délégué. Le groupe de travail «Article 29» ainsi que le contrôleur européen de la protection des données ont signalé que dans plusieurs dispositions du règlement proposé, des compétences déléguées à la Commission portent sur des éléments essentiels[9].

En outre, dans certains cas, il est important de garantir la sécurité juridique. La fixation de normes pour les instruments contraignants de l'UE assure la sécurité juridique, ainsi que le respect de règles du jeu équitables au sein de l'UE. Il existe des situations dans lesquelles un instrument communautaire contraignant qui spécifierait une disposition du règlement serait le moyen le plus approprié d'assurer la sécurité juridique et la protection de la personne concernée, ainsi que d'éviter d'accroître les disparités entre les États membres.

Mais dans d'autres situations, une approche souple et tenant compte des différences culturelles pourrait être plus appropriée pour assurer l'application pratique de la réglementation. Dans ce cas, il pourrait s'avérer plus approprié de fournir des orientations sous la forme de lignes directrices publiées par le comité européen de la protection des données, qui reconnaissent la nécessité d'une certaine souplesse et soutiennent l'introduction du principe de responsabilité. En dernier recours, la question est du ressort de la Cour de justice et des juridictions nationales.

Le choix de traiter d'un problème spécifique se rapportant à la protection des données dans le cadre d'un ou de plusieurs des instruments mentionnés précédemment devrait être fait sur la base de critères clairs.

Les critères utilisés pour cette évaluation sont les suivants:

- la question concerne-t-elle ou non une partie essentielle du règlement?
- la question doit-elle être traitée à l'échelon européen ou national (c'est-à-dire existe-t-il un besoin d'harmonisation)?
- un instrument juridiquement contraignant est-il nécessaire, ou un instrument plus souple convient-il?
- l'instrument est-il compatible avec le principe de la neutralité technologique?
- y a-t-il lieu de fournir des orientations supplémentaires (c'est-à-dire doit-on ou non laisser au responsable du traitement le soin de donner corps à la réglementation, selon

[9] Avis 1/2012 (WP 191), page 7 et avis du contrôleur européen de la protection des données (CEPD), paragraphe 74.

les circonstances de la situation, toujours sous réserve de la surveillance, du contrôle de l'application et du contrôle juridictionnel)?

Dans l'annexe du présent avis, les articles dans lesquels des actes délégués sont proposés sont recensés et analysés, et une évaluation a été réalisée pour déterminer si un acte délégué est effectivement le moyen le plus approprié pour régler le(s) problème(s) concerné(s). Parmi les autres moyens considérés comme étant appropriés pour fournir des orientations supplémentaires, à côté d'un acte délégué, figurent:

- le traitement de la question dans le texte du règlement;

Au lieu de prévoir la possibilité d'adopter des actes délégués, certains problèmes pourraient ou devraient être intégrés dans le texte du règlement lui-même. Le fait de préciser davantage certaines questions dans le texte du règlement assurerait une harmonisation, car le règlement est directement applicable dans toute l'Union européenne. Toutefois, cette approche risque de ne pas être suffisamment souple pour couvrir toutes les situations possibles et de ne pas être neutre sur le plan technologique. En outre, le processus de réforme risquerait d'être ralenti si on s'efforce d'incorporer davantage de règles dans le règlement lui-même.

- le traitement de la question dans un considérant du règlement;

Certaines des questions pourraient être traitées dans un considérant du règlement, au lieu d'un acte délégué. Dans une certaine mesure, un considérant peut donner des orientations générales utiles sur l'objectif et la raison d'être d'une disposition spécifique. Toutefois, tenter d'intégrer un plus grand nombre d'exemples dans les considérants du règlement risque de ralentir le processus de réforme, ou de créer une mauvaise réglementation obéissant à des intérêts particuliers et non à des principes généraux.

- le renvoi à la législation nationale;

Pour prendre en compte les différences (culturelles, législatives et historiques) entre les États membres, des précisions supplémentaires pourraient également être prévues par le droit national. Cela pourrait cependant porter atteinte à l'objectif d'harmonisation et au fonctionnement du marché intérieur.

- des orientations fournies par le comité européen de la protection des données;

Des orientations fournies par le comité européen de la protection des données peuvent, dans certains cas, être une bonne solution pour remplacer un acte délégué. Des indications fournies par le groupe de travail «Article 29» ne constituent pas un nouvel instrument. Actuellement, le groupe de travail «Article 29» fournit déjà des avis et des recommandations sur toute question relative à la protection des personnes en cas de traitement des données à caractère personnel, conformément à l'article 30 de la directive 95/46. En émettant des avis conjoints, l'actuel groupe de travail «Article 29» contribue à une application harmonisée du cadre juridique. Même si ces avis ne sont pas

juridiquement contraignants en eux-mêmes, ils font autorité et ont donné la preuve de leur valeur ajoutée. Les orientations fournies par le comité européen de la protection des données constituent un instrument souple qui peut être assez facilement adapté, modifié ou mis à jour, par exemple pour suivre les évolutions techniques.

- l'absence d'orientations ou de législation supplémentaires;

Dans certains cas, il pourrait être proposé de ne pas offrir d'orientations ou de législation supplémentaires, lorsque les dispositions en vigueur sont en elles-mêmes assez claires pour toutes les parties prenantes concernées; et les responsables du traitement eux-mêmes devraient alors assurer la conformité avec le règlement, toujours sous réserve de la surveillance, du contrôle de l'application et du contrôle juridictionnel.

ANNEXE

L'article 6, paragraphe 5 – préciser davantage les conditions visées à l'article 6, paragraphe 1, point f), pour divers secteurs et situations de traitement des données, y compris en ce qui concerne le traitement des données à caractère personnel concernant un enfant.

L'article 6, traite de la licéité du traitement, en établissant les six bases juridiques possibles sur lesquelles peuvent reposer les opérations de traitement (points a) à f)), *dont l'une au moins* doit s'appliquer à un moment donné.

Le paragraphe 1, au point f), prévoit que le traitement de données à caractère personnel n'est licite que lorsque et dans la mesure où ce traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement, sauf en cas de primauté des intérêts ou des libertés et droits fondamentaux de la personne concernée, laquelle bénéficie de la protection des données à caractère personnel, notamment dans le cas où la personne concernée est un enfant. Ces considérations ne s'appliquent pas aux traitements effectués par les autorités publiques dans l'exécution de leurs missions.

Conformément à l'article 6, paragraphe 1, point f), un intérêt légitime peut être un motif légal de traitement de données à caractère personnel lorsque et dans la mesure où certaines conditions ont été respectées, ce qui nécessite une mise en balance des différents éléments, en fonction des circonstances propres à chaque cas.

Selon le principe de responsabilité (qui est traité dans l'article 22 de la proposition de règlement), il convient de laisser au responsable du traitement le soin de décider s'il existe un intérêt légitime justifiant certains traitements de données ou si un tel intérêt est surpassé par les droits et libertés fondamentales de la personne concernée. Ceci fera l'objet d'une surveillance, d'un contrôle de l'application et d'un contrôle juridictionnel.

Néanmoins, comme cela concerne un des fondements juridiques nécessaire pour autoriser le traitement, il est essentiel de fournir des orientations supplémentaires pour parvenir à une compréhension commune de la disposition concernée. Des orientations supplémentaires sur des critères communs ou des exemples concernant la notion d'intérêt légitime seraient utiles pour assurer la cohérence de l'application et de la mise en œuvre.

Compte tenu de la multiplicité des cas de figure (actuels et futurs) de ce qui pourrait constituer un intérêt légitime, et des cas où ces intérêts seraient surpassés par les intérêts ou les droits et libertés fondamentales de la personne concernée, un instrument plus souple semble plus approprié qu'un instrument contraignant.

Par ailleurs, on peut douter du caractère approprié d'un acte délégué, s'agissant de traiter de cet élément essentiel du règlement.

S'en remettre au droit national pour de décider de tout règlement ultérieur donnerait lieu à des divergences d'interprétation et d'application non souhaitables. Les responsables du traitement des données seraient en effet autorisés à traiter des données sur la base de ce motif dans tel État membre et pas nécessairement dans tel autre. Afin d'assurer la cohérence de l'interprétation et l'application de cette base juridique pour le traitement, l'orientation devrait par conséquent être mise en place au niveau européen.

Pour permettre la souplesse nécessaire, au lieu de traiter de cette question dans un acte délégué, il semblerait plus approprié que le comité européen de la protection des données publie des lignes directrices expliquant dans quelles circonstances le motif d'«intérêt légitime» peut être invoqué et comment déterminer, à l'aide d'exemples concrets, si l'intérêt ou les droits et libertés fondamentales de la personne concernée ne l'emportent pas sur de tels intérêts.

L'article 8, paragraphe 3 – préciser davantage les critères et conditions applicables pour les méthodes d'obtention du consentement vérifiable visé au premier paragraphe. Ce faisant, la Commission doit envisager des mesures spécifiques pour les micro, petites et moyennes entreprises.

L'article 8, paragraphe 1, prévoit qu'aux fins du présent règlement, s'agissant de l'offre directe de services de la société de l'information aux enfants , le traitement des données à caractère personnel relatives à un enfant de moins de treize ans n'est licite que si et dans la mesure où le consentement est donné ou autorisé par un parent de l'enfant ou par une personne qui en a la garde. Le responsable du traitement s'efforce raisonnablement d'obtenir un consentement vérifiable, compte tenu des moyens techniques existants.

Selon le principe de responsabilité, il appartient au responsable du traitement de s'assurer de l'obtention d'un consentement vérifiable, en tenant compte de la technologie disponible.

Un document juridique précisant les critères et les exigences applicables aux méthodes permettant d'obtenir un consentement vérifiable risquerait de ne pas être suffisamment souple et pourrait également ne pas satisfaire suffisamment à l'obligation de neutralité sur le plan technologique.

De plus, permettre de traiter de cette question dans la législation nationale conduirait à des divergences entre les obligations imposées aux responsables du traitement, ce qui irait à l'encontre de l'objectif d'harmonisation et de création de conditions de concurrence équitables, et n'apporterait pas la souplesse requise.

En conclusion, il existe d'ores et déjà une obligation manifeste pour le responsable du traitement de faire tous les efforts raisonnables pour obtenir un consentement vérifiable, en tenant compte des technologies existantes. Il ne semble donc pas nécessaire pour cela de fournir des orientations supplémentaires dans un acte délégué.

Quant à envisager une approche spécifique aux micro, petites et moyennes entreprises, il ne semble pas y avoir de raison impérieuse de le faire. En effet, puisque la raison de l'introduction de cet article est que les enfants sont des personnes vulnérables, il semblerait étrange d'exclure les micro, petites et moyennes entreprises de l'obligation d'obtenir un consentement vérifiable lorsqu'il s'agit des données à caractère personnel d'enfants. En outre, un acte délégué ne peut jamais introduire des dérogations pour les petites et moyennes entreprises si ces dérogations ne sont pas déjà prévues dans le texte du règlement lui-même.

L'article 9, paragraphe 3 – préciser davantage les critères, conditions et garanties appropriées pour le traitement des catégories particulières de données à caractère personnel visés à l'article 9, paragraphe 1 ainsi que les dérogations prévues à l'article 9, paragraphe 2.

L'article 9 traite de catégories particulières de données à caractère personnel, et prévoit une interdiction de traitement des catégories mentionnées, sauf dans les dix dérogations figurant au paragraphe 2.

Cet article rappelle la manière dont la directive en vigueur envisage les catégories particulières de données, en interdisant expressément le traitement de celles-ci, mais en prévoyant quelques dérogations. En ce qui concerne *les critères et conditions*, la situation actuelle ne semble pas susciter beaucoup de problèmes; par conséquent, il ne paraît pas nécessaire de préciser les critères et conditions s'appliquant au traitement de catégories particulières de données à caractère personnel.

Comme, de manière générale, les paragraphes 1 et 2 a) à f) de l'article interdisent déjà de manière suffisamment claire le traitement des catégories particulières de données à caractère personnel mentionnées, sauf dans certaines circonstances, il ne semble pas nécessaire de préciser davantage les critères et les conditions de ces dispositions.

Néanmoins, l'expérience semble montrer que dans certains cas, il est utile de fournir des orientations concernant ce qui constituerait des mesures de sécurité appropriées.

La définition de mesures de sécurité appropriées ne pouvant s'effectuer qu'au cas par cas, il serait impossible de fournir des orientations supplémentaires dans un document juridiquement contraignant. Par conséquent, un instrument plus souple serait le plus adapté pour fournir davantage d'indications sur ce qui constituerait des mesures de sécurité appropriées.

Le comité européen de la protection des données pourrait donc émettre des orientations sur cette question. Dans la mesure du possible, des exemples non exhaustifs pourrait également être fournis dans un considérant du règlement.

En ce qui concerne le paragraphe 2, point g), le règlement prévoit des dérogations à l'interdiction générale en ce qui concerne les tâches réalisées dans l'intérêt public. Il serait logique que le contrôleur apprécier si la dérogation peut s'appliquer, toujours sous réserve de procédures de surveillance, de contrôle de l'application et de contrôle juridictionnel. Toutefois, il pourrait être utile d'ajouter à cette dérogation quelques orientations supplémentaires afin d'assurer l'harmonisation et la cohérence de son application au niveau européen.

Compte tenu de la grande diversité des situations dans lesquelles un traitement des données peut être autorisé sur la base de la dérogation pour les tâches réalisées dans l'intérêt public, un acte délégué ne semble pas être un instrument approprié. Un instrument plus souple serait plus utile pour fournir des orientations au responsable du traitement lorsque, malgré l'interdiction générale, il peut traiter des données à caractère personnel sur la base de cette dérogation.

En outre, et selon l'avis du groupe de travail «Article 29» sur les propositions présentées, il faudrait, dans la mesure du possible, définir pour chaque article la notion de l'intérêt général particulier.

Compte tenu de ce qui précède, l'intérêt général particulier prévu à l'article 9, paragraphe 2, point g), devrait être clarifié davantage dans le texte du règlement lui-même et éventuellement explicité dans un considérant.

L'article 12, paragraphe 5 – préciser davantage les critères et conditions

concernant les demandes manifestement excessives et le paiement de frais, prévus à l'article 12, paragraphe 4.

L'article 12 concerne spécifiquement les frais à percevoir lorsque une demande faite par une personne concernée est manifestement excessive.

L'article 12, paragraphe 4, prévoit que les informations fournies et les mesures prises à la demande des personnes concernées souhaitant exercer leurs droits sont gratuites. Lorsque les demandes sont manifestement excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut exiger le paiement de frais pour fournir les informations ou pour prendre les mesures demandées, ou s'abstenir de prendre les mesures demandées. Dans ce cas, il incombe au responsable du traitement de prouver le caractère manifestement excessif de la demande.

Cet article dispose au paragraphe 4:«[...] il incombe au responsable du traitement de prouver le caractère manifestement excessif de la demande». Selon le principe de responsabilité, il conviendrait de laisser à l'appréciation du responsable du traitement de déterminer si la demande est manifestement excessive. Et cela, toujours sous réserve de la surveillance, du contrôle de l'application et du contrôle juridictionnel.

Étant donné que pour apprécier le caractère manifestement excessif d'une demande, il faut toujours l'examiner au cas par cas, compte tenu de l'ensemble des circonstances qui l'entourent, il semble plus approprié de préciser les critères et les conditions dans le cadre d'un instrument plus souple.

En ce qui concerne les frais pouvant être appliqués lorsqu'une demande est manifestement excessive, il serait impossible ou inapproprié de les prévoir dans un instrument juridiquement contraignant, ou même au niveau de l'UE, car les différences dans les divers États membres ou entre les secteurs ne seraient pas prises en considération.

En conclusion, il ne semble pas nécessaire de prévoir une législation ou des orientations supplémentaires en ce qui concerne les critères et conditions applicables aux demandes manifestement excessives et aux frais prévus à l'article 12, paragraphe 4. Néanmoins, si une telle disposition devait s'avérer nécessaire, le montant maximum exigible pourra être fixé dans le droit national.

L’article 14, paragraphe 7 – préciser davantage:
- les critères de classification dans les catégories de destinataires visés à l'article 14, paragraphe 1, point f),
- les exigences de notification d'un accès potentiel visé à l'article 14, paragraphe 1, point g);
- les critères relatifs aux informations complémentaires nécessaires visées à l’article 14, paragraphe 1, point h), pour des circonstances et secteurs particuliers; et
- les conditions et les garanties appropriées concernant les exceptions prévues à l’article 14, paragraphe 5, point b).
Pour cela, la Commission prendra des mesures appropriées en faveur des micro, petites et moyennes entreprises.

L'article 14 concerne les informations à fournir à la personne concernée.

Le paragraphe 1, points f) à h), prévoit que lorsque des données à caractère personnel relatives à une personne sont collectées, le responsable du traitement doit fournir à la personne concernée au moins les destinataires ou, le cas échéant, les catégories de destinataires, des données à caractère personnel (point f)), que le responsable du traitement a l’intention de transférer vers un pays tiers ou une organisation internationale, doit l'informer du niveau de protection offert par ce pays tiers ou cette organisation internationale, en référence à une décision relative au niveau de protection adéquat par la Commission (point g)), ainsi que lui fournir toute information supplémentaire nécessaire pour garantir un traitement approprié à l'égard de la personne concernée, compte tenu des circonstances particulières dans lesquelles des données à caractère personnel sont collectées (point h)).

Le paragraphe 5, point b, prévoit que les quatre premiers alinéas de l'article 14 ne s’appliquent pas lorsque les données ne sont pas collectées auprès de la personne concernée ou que la fourniture de telles informations s'avère impossible ou nécessiterait des efforts disproportionnés.

Les droits et obligations énoncés dans le présent article sont déjà tout à fait clairs. En particulier, par rapport à la directive 95/46/CE, l'article prévoit un cadre plus clair et des orientations plus nombreuses pour les parties prenantes concernées.

En outre, les responsabilités du responsable du traitement des données doivent être prise en compte, en ce qui concerne notamment les critères de classification dans les catégories de destinataires visées à l'article 14, paragraphe 1, point f), les exigences en matière de notification d'un accès potentiel visé à l'article 14, paragraphe 1, point g), et les critères concernant les informations complémentaires nécessaires visées à l’article 14, paragraphe 1, point h), pour des secteurs et circonstances spécifiques.

En ce qui concerne les conditions et garanties appropriées relatives aux exceptions prévues à l'article 14, paragraphe 5, point b), le responsable du traitement devrait également être en mesure d'évaluer et de démontrer si la fourniture d'informations implique un effort disproportionné, sous réserve de la surveillance, du contrôle de l'application et du contrôle juridictionnel.

Proposer des indications plus précises afin de définir la notion d'effort disproportionné serait néanmoins utile, étant donné que cela représente une dérogation à l'un des droits fondamentaux d'une personne concernée (le droit à l'information). Il s'agit d'un droit particulièrement important lorsque le responsable du traitement n'a pas collecté les données directement auprès des personnes concernées.

Il conviendrait de fournir de plus amples orientations à l'échelon européen afin d'harmoniser les pratiques à cet égard. En effet, dans le monde interconnecté d'aujourd'hui, des interprétations divergentes de cette exception auraient un impact grave à la fois sur les personnes concernées et les responsables du traitement, et compromettraient l'harmonisation des pratiques. Le comité européen de la protection des données serait le mieux placé pour fournir de telles orientations. Pour des raisons de sécurité juridique, un instrument contraignant pourrait être envisagé, qui se limiterait à établir des conditions et garanties pour les questions principales.

Les conditions principales et les garanties appropriées pour l'exemption visée à l'article 14, paragraphe 5, point b) pourraient figurer dans un acte délégué, ce qui dispenserait le responsable du traitement de fournir des informations à la personne concernée. Toutefois, des indications plus détaillées de la part du comité européen de la protection des données permettraient de pouvoir mieux déterminer les cas dans lesquels les responsables du traitement pourraient faire usage de la dérogation en partant d'une analyse de circonstances diverses et de contextes concrets.

La mise en place d'obligations différentes (moins strictes) qui s'appliqueraient aux entités responsables du traitement en fonction de leur taille pourrait gravement porter atteinte à la finalité de l'article, qui consiste à obliger les responsables du traitement à assurer une transparence permettant aux personnes concernées de faire des choix éclairés. Par conséquent, l'obligation de fournir les informations nécessaires afin que la personne concernée puisse faire un choix éclairé devrait être applicable quelle que soit la taille de l'entité responsable du traitement des données. En outre, un acte délégué ne peut en aucun cas introduire de dérogations pour les petites et moyennes entreprises si ce n'est pas déjà prévu dans le texte du règlement lui-même.

L'article 15, paragraphe 3 – préciser davantage les critères et les exigences applicables à la communication à la personne concernée du contenu des données à caractère personnel visées à l'article 15, paragraphe 1, point g).

L'article 15 porte sur le droit d'accès de la personne concernée et le paragraphe 1, point g), traite spécifiquement de la communication de données à caractère personnel faisant l'objet d'un traitement, et de toute information disponible sur l'origine de ces données.

Même si l'article 15 lui-même traite du droit d'accès des personnes concernées, la question qui devrait être encore précisée dans la proposition d'acte délégué se rapporte aux obligations des responsables du traitement. À cet égard, selon le principe de responsabilité, il convient de laisser au responsable du traitement le soin de s'assurer qu'il est en conformité avec la législation, toujours sous réserve de la surveillance, du contrôle de l'application et du contrôle juridictionnel.

En outre, le droit de la personne concernée est clair en ce sens que l'article prévoit que celle-ci doit recevoir des informations sur les données à caractère personnel faisant l'objet d'un traitement, ainsi que toute information disponible quant à l'origine de ces données.

Par conséquent, il ne semble pas qu'une nouvelle législation ou de nouvelles recommandations soient nécessaires.

N.B.: La question de savoir si l'article 15, paragraphe 1, point g), se réfère également aux données à caractère personnel qui sont effectivement traitées, comme semble l'indiquer le paragraphe 3, pourrait cependant être clarifié davantage.

L'article 17, paragraphe 9 – préciser davantage:
- les exigences et les critères relatifs à l'application du paragraphe 17, point 1) (droit à l'oubli) dans des secteurs spécifiques ou des circonstances spécifiques de traitement de données; et,
- les conditions présidant à la suppression des liens vers des données à caractère personnel, à la copie ou à la reproduction de ces données dans le cadre de services de communication accessibles au public, comme prévu au paragraphe 2 de l'article 17; et,
- les conditions et les critères applicables à la limitation du traitement des données à caractère personnel, visés au paragraphe 4 de l'article 17.

L'article 17 concerne le droit à l'oubli.

Le paragraphe 1 dispose que la personne concernée a le droit d'obtenir du responsable du traitement l'effacement des données à caractère personnel la concernant et la cessation de la diffusion de ces données, en particulier en ce qui concerne les données à caractère personnel que la personne concernée a rendues disponibles lorsqu'elle était enfant, quand ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées (point a)); lorsque la personne concernée retire son consentement ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement (point b)); lorsque la personne concernée s'oppose au traitement de données à caractère personnel en vertu de l'article 19, paragraphe c); ou lorsque le traitement des données n'est pas conforme au règlement pour d'autres motifs (point d)).

Les actes délégués proposés préciseraient davantage les conditions d'application du droit à l'oubli s'appliquant à différents secteurs ou opérations de traitement, les conditions de suppression des liens, de copie et de reproduction, ainsi que les restrictions aux opérations de traitement.

Pour assurer une interprétation et une mise en œuvre harmonisées de l'article 17, il serait utile de fournir des orientations supplémentaires à l'échelon européen, de sorte que tant les personnes concernées que les responsables du traitement sachent quels sont leurs droits et leurs obligations dans le reste de l'UE.

Comme le règlement lui-même ne peut pas traiter de manière adéquate toutes les situations pertinentes, il conviendrait qu'un autre instrument fournisse de plus amples orientations.

Afin de garantir la sécurité juridique des responsables du traitement des données et des personnes concernées, il conviendrait de traiter dans un document juridiquement contraignant l'application du droit à l'oubli concernant différents secteurs et opérations de traitement, les conditions de suppression des liens, de copie et de reproduction, ainsi que les restrictions aux opérations de traitement.

Par conséquent, un acte délégué semble effectivement être le moyen le plus indiqué, pour autant qu'il soit adopté au moment de l'entrée en vigueur du règlement.

L’article 20, paragraphe 5, préciser davantage les critères et conditions applicables aux mesures nécessaires pour sauvegarder les intérêts légitimes de la personne concernée visés à l’article 20, paragraphe 2) (dérogations à l'interdiction de profilage des demandeurs).

L'article 20 concerne le profilage et le second paragraphe dispose que, sous réserve des autres dispositions du règlement, une personne ne peut être soumise au profilage que si le traitement est effectué dans le cadre de la conclusion ou de l'exécution d'un contrat, lorsque la demande de conclusion ou d'exécution de contrat introduite par la personne concernée a été satisfaite ou, qu'ont été invoquées des mesures visant à sauvegarder les intérêts légitimes de la personne concernée, telles que le droit d’obtenir une intervention humaine (point a), ou lorsque le traitement est expressément autorisé par la législation de l'Union ou d'un État membre, législation prévoyant également des mesures appropriées pour la sauvegarde des intérêts légitimes de la personne concernée (point b); ou encore lorsque le traitement est fondé sur le consentement de la personne concernée (point c).

L’article 20, paragraphe 1, prévoit que «Toute personne physique a le droit de ne pas être soumise à une mesure produisant des effets juridiques à son égard ou l'affectant de manière significative (...) destiné à évaluer certains aspects personnels (...) ou à analyser ou prévoir en particulier le rendement professionnel de celle-ci, sa situation économique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement». Le deuxième paragraphe prévoit trois dérogations à ce droit.

La question que l'acte(ou les actes) délégué(s) proposé(s) devra (devront) couvrir semble se rapporter à l'obligation qui incombe au responsable du traitement de déterminer si, malgré l'interdiction générale, il peut soumettre une personne aux mesures visées à l'article 20, paragraphe 1, sur la base des intérêts légitimes des personnes concernées.

Un instrument juridiquement contraignant semble être le plus indiqué étant donné qu'un responsable du traitement n'est pas toujours en mesure de déterminer quel type de mesures sont appropriées en vue de préserver l'intérêt légitime de la personne concernée et que, de plus, la disposition concerne une dérogation à un droit de la personne concernée, laquelle a droit à la sécurité juridique. Il conviendrait de fournir des précisions supplémentaires au niveau européen, afin d'éviter toute fragmentation et d'assurer le même niveau de protection pour toutes les personnes.

Un acte délégué pourrait donc être un instrument approprié, à condition qu'il soit adopté simultanément à l'entrée en vigueur du règlement. En outre, il pourrait également être utile que le comité européen de la protection des données fournisse des orientations supplémentaires sur les critères et conditions s'appliquant à des mesures permettant la sauvegarde des intérêts légitimes de la personne concernée.

L'article 22, paragraphe 4 – préciser davantage:
- tous autres critères et exigences supplémentaires concernant les mesures appropriées visées à l'article 22, paragraphe 1, autres que celles déjà visées à l'article 22, paragraphe 2;
- les conditions de vérification et mécanismes d'audit visées à l'article 22, paragraphe 3; et,
- les critères de proportionnalité visés à l'article 22, paragraphe 3, et la considération de mesures spécifiques s'appliquant aux micro, petites et moyennes entreprises.

L'article 22 est «l'article de la responsabilité générale», et au premier paragraphe, il prévoit que le responsable du traitement adopte des règles internes et met en œuvre les mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du règlement. Le paragraphe 2 désigne les éléments sur lesquels ces mesures portent en particulier, et le troisième paragraphe dispose que le responsable du traitement met en œuvre des mécanismes pour vérifier l'efficacité de ces mesures. Le cas échéant, cette vérification est effectuée par des auditeurs indépendants internes ou externes.

L'article 22 fait obligation aux responsables du traitement de se conformer au règlement; il est fondé sur le principe de responsabilité. Conformément à ce principe, il appartient au responsable du traitement de décider des règles à adopter et des mesures à prendre pour garantir, et être à même de démontrer, la conformité avec le présent règlement, à condition que celles-ci soient appropriées et efficaces. Et cela, toujours sous réserve de la surveillance, du contrôle de l'application et du contrôle juridictionnel.

Comme le deuxième paragraphe de cet article fournit déjà des exemples non exhaustifs de la façon de donner corps à l'obligation générale, il semble inutile de détailler davantage d'autres critères ou exigences.

Il convient également de laisser au responsable du traitement le soin de mettre en œuvre des mécanismes permettant de vérifier l'efficacité des mesures adoptées, car le choix du mécanisme le plus approprié dépend du secteur et du modèle économique.

En conclusion, étant donné que l'article lui-même donne corps au principe de responsabilité, il semble inutile de proposer des critères ou exigences supplémentaires concernant les mesures appropriées autres que ceux déjà prévus au paragraphe 2, ou concernant les conditions pour le mécanisme de vérification et d'audit.

S'agissant de l'attention particulière portée aux micro, petites et moyennes entreprises, l'obligation générale de rendre compte, d'adopter des règles et de mettre en œuvre des mesures appropriées en vue de garantir, et d'être en mesure de démontrer, la conformité au présent règlement, doit s'appliquer indépendamment de la taille de l'entité responsable du

traitement. Néanmoins, les micro, petites et moyennes entreprises devraient bien sûr être autorisées à adopter des mécanismes et mesures qui soient à leur échelle. En outre, un acte délégué ne peut jamais introduire des dérogations pour les petites et moyennes entreprises si cela n'est pas déjà prévu dans le texte du règlement lui-même.

.

L'article 23, paragraphe 3 – préciser davantage les critères et conditions s'appliquant aux mesures et mécanismes appropriés visés à l'article 23, paragraphes 1 et 2, notamment en ce qui concerne la protection des données dès la conception, applicables dans tous les secteurs, produits et services.

L'article 23 concerne les principes de la protection des données dès la conception et par défaut.

Compte tenu du principe de responsabilité énoncé à l'article 22, il conviendrait de laisser à l'appréciation du contrôleur de déterminer quelles mesures et procédures techniques et organisationnelles appropriées il convient de mettre en œuvre pour assurer le respect des principes de la protection des données dès la conception et par défaut.

En outre, l'obligation imposée aux responsables du traitement à l'article 23 est déjà très explicite car elle fait peser sur ceux-ci la responsabilité de la mise en œuvre de mesures et procédures adéquates.

Il semble quasiment impossible de tenir compte de tous les cas de figure possibles dans le présent règlement, car on ne peut apprécier qu'au cas par cas si le responsable du traitement a pris les mesures appropriées et suivi les procédures adéquates compte tenu de l'état des connaissances et du coût de la mise en œuvre.

En conclusion, aucune législation ou orientations supplémentaires ne semblent nécessaires. Néanmoins, des orientations fournies par le comité européen de la protection des données peuvent s'avérer utiles.

L'article 26, paragraphe 5 – préciser davantage:
- les critères et exigences applicables aux responsabilités, fonctions et tâches associées à un sous-traitant, conformément à l'article 26, paragraphe 1; et,
- les conditions qui permettent de faciliter le traitement des données à caractère personnel au sein d'un groupe d'entreprises, notamment à des fins de contrôle et d'établissement de rapports.

L'article 26, paragraphe 1, prévoit que lorsque le traitement est effectué pour son compte, le responsable du traitement choisit un sous-traitant qui présente des garanties suffisantes pour mettre en œuvre des mesures et procédures techniques et organisationnelles appropriées, de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et garantisse la protection des droits de la personne concernée, en ce qui concerne notamment les mesures de sécurité technique et d'organisation régissant le traitement à effectuer, et veille au respect de ces mesures.

Il ne paraît pas nécessaire de préciser davantage les critères et exigences concernant les responsabilités, fonctions et tâches associées à un sous-traitant, ni de préciser les conditions qui permettent de faciliter le traitement des données à caractère personnel au sein d'un groupe d'entreprises, notamment à des fins de contrôle et d'établissement de rapports, compte tenu des exigences déjà prévues par le règlement, en particulier pour ce qui est de la responsabilité du responsable du traitement.

Les responsables du traitement ont l'obligation de s'assurer que le sous-traitant fournit des garanties suffisantes de manière à ce que le traitement des données soit conforme aux dispositions du présent règlement. En outre, le deuxième paragraphe de cet article précise déjà quels aspects seront couverts par le contrat ou tout autre document contraignant.

En outre, de nombreux facteurs peuvent influer sur la relation entre un responsable du traitement et un sous-traitant, et la façon de donner corps à cette obligation doit être établie au cas par cas.

Quant à détailler davantage les conditions permettant de faciliter le traitement des données à caractère personnel au sein d'un groupe d'entreprises, il convient également d'en laisser le soin au responsable du traitement en vertu du principe de responsabilité, étant donné qu'il existe déjà une obligation de veiller à ce que, dans le cadre d'un contrat contraignant, l'opération de traitement réponde aux exigences du présent règlement.

En outre, lorsque des données sont échangées avec des parties d'une entreprise située en dehors de l’EEE, la possibilité d'utiliser des règles d'entreprise contraignantes est déjà prévue dans le présent règlement.

Compte tenu de ce qui précède, aucune législation ou orientations supplémentaires ne sont nécessaires.

Le paragraphe 5 de l'article 28 – préciser davantage les critères et exigences applicables à la documentation visée au paragraphe 1 de l'article 28, pour tenir compte, en particulier, des responsabilités du responsable du traitement et du sous-traitant et, le cas échéant, du représentant du responsable du traitement.

L'article 28 concerne l'obligation faite aux responsables du traitement de conserver une trace documentaire des traitements.

Selon le principe de responsabilité, il semblerait opportun de laisser au responsable du traitement, au sous-traitant et au représentant le soin de décider des modalités précises pour respecter l'exigence de conformité en ce qui concerne la documentation.

En outre, le deuxième paragraphe de l'article 28 prévoit déjà une liste non exhaustive des éléments qui devraient au minimum être étayés par des documents justificatifs. **Il ne semble pas nécessaire de préciser davantage les critères et exigences en question.**

L'article 30, paragraphe 3 – préciser davantage les critères et exigences applicables aux mesures techniques et organisationnelles visées à l'article 30, paragraphes 1 et 2, y compris le point de savoir quelles sont les techniques les plus récentes, pour des secteurs spécifiques et dans des cas spécifiques de traitement de données, notamment compte tenu de l'évolution des techniques et des solutions de protection des données dès la conception ainsi que par défaut, sauf si l'article 30, paragraphe 4, s'applique (actes d'exécution).

L'article 30 concerne la sécurité du traitement des données.

Conformément au principe de responsabilité, il appartient au responsable du traitement de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques présentés par le traitement et la nature des données à caractère personnel, compte tenu des techniques les plus récentes et des coûts liés à la mise en œuvre.

Préciser davantage les critères et conditions s'appliquant aux mesures techniques et organisationnelles ne permettrait pas d'aborder tous les cas de figure différents qui peuvent se produire dans les divers secteurs et opérations de traitement.

L'un des objectifs de la révision du cadre juridique de la protection des données est de conserver une neutralité technologique. En revanche, les actes délégués proposés définiraient également les meilleures techniques. Même lorsqu'un acte délégué n'est pas neutre sur le plan technologique, il pourrait être inapproprié de recommander dans un instrument juridiquement contraignant certaines techniques. L'acte en question pourrait en outre être dépassé au moment de son adoption.

Dès lors, il ne semble pas indiqué d'ajouter d’autres spécifications au moyen d'un acte délégué. Toutefois, de nouvelles orientations fournies par le comité européen de la protection des données pourraient être envisagées, le cas échéant.

L’article 31, paragraphe 5 – préciser davantage les critères et conditions applicables pour constater une violation de données visée à l'article 31, paragraphes 1 et 2, et le contexte particulier dans lequel un responsable du traitement et un sous-traitant sont tenus de notifier la violation de données à caractère personnel.

L'article 31 concerne l'obligation du responsable du traitement d'informer l'autorité de contrôle de toute violation de données à caractère personnel.

Le paragraphe 1 prévoit qu'en cas de violation de données à caractère personnel, le responsable du traitement en adresse notification à l'autorité de contrôle, sans retard injustifié et, si possible, 24 heures au plus tard après en avoir pris connaissance. Lorsqu'elle a lieu après ce délai de 24 heures, la notification comporte une justification à cet égard.

En vertu de l’article 26, paragraphe 2, point f), le sous-traitant alerte et informe le responsable du traitement immédiatement après avoir constaté la violation de données à caractère personnel.

Les actes délégués proposés se rapportent aux critères et exigences relatives à l'établissement d'une violation de données et au contexte particulier dans lequel un responsable du traitement et un sous-traitant sont tenus de notifier la violation de données à caractère personnel.

Il importe en effet de fournir une orientation concernant les critères et exigences de la constatation d'une violation de données à caractère personnel et les circonstances particulières dans lesquelles une violation doit être notifiée.

Il conviendrait de fournir des orientations supplémentaires à l'échelle européenne pour assurer une mise en œuvre et l'application harmonisées de l’obligation de notifier l’autorité de contrôle de toute violation de données à caractère personnel. La notion de violation des données à caractère personnel doit également être définie.

Eu égard à l'importance des textes juridiquement contraignants pour toutes les parties concernées, il est important que ces textes soient clairs; et comme il s'agit ici d'une partie essentielle de la réglementation et des obligations à respecter, il conviendrait de traiter de cette question dans le texte du règlement lui-même.

Par conséquent, au lieu de préciser davantage, au moyen d'un acte délégué, les critères et exigences applicables à l'établissement d'une violation de données et les circonstances dans lesquelles elle doit être notifiée, il y a lieu d'en préciser au moins les lignes principales dans le texte du règlement.

Il serait souhaitable de fournir un certain nombre de précisions dans un acte délégué, à condition qu'il soit adopté avant l'entrée en vigueur du règlement ou en même temps.

L'article 32 paragraphe 5 – préciser davantage les critères et exigences concernant les circonstances, visées au paragraphe 1, dans lesquelles une violation de données à caractère personnel est de nature à porter atteinte aux données à caractère personnel.

L'article 32 concerne l'obligation faite au responsable du traitement de communiquer toute violation de données à caractère personnel à la personne concernée.

Le paragraphe 1 dispose que lorsque la violation de données à caractère personnel est susceptible de porter atteinte à la protection des données à caractère personnel ou à la vie privée de la personne concernée, le responsable du traitement, après avoir procédé à la notification prévue à l'article 31, communique la violation sans retard indu à la personne concernée.

L'acte délégué proposé porte sur les critères et exigences concernant les circonstances dans lesquelles une violation de données à caractère personnel est de nature à porter atteinte aux (à la protection des) données à caractère personnel ou à la vie privée de la personne concernée.

En effet, il est important de fournir des orientations sur les critères et les exigences applicables aux circonstances dans lesquelles une violation des données à caractère personnel est susceptible d'avoir un tel effet préjudiciable. Il convient de clarifier les conditions justifiant une communication à la personne concernée.

Des éclaircissements supplémentaires devraient être fournis au niveau européen pour assurer une mise en œuvre et une application harmonisées de l'obligation de communiquer une violation de données à caractère personnel à la personne concernée.

Eu égard à l'importance de ces critères pour toutes les parties intéressées, il importe de les préciser dans des textes juridiquement contraignants; et comme il s'agit ici d'une partie essentielle de la réglementation et des obligations à respecter, il conviendrait de traiter de cette question dans le texte du règlement lui-même.

Par conséquent, au lieu de préciser davantage dans un acte délégué les critères et exigences liés aux circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'avoir un effet préjudiciable et doit être communiquée à la personne concernée, il conviendrait de traiter de cela, au moins dans les grandes lignes, dans le texte du règlement.

Il serait souhaitable de prévoir un certain nombre de précisions dans un acte délégué, pour autant qu'il soit adopté au plus tard lors de l'entrée en vigueur du règlement.

L'article 33, paragraphe 6 – préciser davantage:
- les critères et les conditions s'appliquant aux opérations de traitement susceptibles de présenter les risques particuliers visés à l'article 33, paragraphes 1 et 2; et,
- les exigences applicables à l'analyse d'impact prévue à l'article 33, paragraphe 3, y compris les conditions de modularité, de vérification et d'auditabilité.
Ce faisant, la Commission envisage des mesures spécifiques pour les micro, petites et moyennes entreprises.

L'article 33, paragraphe 6 concerne l'obligation d'effectuer une analyse d'impact sur la protection des données à caractère personnel.

Le premier paragraphe prévoit que lorsque les traitements présentent des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités, le responsable du traitement ou le sous-traitant agissant pour le compte du responsable du traitement effectuent une analyse de l'impact des traitements envisagés sur la protection des données à caractère personnel. Le paragraphe 2 prévoit cinq opérations de traitement qui présentent des risques particuliers.

Le paragraphe 3 prévoit que l'analyse contient au moins une description générale des traitements envisagés, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face aux risques, les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données à caractère personnel et à apporter la preuve de la conformité avec le règlement, en tenant compte des droits et intérêts légitimes des personnes concernées par les données et des autres personnes touchées.

Les responsables du traitement procèdent à une analyse d'impact relative à la protection des données lorsqu'un traitement présente (est susceptible de présenter) des risques particuliers pour les droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités. Selon le principe de responsabilité, il convient de laisser à l'appréciation du contrôleur de déterminer si les opérations de traitement présentent (sont susceptibles de présenter) des risques particuliers pour les droits et libertés des personnes concernées.

Il s'agit toutefois d'une question importante, qui a une incidence sur la question de savoir si un responsable du traitement est tenu de procéder à une analyse de l'impact des traitements envisagés sur la protection des données à caractère personnel et si ceux-ci présentent des risques particuliers au regard des droits et libertés des personnes concernées. La cohérence au niveau européen est importante pour assurer une interprétation et une application harmonisées de l'article en question.

Les exigences d'ordre général sur les modalités de la détermination des risques spécifiques liés à une opération de traitement peuvent être fixées dans un acte délégué. À titre alternatif ou complémentaire, une orientation supplémentaire fournie par le comité

européen de la protection des données pourrait être prévue, à condition qu'une éventuelle liste d'opérations de traitement identifiée comme présentant des risques particuliers ne soit pas considérée comme exhaustive.

Tout en tenant compte de l'attention spéciale portée aux micro, petites et moyennes entreprises, il ne semble pas y avoir de raison impérieuse de créer des conditions spéciales pour elles. En particulier, puisque l'objectif de cet article est d'établir des garanties supplémentaires dans le cas où une opération de traitement présente (ou est susceptible de présenter) des risques particuliers au regard des droits et libertés des personnes concernées, il ne convient pas d'exempter de cette obligation les entités responsables du traitement pour des raisons de taille. En outre, l'article lui-même prévoit déjà un seuil lorsqu'il énonce: "susceptibles de présenter des risques particuliers…»; il s'agit là d'une exemption reposant sur la nature du traitement, ce qui est plus logique qu'une exemption reposant sur le nombre de salariés. En outre, un acte délégué ne peut jamais introduire de dérogation pour les petites et moyennes entreprises si cela n'est pas déjà prévu dans le texte du règlement lui-même.

L'article 34 paragraphe 8 – préciser davantage les critères et exigences applicables à la détermination du niveau élevé de risques particuliers visés à l'article 34, paragraphe 2, point a) (procédure de consultation préalable après une analyse d'impact relative à la protection des données).

L'article 34 concerne l'obligation faite aux responsables du traitement d'obtenir de l'autorité de contrôle une autorisation ou une consultation préalables. L'article 34, paragraphe 2, point a), traite en effet spécifiquement de l'obligation, pour les responsables du traitement, de consulter l'autorité de contrôle avant le traitement de données à caractère personnel, en vue d'assurer la conformité du traitement prévu avec le présent règlement et, notamment, d'atténuer les risques pour les personnes concernées, lorsque l'analyse d'impact a indiqué que les opérations de traitement sont du fait de leur nature, de leur portée ou de leurs finalités, susceptibles de présenter un niveau élevé de risques particuliers.

Les actes délégués proposés devraient préciser davantage les critères et conditions applicables à la détermination du niveau élevé de risque spécifique présenté par une opération de traitement, à la suite d'une analyse d'impact relative à la protection des données.

Bien qu'il semble approprié de laisser le soin au responsable du traitement de décider si les risques mis en évidence par une analyse d'impact sont d'un niveau élevé ou non, comme ces risques portent sur les données ou la vie privée de la personne concernée, il importe de fournir des orientations plus précises. Il conviendrait de préciser les critères et conditions au niveau européen, en vue d'assurer une approche harmonisée dans toute l'UE.

Comme toutes les opérations de traitement sont différentes, le fait que le niveau de risques spécifiques soit élevé ou pas dépend du fond de l'affaire. Comme il est quasiment impossible d'aborder tous les cas de figure possibles dans un document juridiquement contraignant, un instrument plus souple semble plus indiqué.

En outre, étant donné que les autorités de contrôle doivent traiter les demandes d'autorisation préalable et de consultation, il serait plus approprié que le comité européen de la protection des données publie des orientations, d'autant plus que celui-ci intervient déjà dans les cas pour lesquels une consultation préalable est jugée nécessaire par les autorités.

En conclusion, au lieu d'un acte délégué, il serait plus approprié d'utiliser des lignes directrices publiées par le comité européen de la protection des données pour préciser les critères et conditions applicables pour la détermination du niveau élevé de risques particuliers que des opérations de traitement sont susceptibles de présenter, après réalisation d'une analyse d'impact sur la protection des données.

L'article 35, paragraphe 11 – préciser davantage:
- les critères et les exigences concernant les activités de base du responsable du traitement ou du sous-traitant visés à l'article 35, paragraphe 1, point c); et,
- les critères concernant les qualités professionnelles du délégué à la protection des données visé à l'article 35, paragraphe 5.

L'article 35 prévoit l'obligation pour les responsables du traitement et les sous-traitants de désigner systématiquement un délégué à la protection des données lorsque: le traitement est effectué par un organisme ou une autorité publics (paragraphe 1, point a)); le traitement est effectué par une entreprise employant 250 personnes ou plus (paragraphe 1, point b)); les principales activités du responsable du traitement ou du sous-traitant consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique des personnes concernées (paragraphe 1, point c)).

L'article 35, paragraphe 5, prévoit que le responsable du traitement ou le sous-traitant désignent le délégué à la protection des données sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées dans le domaine de la législation et des pratiques en matière de protection des données.

L'un des actes délégués proposés aurait pour effet de préciser davantage les critères et conditions applicables aux activités principales du responsable du traitement ou du sous-traitant, consistant en traitements qui, du fait de leur nature, de leur champ d'application et/ou de leurs finalités, nécessitent un suivi régulier et systématique des personnes concernées.

Des règles supplémentaires à l'échelon européen seraient utiles pour assurer une interprétation et l'application harmonisées de l'article 35. Inscrire ces règles dans un document juridiquement contraignant permettrait de couvrir différentes situations, au moins dans les grandes lignes, mais ne pourrait probablement pas couvrir toutes les situations.

Un acte délégué établissant les lignes principales serait un instrument approprié. En outre, des orientations données par le comité européen de la protection des données permettraient de préciser davantage les critères et les exigences s'appliquant aux activités de base d'un responsable du traitement ou d'un sous-traitant et exigeant un suivi des personnes concernées.

Un acte délégué est également proposé pour préciser davantage les critères concernant les qualités professionnelles demandées au délégué à la protection des données.

Outre le principe de responsabilité, il conviendrait au moins dans une certaine mesure de laisser au responsable du traitement ou au sous-traitant le soin d'évaluer les qualités professionnelles du délégué à la protection des données. Les qualités que l'on souhaite que ces délégués possèdent peuvent varier considérablement en fonction du secteur et du modèle économique. Cependant, les approches très divergentes à ce sujet entre les divers États

membres – au niveau sectoriel ou non - porteraient gravement atteinte aux objectifs de conditions de concurrence équitable et de confiance mutuelle visés par le règlement proposé.

En conclusion, il conviendrait qu'un acte délégué précise davantage, dans les grandes lignes, les critères à prendre en compte pour les qualités professionnelles du délégué à la protection des données. Des indications supplémentaires pourraient être fournies par le comité européen de la protection des données.

L'article 37, paragraphe 2 - préciser davantage les critères et conditions applicables aux missions, à la certification, au statut, aux prérogatives et aux ressources du délégué à la protection des données visés au paragraphe 1.

L'article 37 traite des missions du délégué à la protection des données, et le premier paragraphe précise les missions minimales que le responsable du traitement ou le sous-traitant peuvent lui confier.

L'obligation générale faite à l'article 37, paragraphe 1, est déjà claire car elle donne au responsable du traitement et au sous-traitant la responsabilité de veiller à ce que certaines missions soient confiées au délégué à la protection des données. En outre, la liste de tâches figurant au paragraphe 1 précise aussi les missions que le délégué doit au moins se voir confier.

Selon le principe de responsabilité, il conviendrait, au moins dans une certaine mesure, de laisser au responsable du traitement ou au sous-traitant le soin d'établir les conditions dans lesquelles le délégué à la protection des données doit être mis à contribution. Ces conditions peuvent varier en fonction de divers facteurs.

Cependant, les approches très divergentes à cet égard entre les divers États membres – au niveau sectoriel ou non - porteraient là aussi gravement atteinte aux objectifs de conditions de concurrence équitable et de confiance mutuelle visés par le règlement proposé. En outre, ces conditions affecteront également l'indépendance des délégués à la protection des données.

En conclusion, il serait approprié qu'un acte délégué précise davantage, dans les grandes lignes, les missions, la certification, le statut, les prérogatives et les ressources du délégué à la protection des données visés à l'article 37, paragraphe 1. Des indications supplémentaires pourraient être fournies par le comité européen de la protection des données.

L'article 39, paragraphe 2 – préciser davantage:
- Les critères et exigences applicables aux mécanismes de certification en matière de protection des données, visés à l'article 39, paragraphe 1, y compris les conditions d'octroi et de révocation; et,
- les exigences en matière de reconnaissance au sein de l'Union et dans les pays tiers.

L'article 39 prévoit que les États membres et la Commission encouragent, en particulier au niveau européen, la mise en place de mécanismes de certification en matière de protection des données ainsi que de marques et labels de protection des données, qui permettent aux personnes concernées d'évaluer rapidement le niveau de protection offert par les responsables du traitement et les sous-traitants.

Il importe de fournir des orientations supplémentaires, car la fiabilité des mécanismes de certification en matière de protection des données, des marques et des labels, dépend étroitement des critères et exigences fixés pour les établir.

Puisque les mécanismes de certification doivent être encouragés, en particulier au niveau européen, il conviendrait de préciser davantage les critères et conditions également au niveau européen.

Eu égard à la difficulté de définir tous les critères et exigences dans leur intégralité dans le texte du présent règlement, il serait approprié d'adopter un instrument plus souple permettant de fournir d'autres critères et des lignes directrices pour les mécanismes de certification en matière de protection des données, y compris les conditions d'octroi, de révocation et de reconnaissance au sein de l'Union et dans les pays tiers.

Afin d'assurer la sécurité juridique des personnes concernées qui s'appuient sur les mécanismes de certification, les marques et les labels, un acte délégué semblerait en effet être l'instrument le plus approprié.

L'article 43, paragraphe 3 – préciser davantage:
- les critères et exigences applicables aux règles d'entreprise contraignantes au sens du présent article, notamment en ce qui concerne les critères applicables à leur approbation;
- l'application du paragraphe 2, points b, d), e) et f), aux règles d'entreprise contraignantes auxquelles adhèrent les sous-traitants; et,
- les exigences nécessaires supplémentaires pour assurer la protection des données à caractère personnel des personnes concernées en question.

L'article 43 porte sur les transferts internationaux encadrés par des règles d'entreprise contraignantes. Le paragraphe 2, points b), c), d), e) et f) indique que les règles d'entreprise contraignantes doivent au moins préciser les transferts de données ou l'ensemble des transferts de données (point b), les principes généraux de protection des données, les mesures visant à garantir la sécurité des données et les exigences en matière de transferts ultérieurs à des organismes qui ne sont pas liées par ces règles (point d), les droits des personnes concernées et les moyens d'exercer ces droits (point e), et l'acceptation, par le responsable du traitement ou par un sous-traitant établi sur le territoire d'un État membre de la responsabilité de toute violation des règles d'entreprise contraignantes par toute entité appartenant au groupe d'entreprises non établie dans l'Union (point f).

En premier lieu, des actes délégués sont prévus afin de préciser davantage, de manière générale, les critères et les exigences relatifs aux règles d'entreprise contraignantes au sens de l'article et, en particulier, les critères s'appliquant à leur approbation. Toutefois le premier paragraphe précise déjà qu'il appartient à l'autorité de contrôle, conformément au mécanisme de contrôle de la cohérence prévu à l'article 58, d'approuver les règles d'entreprise contraignantes. Ce même paragraphe prévoit également certaines conditions que l'autorité de contrôle doit prendre en compte.

Il semble qu'un nombre suffisant de mécanismes de contrôle est ainsi mis en place pour assurer que des règles d'entreprise contraignantes couvrent tous les éléments nécessaires. De plus, compte tenu du fait que le mécanisme de cohérence devrait être utilisé pour l'approbation de règles d'entreprise contraignantes, on note déjà un engagement au niveau européen.

En outre, il incombe aux autorités de contrôle d'approuver ces règles. La création d'actes délégués précisant davantage les critères et exigences s'appliquant en général à ces règles, et, en particulier, à leur approbation risquerait de porter atteinte à l'indépendance des autorités de contrôle et du comité européen de la protection des données.

Par conséquent, il ne semble pas nécessaire de préciser davantage les critères et les exigences s'appliquant en général aux règles d'entreprise contraignantes et, en particulier, à leur approbation.

En second lieu, des actes délégués sont prévus pour préciser davantage l'application de l'article 43, paragraphe 2, points b), d), e) et f), aux règles d'entreprise contraignantes auxquelles adhèrent les sous-traitants. Étant donné que cela concerne des questions critiques qui doivent être précisées dans des règles d'entreprise contraignantes, il serait utile d'assurer une plus grande harmonisation.

Comme les règles d'entreprise contraignantes seront applicables dans l'ensemble de l'UE, il convient d'en assurer une application et une interprétation harmonisées.

Les règles d'entreprise contraignantes dépendant du modèle économique appliqué par les entreprises et du secteur dans lequel celles-ci opèrent, il est pratiquement impossible de traiter de toutes les situations dans le règlement lui-même. Par conséquent, un instrument plus souple pourrait être utilisé.

Un acte délégué serait un instrument approprié. Par ailleurs, étant donné que le comité européen de la protection des données participera au processus découlant de l'obligation d'utiliser le mécanisme de contrôle de la cohérence pour l'approbation des règles d'entreprise contraignantes, il serait logique que ce comité publie des orientations sur l'application des articles en question aux règles d'entreprise contraignantes auxquelles adhèrent les sous-traitants.

En troisième lieu, des actes délégués sont proposés en ce qui concerne les exigences nécessaires supplémentaires visant à assurer la protection des données à caractère personnel des personnes concernées.

Conformément au principe de responsabilité, il convient de laisser au responsable du traitement ou au sous-traitant lui-même le soin d'assurer le respect de la loi, toujours sous réserve de la surveillance, du contrôle de l'application et du contrôle juridictionnel. En outre, cet article semble déjà exposer clairement et de manière détaillée la façon dont les règles d'entreprise contraignantes doivent être approuvées, par qui, selon quels critères et ce qu'elles devraient au minimum couvrir.

Il incombe aux autorités de contrôle d'approuver les règles d'entreprise contraignantes et, si nécessaire, de prendre des mesures coercitives; par conséquent, des actes délégués portant sur des exigences nécessaires supplémentaires pour assurer la protection des données à caractère personnel de la personne concernée présenteraient un risque sérieux de porter atteinte à l'indépendance des autorités de contrôle.

Comme le comité européen de la protection des données participera au processus découlant de l'obligation d'utiliser le mécanisme de contrôle de la cohérence pour l'approbation des règles d'entreprise contraignantes, il serait logique qu'il publie des

orientations sur l'application des articles en question aux règles d'entreprise contraignantes auxquelles adhèrent les sous-traitants.

L'article 44, paragraphe 7 – préciser davantage:
- les «motifs importants d'intérêt général» au sens de l'article 44, paragraphe 1, point d); ainsi que:
- les critères et exigences concernant les garanties appropriées prévues à l'article 44, paragraphe 1, point h).

L'article 44 traite des dérogations à l'interdiction générale de transférer des données à caractère personnel vers un pays tiers ou une organisation internationale.

Le paragraphe 1, point d), prévoit qu'un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou une organisation internationale peut être autorisé à condition qu'il soit nécessaire pour des motifs importants d'intérêt général.

Le paragraphe 1, point h), prévoit qu'un transfert puisse être effectué à condition qu'il soit nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou le sous-traitant, qu'il ne puisse pas être qualifié de fréquent ou de massif et que le responsable du traitement ou le sous-traitant aient évalué toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données et offert, sur la base de cette évaluation, des garanties appropriées au regard de la protection des données à caractère personnel, s'il y a lieu.

Des actes délégués sont proposés pour préciser davantage ce qui constitue un «motif important d'intérêt général» concernant une dérogation à l'interdiction générale de transfert de données à caractère personnel vers des pays tiers ou des organisations internationales. La spécification de «motifs importants d'intérêt général» concerne un élément essentiel déterminant la licéité des transferts de données, et devrait par conséquent figurer dans le règlement lui-même.

Cette spécification doit être faite dans le texte du règlement lui-même, afin de garantir une mise en œuvre harmonisée dans l'UE.

Des actes délégués sont également prévus pour préciser les critères et exigences concernant les garanties appropriées visées à l'article 44, paragraphe 1, point h).

Le groupe de travail tient à souligner la nécessité de préciser davantage le terme d'«intérêt légitime» figurant à l'article 44, paragraphe 1, point h) du règlement car il est également mentionné en ce qui concerne la proposition d'acte délégué à l'article 6, paragraphe 5. Ces orientations pourraient être fournies par le comité européen de la protection des données, ou bien/et par ailleurs une liste non exhaustive d'exemples d'«intérêts légitimes» pourrait figurer dans un considérant du règlement.

S'agissant des garanties qui seraient considérées comme étant appropriées, il semble important de fournir de plus amples orientations, puisque cela concerne une dérogation à une

interdiction générale de transférer des données vers des pays tiers ou des organisations internationales, sur la base d'un intérêt légitime et sans intervention d'une autorité de contrôle.

Il serait toutefois impossible de couvrir dans le règlement lui-même l'ensemble des divers cas de figure (présents et futurs) propres à définir des garanties appropriées. Par conséquent, un instrument plus souple serait plus approprié.

Afin d'assurer l'harmonisation de l'interprétation et de la mise en œuvre, un acte délégué semble donc être un instrument approprié. En outre, le comité européen de la protection des données pourrait fournir des orientations pour préciser davantage les garanties appropriées mentionnées à l'article 44, paragraphe 1, point h).

L'article 79, paragraphe 7 – mise à jour des montants des amendes administratives visés à l'article 79, paragraphe 4, 5 et 6, en tenant compte des critères énoncés au paragraphe 2.

L'article 79 traite des sanctions administratives. Les paragraphes 4, 5 et 6, établissent le plafond maximal des amendes et le paragraphe 2 prévoit que la sanction administrative soit dans chaque cas, effective, proportionnée et dissuasive, et prévoit d'autres critères pour fixer l'ordre de grandeur de ces amendes.

Étant donné que le nouveau paquet juridique devrait être en vigueur pendant au moins plusieurs décennies, il est important de permettre l'indexation des montants des amendes et de prévoir ainsi leur évolution future.

Pour éviter des écarts entre États membres et assurer une harmonisation maximale dans l'UE, ces montants devraient être mis à jour au niveau de l'UE.

Afin d'assurer une plus grande clarté de compréhension à toutes les parties prenantes concernées, il convient d'utiliser un instrument juridiquement contraignant.

Par conséquent, il semble approprié d'utiliser des actes délégués pour la mise à jour des montants des amendes administratives visés aux paragraphes 4, 5 et 6 de l'article 79, en tenant compte des critères énoncés au paragraphe 2 de cet article.

L'article 81, paragraphe 3 – préciser les motifs d'intérêt général dans le domaine de la santé publique au sens du paragraphe 1, point b); ainsi que:
- les critères et exigences applicables aux garanties encadrant le traitement des données à caractère personnel aux fins prévues au paragraphe 1.

L'article 81 prévoit que, dans les limites du présent règlement et conformément à l'article 9, paragraphe 2, point h), les traitements des données à caractère personnel relatives à la santé doivent être effectués sur la base du droit de l'Union ou de la législation d'un État membre qui prévoient des garanties appropriées et spécifiques des intérêts légitimes de la personne concernée, et doivent être nécessaires aux fins de la médecine préventive ou du travail (point a)) ou pour des motifs d'intérêt général dans le domaine de la santé publique (point b))ou pour d'autres motifs d'intérêt général dans des domaines tels que la protection sociale (point c)).

Les actes délégués proposés serviraient à préciser davantage les motifs d'intérêt général dans le domaine de la santé publique, ainsi que les critères et exigences applicables aux garanties encadrant le traitement des données à caractère personnel aux fins prévues à l'article 81, paragraphe 1.

Une définition des motifs d'intérêt général dans le domaine de la santé publique et des critères et exigences applicables aux garanties devrait figurer dans un acte juridique contraignant. Étant donné qu'il est impossible de fournir de telles informations spécifiques dans le texte du règlement lui-même, un instrument différent serait plus approprié.

Cependant, l'article 81, paragraphe 1, prévoit de laisser une certaine latitude aux États membres pour établir dans leur législation nationale la licéité du traitement des données dans le secteur de la santé.

Par conséquent, les actes délégués semblent être les instruments les plus appropriés, sous réserve de l'article 81, paragraphe 1.

L’article 82, paragraphe 3 – préciser davantage les critères et exigences applicables aux garanties encadrant le traitement des données à caractère personnel aux fins prévues au paragraphe 1.

L'article 82 porte sur le traitement des données en matière d'emploi.

L'acte (ou les actes) délégué(s) proposé(s) servirai(en)t à préciser davantage les critères et conditions applicables aux garanties encadrant le traitement des données à caractère personnel en matière d'emploi.

Des critères et exigences supplémentaires applicables aux garanties encadrant le traitement des données à caractère personnel dans ce contexte devraient figurer dans un acte juridique contraignant. Étant donné qu'il est impossible de fournir de telles informations spécifiques dans le texte du règlement lui-même, un autre instrument serait plus approprié.

Néanmoins, l’article 82, paragraphe 1, prévoit de laisser aux États membres une certaine latitude pour établir dans leur législation nationale la licéité du traitement des données en matière d'emploi.

Par conséquent, les actes délégués semblent être l'instrument le plus approprié, sous réserve de l'article 82, paragraphe 1.

L'article 83, paragraphe 3 – préciser davantage:
- les critères et les exigences applicables au traitement de données à caractère personnel aux fins prévues à l'article 83, points 1) et 2); ainsi que:
- toute limitation nécessaire des droits d'information et d'accès de la personne concernée; et,
- les conditions et garanties applicables aux droits de la personne concernée dans les circonstances en cause.

L'article 83 concerne le traitement de données à des fins de recherche historique, statistique ou scientifique.

Le paragraphe 1 prévoit que, dans les limites du règlement, les données à caractère personnel ne peuvent faire l'objet d'un traitement à des fins de recherche historique, statistique ou scientifique que si ces finalités ne peuvent être atteintes d'une autre façon par un traitement de données qui ne permettent pas ou ne permettent plus d'identifier la personne concernée (point a)), ou si les données permettant de rattacher des informations à une personne concernée identifiée ou identifiable sont conservées séparément des autres informations, à condition que ces fins puissent être atteintes de cette manière (point b)).

Le paragraphe 2 prévoit que les organismes effectuant des recherches historiques, statistiques ou scientifiques ne peuvent publier ou divulguer des données à caractère personnel que si la personne concernée a donné son consentement (point a)), ou si la publication de données à caractère personnel est nécessaire pour présenter les résultats de la recherche ou pour faciliter la recherche, sous réserve que les libertés ou les droits fondamentaux de la personne concernée ne prévalent pas sur l'intérêt de la recherche (point b)), ou encore si la personne concernée a rendu publiques les données en cause (point c)).

Des actes délégués sont proposés afin de préciser davantage les critères et conditions applicables au traitement des données à caractère personnel, à des fins de recherche historique, statistique ou scientifique, si cela satisfait aux exigences et aux critères prévus aux paragraphes 1 et 2.

Les critères définis dans l'article en question sont déjà très clairs en ce sens que celui-ci prévoit que les données ne peuvent être traitées qu'à des fins historiques, statistiques ou scientifiques si cela satisfait aux deux conditions mentionnées. Dans tous les autres cas, le traitement est interdit. Ces critères constituent des éléments essentiels pour déterminer la licéité du traitement.

Si d'autres conditions doivent être remplies pour pouvoir traiter des données à des fins historiques, statistiques ou scientifiques, les exigences en la matière devraient figurer dans le texte du règlement proprement dit, afin d'assurer l'harmonisation des pratiques et la clarté et la sécurité juridiques pour toutes les parties prenantes concernées.

En ce qui concerne les actes délégués proposés pour préciser davantage les éventuelles limitations des droits à l'information et à l'accès de la personne concernée, ainsi que celles proposées en vue de préciser les conditions et garanties applicables aux droits de la personne concernée dans les circonstances en cause, on ne peut pas établir clairement où une possibilité de limiter ces droits est prévue (ce n'est pas non prévu dans les articles 14 et 15). En tout état de cause, comme il s'agit d'un élément essentiel, il devrait figurer dans le règlement lui-même.

S'il existe une possibilité pour que des organismes réalisant des recherches historiques, statistiques ou scientifiques limitent les droits de la personne concernée, il conviendrait de traiter cette question dans un document juridiquement contraignant afin d'assurer la clarté et la sécurité juridique pour les personnes concernées.

Par conséquent, il devrait en être pleinement tenu compte dans le texte du règlement lui-même, ou alors un acte délégué, déjà adopté au moment de l'entrée en vigueur de ce règlement, devrait préciser davantage ce point.

Des orientations supplémentaires, pourraient, le cas échéant, être fournies par le comité européen de la protection des données ou être précisées dans un code de conduite applicable dans tous les pays de l'UE.