Avis n° 23/2015 du 17 juin 2015

Objet: Avis d'initiative en vue du trilogue à venir sur les propositions de Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données telles que déposées par la Commission européenne et votées par le Parlement européen et le Conseil (CO-A-2015-024)

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 29 ;

Vu le rapport de M. Willem Debeuckelaere, Président;

Émet, le 17 juin 2015, l'avis suivant :

Table des matières

Introduction

1. À deux reprises déjà, la Commission de la protection de la vie privée (ci-après « la CPVP ») a pris position dans le cadre de la réforme du cadre règlementaire de la protection des données initiée le 25 janvier 2012 par la Commission européenne (ci-après la « COM »), réforme matérialisée par deux propositions de textes : (1) une proposition de *Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données* (COM(2012)0011 et ci-après « le projet de Règlement ») et (2) une proposition de *Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données* (COM(2012)0010).

2. Le 21 novembre 2012, la CPVP adoptait un avis critique sur le projet de Règlement tel que déposé par la COM[1].

3. Le 5 février 2014, la CPVP adoptait un avis tout aussi critique sur la proposition amendée de la Commission LIBE du Parlement européen (commission chef de file), position du 17 octobre 2013 confirmée par le Parlement européen (ci-après « le PE ») dans sa composition plénière en mars 2014[2].

4. Les négociations en cours au Conseil se sont achevées par l'adoption d'un texte reflétant le point de vue des 28 États membres de l'Union au terme du Conseil Justice et Affaires intérieures du 15 juin 2015[3].

5. Dans la perspective du trilogue imminent entre la COM, le PE et le Conseil, la CPVP choisit d'exposer *certaines préoccupations majeures au regard des 3 textes* ainsi que d'exprimer son soutien à l'une ou l'autre proposition sur la table. Son analyse ne se veut *pas*

---

[1] Avis d'initiative 35/2012 sur la proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Version néerlandaise : http://www.privacycommission.be/sites/privacycommission/files/documents/advies_35_2012_0.pdf, Version française : http://www.privacycommission.be/sites/privacycommission/files/documents/avis_35_2012_0.pdf, Version anglaise : http://www.privacycommission.be/sites/privacycommission/files/documents/Opinion_35_2012.pdf.

[2] Avis d'initiative 10/2014 portant sur la proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, tel que voté par la Commission LIBE du Parlement européen le 17 octobre 2013.

Version néerlandaise : http://www.privacycommission.be/sites/privacycommission/files/documents/advies_10_2014.pdf, Version française : http://www.privacycommission.be/sites/privacycommission/files/documents/avis_10_2014.pdf, Version anglaise : http://www.privacycommission.be/sites/privacycommission/files/documents/Opinion%2010-2014.pdf.

[3] http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/fr/pdf.

exhaustive mais ciblée. Ses choix et son positionnement sont guidés par le souci de garantir, dans le texte et en pratique, un niveau élevé de protection, au minimum équivalent à celui offert à ce jour par la directive 95/46/CE. Un niveau de protection inférieur à celui-ci serait inacceptable. Une attention particulière sera accordée à la proposition du Conseil sur laquelle la CPVP ne s'est pas encore exprimée mais plus généralement, la démarche de la CPVP s'inscrit, comme déjà mentionné, dans la perspective du trilogue.

6. Cet avis s'adresse dès lors directement à la COM, au PE – en particulier au rapporteur de la Commission LIBE J-F Albrecht ainsi qu'aux « shadow » rapporteurs – et au Conseil, en particulier à la présidence luxembourgeoise à venir ainsi qu'à tout autre stakeholder intéressé. Par cet avis, la CPVP s'adresse bien entendu aussi aux autorités et aux parlementaires belges ainsi qu'à toute autre personne intéressée.

Chapitre I – Dispositions générales

Article 1 - Objet et objectifs

7. La CPVP prend acte du point de vue du Conseil selon lequel le règlement n'empêche pas qu'un État membre adopte des dispositions spécifiques pour *adapter* les dispositions du Règlement. Ce qui importe à cet égard, c'est que cette possibilité n'entraîne aucune diminution du niveau de protection (voy. aussi le point 16 infra).

Article 2 - Champ d'application matériel

8. Dans les grandes lignes, la CPVP approuve le champ d'application matériel. Elle formule toutefois les remarques suivantes.

9. Bien que la CPVP puisse marquer son accord sur la disposition de l'article 2, (2), point a), elle fait remarquer l'absence d'aperçu clair et intelligible des activités qui ne relèvent pas de la sphère du droit européen. Plusieurs tentatives de préciser ce point - et donc d'indiquer quelles activités ne sont *pas* régies par le Règlement - se sont révélées insuffisantes. Il en résulte un manque de clarté persistant sur ce point, alors qu'il est toutefois évidemment important pour les États membres dans l'application de la législation.

10. La CPVP attire par ailleurs l'attention sur la nécessaire concordance entre l'article 2, point e) du projet de Règlement et l'article 1er du projet de Directive. Cela vaut également par extension pour les aspects communs des deux textes qui doivent être cohérents et compris de manière uniforme.

11. En ce qui concerne l'exception pour les finalités domestiques ("household exemption"), la CPVP constate que le Conseil a supprimé quelques mots de la proposition initiale de la COM. Il ajoute toutefois au considérant 15 que l'absence de lien avec une activité professionnelle ou commerciale est suffisante, ce qui emporte une extension de l'exception. La CPVP comprend l'idée sous-jacente (qui consiste à limiter la portée). Elle estime qu'il faut toutefois éviter d'étendre trop largement la portée de cette exception. La CPVP est plutôt favorable à une exception limitée qui ne vaut que pour des activités "purement" domestiques, comme c'est actuellement le cas aux termes de la directive 95/46/CE et consacré par la jurisprudence de la Cour de justice de Luxembourg[4]. Cela implique que le nombre de personnes que cible le traitement joue ou peut jouer un rôle, en ce sens que ce n'est que si le traitement vise un nombre limité de personnes que l'exception peut être appliquée. Pour ces différentes raisons, la CPVP adhère au texte du PE.

Article 3 - Champ d'application territorial

12. La CPVP approuve le champ d'application territorial tel que repris dans les textes de toutes les institutions concernées et marque sa préférence pour la formulation du Conseil qui souligne que le "suivi" (du comportement des personnes concernées) doit rester limité au comportement qui a lieu au sein de l'Union européenne.

13. La CPVP fait toutefois remarquer qu'il est recommandé et même nécessaire de décrire plus précisément le régime qui s'applique aux sous-traitants. En effet, l'application du règlement à l'égard des sous-traitants ne peut porter que sur les dispositions qui les concernent spécifiquement. Ce régime doit dès lors être clair. Il s'agit de l'article 26 (1a), (2) et (2a) (obligations du sous-traitant en ce qui concerne les sous-traitants ultérieurs et le contrat avec le responsable de traitement), de l'article 28 (2a) et (3) (obligation de conserver la documentation et de la mettre à disposition du responsable de traitement), de l'article 30 (1) et (2b) (mesures techniques et organisationnelles appropriées et fait de prévoir des instructions), de l'article 31 (2) (notifications des data breach au responsable de traitement), de l'article 35 (désignation du délégué à la protection des données (DPO), le cas échéant), des articles 38 et 39 (dispositions relatives aux codes de conduite et aux certifications – dans la mesure où cette possibilité s'applique aux sous-traitants, il en découle également des obligations) et de l'article 42 (relatif aux flux de données transfrontières).

[4] Notamment dans l'arrêt Lindqvist, CJ, 6 novembre 2003, C-101/01.

Article 4 – Définitions

14. Le cas échéant, les définitions sont analysées au regard des dispositions de fond qui en font état (comme l'établissement principal (Chapitre VI) et les données relatives à la santé (article 9)).

15. La CPVP renvoie en outre à ses remarques précédentes relatives à la *pseudonymisation*[5] dont il sera également question ailleurs dans cet avis au regard de l'article 10 (point 27 infra).

Chapitre II – Principes

Articles 5 et 6 – Principe de finalité et bases de légitimité

L'exercice d'une obligation légale et la poursuite d'un intérêt public – encadrement par la loi et adaptations admises

16. S'agissant de l'article 6.3. du projet de Règlement, la CPVP soutient le texte proposé par le Conseil. Le fondement juridique du traitement de données nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est tenu (art. 6 c)) et celui du traitement nécessaire à l'exécution d'une mission effectuée dans l'intérêt général ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement (art. 6 e)), doit, en application de l'article 6.3., être prévu par le droit de l'Union ou le droit national. La flexibilité accordée au secteur public aux termes de l'article 6.3. alinéa 3 du texte du Conseil (adaptation de certains aspects du projet de Règlement via la législation nationale) est particulièrement soutenue par la CPVP.

Les traitements ultérieurs "incompatibles" admissibles ?

17. Le principe de finalité est un des principes fondateurs de la protection des données personnelles. Outre l'article 6 § 1 b) de la directive 95/46/CE[6], il est consacré à l'article 8 de la Charte des droits fondamentaux de l'Union. C'est à l'aune de la finalité poursuivie par le responsable de traitement que peut notamment s'apprécier le respect du principe de proportionnalité, autre principe essentiel du régime de protection. Porter atteinte au principe de finalité, c'est nécessairement réduire la maîtrise informationnelle de la personne concernée et partant, réduire l'effectivité des droits qui lui sont reconnus et qui poursuivent l'objectif de réaliser cette maîtrise.

---

[5] Voir les remarques aux points 11 à 13 de l'avis n° 10/2014.

[6] Le principe de finalité est également consacré, dès 1981, à l'article 5 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) du Conseil de l'Europe à laquelle l'ensemble des États membres de l'Union sont Parties.

18. Si la CPVP est d'avis que des traitements ultérieurs de données doivent pouvoir s'opérer, elle n'en est pas moins d'avis que les données collectée ne peuvent, comme aujourd'hui requis par la directive 95/46/CE, être traitées pour une finalité incompatible avec la finalité initiale de leur collecte. Un traitement ultérieur pour une finalité incompatible n'est pas admissible.

19. La CPVP soutient dès lors le début de l'article 5b) proposé par les 3 institutions qui indique, dans des termes identiques à ceux de la directive 95/46/CE, que *"personal data shall be collected for specified, explicit and legitimate purposes and no further processed in a way incompatible with those purposes (purpose limitation)"*.

20. Quant à la position du Conseil, la CPVP est fermement opposée à l'article 6.4. qui indique, non sans créer une confusion certaine, qu'en cas de traitement pour une finalité *incompatible* avec la finalité initiale, le traitement ultérieur peut intervenir pour autant qu'il s'appuie sur une des bases de légitimité prévue à l'article 6.

21. Dans ce cas, la CPVP est d'avis que la base de légitimité de l'article 6f), soit l'intérêt légitime du responsable de traitement, doit être exclue. La CPVP revient à cet égard sur le point de vue qu'elle a antérieurement exprimé (point 36 de l'avis 35/2012) et au terme duquel elle indiquait que *"s'agissant d'un nouveau traitement, il doit satisfaire à l'ensemble des conditions légales et doit également trouver une base de légitimité. Toutes les hypothèses prévues à l'article 6 a) à f) devraient, dans ce cas, pouvoir s'appliquer"*. En effet, la CPVP est d'avis qu'il ne s'agit pas d'un "nouveau traitement" au sens propre du terme, dès lors qu'il s'inscrit dans le prolongement d'un premier traitement, pour lequel seul, la personne concernée a donné son consentement, sans information sur les traitements ultérieurs etc. Admettre un traitement ultérieur sur la seule base de l'intérêt légitime du responsable de traitement reviendrait à éroder, voire à nier, le principe de finalité. Subsidiairement, si le législateur européen devait s'engager dans cette voie, la CPVP insiste pour que l'ensemble des dispositions du régime de protection soient appliquées à ce "nouveau traitement" et non pas uniquement l'exigence d'une base de légitimité.

22. Enfin, la CPVP soutient l'initiative du Conseil de prévoir une certain nombre de critères à l'aune desquels la compatibilité du traitement ultérieur peut s'apprécier (article 6.3a)) avec toutefois les réserves suivantes : (1) il serait d'une part, plus exact de parler d'absence d'incompatibilité comme dans le libellé actuel de l'article 6 § 1 b) de la directive 95/46/CE et (2) d'autre part, l'existence de garanties adéquates (adequate safeguards) n'est pas un critère pertinent dans cette appréciation et ne pourrait justifier qu'un

traitement ultérieur "incompatible" soit légitimement opéré. Enfin, (3) cette liste ne peut être exhaustive. Une alternative serait d'en déplacer le contenu dans un considérant.

Article 9 – Catégories spéciales de données

Définition de la donnée relative à la santé

23. S'agissant des données relatives à la santé, la CPVP avait indiqué dans ses avis 35/2012 et 10/2014 précédents, que cette définition était trop large, ne tenait pas suffisamment compte des contextes multiples dans lesquels les traitements de données relatives à la santé peuvent intervenir, ni de la finalité poursuivie par le traitement et était, *in fine*, impraticable. Même dans sa version la plus restreinte proposée par le Conseil, les données de santé y demeurent définies comme *"data related to the physical or mental health of an individual which reveal information about his or her health status"* et le considérant 26 reste trop large[7].

24. À titre d'alternative à la limitation de la définition, laquelle alternative apporterait davantage de sécurité juridique, la CPVP suggère de maintenir une définition large de la donnée relative à la santé tout en prévoyant des conditions de traitement distinctes (base de légitimité notamment, qui peut les traiter, niveau de sécurisation) selon qu'elles sont traitées pour l'information sensible qu'elles révèlent ou non.

25. De manière générale, cette approche téléologique pour déterminer si *certaines* données à tout le moins (à l'exclusion des données génétiques par exemple), dont les données de santé, doivent être traitées selon les règles relatives aux données sensibles (telle celle adoptée par le Conseil de l'Europe aux termes de son projet de Convention 108 révisée) est davantage conforme à la réalité des risques encourus – notamment de discrimination – par la personne concernée ainsi qu'à la pratique de certaines autorités de protection des données dont la CPVP.

Quant aux bases de légitimité du traitement des données de santé

26. Si la CPVP soutient la proposition du Conseil qui ajoute un certain nombre de bases de légitimité utiles permettant le traitement de données relatives à la santé dans le secteur des soins de santé mais aussi de la sécurité sociale, de même qu'à des fins de

[7] Personal data concerning health should include (…) data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health of the data subject**7**; including information about the registration of the individual for the provision of health services (…); a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; (…) information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; (…) or any information on for example a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as for example from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

"management des systèmes et services de santé", elle est d'avis (voy. supra le point 23) qu'une définition plus limitée de la donnée relative à la santé eut été souhaitable.

Article 10 - Traitements ne permettant/ne requérant pas l'identification

27. Aucun des 3 textes sur la table ne satisfait la CPVP car aucun ne traduit adéquatement la réalité des (besoins des) choses en la matière.

28. Dans son avis 35/2012 (point 55), la CPVP relevait que dans sa version proposée par la COM, cet article 10 prévoyait que lorsque les données traitées ne permettent pas d'identifier une personne physique, le responsable du traitement n'est pas tenu d'obtenir des informations supplémentaires pour identifier la personne concernée afin de respecter les dispositions du projet de Règlement. Elle souhaitait que cette disposition soit éclaircie afin d'éviter d'en déduire qu'en application de celle-ci, le responsable de traitement ne serait plus tenu à aucune obligation.

29. Comme elle l'avait souligné dans son avis 10/2014, la CPVP juge inadmissible qu'un régime de protection "light" soit proposé (supprimant l'exercice des droits) dès lors que les données traitées ne permettrait pas (PE) ou n'exigerait pas (Conseil) d'identifier une personne physique. En particulier, il ne peut être question d'un régime de protection "allégé" lorsque des données pseudonymes sont traitées.

30. Par définition, la pseudonymisation n'empêche pas l'identification des personnes concernées, dès lors que la singularisation (« single out ») est toujours possible. Pour cette raison, la CPVP s'oppose en tout état de cause au paragraphe 2 de l'article 10. Subsidiairement, ne pourraient être visés au paragraphe 2 que les cas dans lesquels la personne ne peut être *authentifiée* par le responsable de traitement (elle ne peut démontrer qu'elle est bien celle qu'elle prétend être). Lorsque le responsable de traitement ne traite que des identifiants digitaux, il est important de ne pas imposer à la personne concernée, comme condition d'exercice de ses droits, de devoir apporter la preuve de son identité civile (par ex. en apportant une copie de sa carte d'identité). En effet, cette information (soit l'identité civile) ne sera d'aucune utilité pour authentifier la personne concernée puisque cette donnée n'aura pas été initialement traitée par le responsable de traitement.

31. L'ambition déclarée de la réforme est de moderniser l'encadrement juridique, de tenir compte de l'omniprésence d'Internet et de renforcer les droits des personnes concernées. Il ne peut dès lors, en conclusion, être question de réduire ces droits dans le cas de l'utilisation d'une identité digitale (distincte de l'identité civile). Une disposition qui

refuserait, par exemple, le droit d'accès à défaut de pouvoir s'identifier ne tient pas compte de l'évolution des comportements des internautes et du développement d'une identité digitale parallèlement à l'identité civile.

32. De manière générale, la CPVP juge essentiel que la notion d'identification ne soit pas exclusivement entendue comme permettant de révéler l'identité civile des personnes concernées (nom, prénom, adresse), mais bien comprise de manière élargie, incluant la singularisation par des identifiants digitaux. La position du Conseil au considérant 52 est sur ce point la bienvenue.

Chapitre III: Droits des personnes concernées

33. Le Chapitre III est consacré aux droits de la personne concernée. La CPVP est particulièrement soucieuse de garantir un haut niveau de protection aux personnes concernées, en leur conférant des droits effectifs. Tout affaiblissement du niveau de protection actuellement garanti par la directive 95/46/CE est inacceptable, car en rupture avec l'acquis communautaire et, plus politiquement parlant, contraire à l'objectif déclaré de la réforme engagée. De manière générale, la CPVP est opposée à l'application de l'approche par les risques ('risk based approach') aux droits de la personne concernée.

Articles 14 et 14a - Droit à l'information en cas de collectes directe et indirecte

34. L'information de la personne concernée est essentielle dès lors qu'elle permet l'exercice des autres droits dont elle est titulaire, tels, par exemple, le droit d'opposition.

Un contenu enrichi pour une transparence accrue

35. La CPVP accueille favorablement les propositions d'ajouts d'éléments d'information visant à accroître la transparence à l'égard de la personne concernée et lui permettant, *de facto*, d'exercer un meilleur contrôle sur ses données tels que : le délai de conservation (formulé de manière exacte en durée quantifiée lorsque cela est possible ou par référence à certains paramètres), les mesures de sécurité mises en place, l'origine des données (collecte indirecte), l'intention d'effectuer un transfert vers un pays tiers et le niveau de protection offert (les garanties mises en oeuvre devraient être également communiquées dès lors qu'elles confèrent elles-mêmes des droits aux personnes concernées), la logique qui préside aux traitements, l'existence de *l'ensemble* des droits reconnus à la personne concernée ainsi que celle de voies de recours auprès de l'autorité de contrôle de protection des données (DPA).

Le moment de la communication de l'information

36. La CPVP est d'avis que l'information doit être donnée à la personne concernée le plus rapidement possible. La CPVP soutient les propositions de texte visant à préciser ce moment au niveau européen. La CPVP est d'avis que cette information doit, en cas de collecte indirecte, être donnée dès l'enregistrement des données ou, dans un délai raisonnable - avec un délai maximal prévu d'1 mois – comme proposé par le Conseil. En cas de collecte directe, l'information doit être donnée au moment où l'information est recueillie ou dans un délai raisonnable (avec un maximum prévu également).

Les exceptions à la communication de l'information

37. La CPVP s'oppose à la suppression, sans autre nuance, du droit à l'information de la personne concernée dès lors que le responsable de traitement serait soumis au secret professionnel. Comme elle l'a précédemment exposé dans son avis 10/2014 sur la position du PE (point 18 et s.), le secret professionnel vise à limiter la communication d'informations couvertes par ce secret aux seuls tiers. Les exceptions autorisées en cas de collecte indirecte ne doivent être ni étendues ni réduites par rapport à celles prévues par la directive 95/46/CE. Ainsi, l'exception d'information dès lors que celle – ci se révèle impossible ou impliquerait des efforts disproportionnés doit demeurer limitée aux traitements réalisés à des fins de recherche scientifique, historique et statistique.

Article 15 - Droit d'accès

Quant aux conditions du droit d'accès

38. La CPVP soutient la gratuité de l'exercice du droit d'accès tel que proposé par le Conseil. Ce droit d'accès doit pouvoir s'exercer à intervalles réguliers (Conseil) et le responsable du traitement doit y donner suite dans un délai donné. L'article 10 de la LVP prévoit actuellement un délai maximal de 45 jours qui se révèle praticable.

Quant au contenu du droit d'accès

39. La CPVP plaide pour un libellé clair qui distingue le droit d'accès du droit d'obtention d'une copie (tel que clairement énoncé par la CJUE dans son arrêt YS c. Pays-Bas du 17 juillet 2014) et du droit à la portabilité.

40. La CPVP soutient la proposition du PE, laquelle complète le régime de la directive 95/46/CE et apporte un certain nombre de correctifs à la proposition de la COM. L'accès à la logique qui sous-tend tout traitement, déjà prévu par la directive 95/46/CE mais au seul minimum pour les décisions automatisées, constitue un renforcement essentiel de la protection de la personne concernée (PE). La CPVP plaide toutefois pour que le droit d'accès emporte également l'accès aux garanties encadrant les flux transfrontières vers des pays tiers (Conseil).

Quant aux exceptions au droit d'accès

41. La CPVP réitère sa remarque quant à l'exception prévue pour les responsables de traitement qui seraient soumis au secret professionnel. Celui-ci ne limite que la communication de données aux tiers. La CPVP s'oppose par ailleurs à l'exception tirée du droit des affaires telle que proposée par le Conseil *("the right to obtain a copy referred to in §1b) shall not apply where such a copy cannot be provided without disclosing personal data of other data subjects or trade secrets of the controller"*). Cette référence au secret des affaires figure déjà au considérant 41 de la directive 95/46/CE. Comme dans ce considérant, un équilibre doit certes être trouvé mais il est exclu que la personne concernée n'ait accès à aucune information la concernant. Ici aussi, l'accès doit être distingué de l'obtention d'une copie.

Article 16 – Droit de rectification

42. La CPVP soutient la proposition formulée par le PE, lequel s'appuie sur la proposition de la COM en la précisant toutefois dans un considérant. Ce considérant explicite que dans les cas où il n'est pas possible de déterminer si oui ou non la donnée est effectivement exacte ou inexacte, la donnée devrait être bloquée tant que la question n'a pas été clarifiée.

43. La CPVP s'oppose à tout affaiblissement de ce droit de rectification par l'insertion de conditions floues et de nature à en restreindre la portée effective tel que proposé par le Conseil. Ainsi, la CPVP s'oppose au segment de phrase *"Having regard to the purposes"*. Le droit de rectification n'a pas à s'apprécier en fonction de la finalité. Si ce libellé devait être conservé, le niveau de protection serait affaibli par rapport au niveau actuellement garanti par la directive 95/46/CE.

Article 18 - Droit à la portabilité

Sur le « principe » du droit

44. La CPVP soutient la proposition formulée par le PE qui lui semble trouver le juste équilibre en la matière. En effet, tout comme le Conseil, le PE énonce que la personne aura le droit d'obtenir du responsable de traitement une copie des données dans un format électronique, interopérable et communément utilisé. La proposition du PE ajoute que *"Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject"*. Dans la mesure où elle n'est prévue qu'en cas de demande de la personne concernée, cette précision est de nature à renforcer le droit consacré sans faire peser d'obligations systématiques et/ou déraisonnables au responsable de traitement.

Quant aux données visées

45. La CPVP n'est pas entièrement satisfaite par les propositions de texte sur la table. Elle est opposée à la limitation de ce droit de la personne concernée de recevoir les données la concernant au seul cas, tel que proposé par le Conseil, où elle aurait *consenti* à les fournir au responsable de traitement (le consentement comme base de légitimité du traitement). La CPVP suggère d'y ajouter le cas où le traitement de données s'inscrit dans le cadre de la réalisation de l'intérêt légitime du responsable de traitement. Il est par ailleurs essentiel que ce "nouveau droit" ne soit pas limité à la réception de données relatives à la personne concernée mais porte également sur ce que cette dernière aurait fourni au responsable de traitement relativement à d'autres.

Article 19 - Droit d'opposition

Quand le droit d'opposition peut-il s'exercer ? Bases de légitimité du traitement auquel la personne concernée s'oppose

46. La CPVP plaide pour un droit d'opposition dans le plus large nombre d'hypothèses possibles, au minimum dans les cas autorisés par la directive 95/46/CE, ce qui n'est formellement le cas dans aucun des textes proposés (COM, PE et Conseil).

47. La CPVP relève qu'aux termes des 3 textes sur la table, le droit d'opposition disparaîtra dans les cas où le consentement de la personne concernée constitue la base légale d'un traitement de données. Comme explicité dans son avis 35/2012 précédent, la CPVP juge cette suppression inacceptable car elle impliquerait un affaiblissement des droits des personnes concernés. Le droit au retrait du consentement ne peut compenser cette suppression dès lors que le retrait du consentement ne compromet pas, à l'inverse du droit d'opposition, la licéité du traitement antérieurement opéré (voir points 75 et s. de l'avis 35/2012).

48. Hormis la suppression du droit d'opposition aux traitements fondés sur le consentement de la personne concernée, la CPVP soutient la position du PE qui conserve l'acquis de la directive 95/46/CE.

49. A l'inverse, la CPVP serait particulièrement préoccupée par et par ailleurs totalement opposée à la suppression du droit d'opposition aux traitements de données fondés sur la mission d'intérêt public du responsable de traitement ou sur l'intérêt général poursuivi par ce dernier.

Quand le droit d'opposition peut-il s'exercer ? Motifs à invoquer par la personne concernée

50. La CPVP est d'avis que le droit d'opposition doit, comme c'est le cas actuellement tant aux termes de la directive 95/46/CE qu'en application de l'article 12 de la LVP, être inconditionnel au regard de traitements de données opérés à des fins de marketing direct.

51. La CPVP soutient dès lors la position du PE qui préserve cet acquis.

Quand est-il fait droit au droit d'opposition ? Appréciation par le responsable de traitement ? Charge de la preuve ?

52. Hormis la position du PE dans les seuls cas où le traitement est fondé sur l'intérêt légitime du responsable de traitement, le responsable de traitement peut, aux termes des 3 textes sur la table, invoquer des raisons légitimes et impérieuses pour ne pas donner suite à l'opposition formulée. Comme elle l'a exprimé dans ses avis 35/2012 (point 77) et 10/2014 (points 32 et S.), la CPVP juge que cette balance des intérêts à opérer par le responsable de traitement lui-même crée le risque inacceptable de voir les responsables de traitement continuellement invoquer leur intérêt légitime pour s'opposer à l'exercice du droit d'opposition.

Article 20 – Profilage

53. Aucun des 3 textes sur la table ne satisfait pleinement la CPVP. Elle est toutefois d'avis que la proposition la plus aboutie est celle du Conseil. La CPVP ne pourrait cependant la soutenir que si les éléments suivants étaient pris en compte:

- Le profilage réalisé à des fins de marketing direct, qui se traduit sous la forme de messages publicitaires spécifiques, doit entrer dans le champ d'application de cet article. Limiter ce dernier à des *décisions* ayant des effets juridiques ou des effets significatifs à l'égard des personnes concernées est insuffisant et limite la portée de la disposition. La CPVP préconise d'ajouter la prise de *mesures* au champ d'application défini par le §1. Celles-ci ne doivent pas produire des effets juridiques comme proposé par la COM.

- Le profilage devrait viser, dans sa définition prévue à l'article 4, tant la constitution d'un profil que l'application d'un profil.

54. De manière plus générale, la CPVP salue la volonté de tenter de règlementer le profilage. Cette volonté ne doit en aucun cas supprimer la protection offerte aujourd'hui par l'article 15 de la directive 95/46/CE (interdiction qui reconnait à la personne un droit et non une seule faculté d'opposition).

Article 21 – Exceptions

55. La CPVP soutient la proposition formulée par le PE à l'exception d'un point.

56. En effet, contrairement aux propositions de la COM et du Conseil qui allongent la liste des motifs pour lesquels les États membres de l'Union peuvent déroger à certains droits et obligations, le PE s'en tient à la liste actuellement prévue par la directive 95/46/CE à l'exception d'un aspect (auquel la CPVP ne souscrit donc pas).

57. La CPVP ne soutient en effet pas la suppression de la notion d'« intérêt général de l'Union ou d'un État membre » (article 21.1 c)) et sa réduction aux seules *« taxation matters »*. Elle privilégie le maintien des exceptions formulées par l'article 13 de la directive 95/46/CE dont la pertinence n'a, à sa connaissance, pas été remise en cause. Un régime juridique inapplicable à défaut de dérogations adéquates entraîne, entre autres effets pervers, les risques de contournement systématique des dispositions et d'interprétation erronée ou volontairement biaisée. En d'autres termes, mieux vaut un régime de protection qui prévoit des exceptions appropriées qu'un régime indistinctement théoriquement applicable mais inapplicable en pratique, par exemple pour le secteur public.

58. Le PE réduit par ailleurs les articles auxquels il peut être dérogé au titre d'exception, ce que soutient la CPVP.

59. Les principes de base énoncés à l'article 5a)-e) demeurent applicables en toute circonstance de même que l'article 20 (profilage) ce qui n'est, par exemple, pas le cas dans le texte original de la COM. Dans le même esprit de protection renforcée, le PE reçoit le soutien de la CPVP en ce qu'il ajoute un certain nombre d'éléments devant figurer, *sans exception*, dans les législations nationales dérogatoires, s'appuyant pour se faire sur la jurisprudence constante de la Cour européenne des droits de l'homme.

Chapitre IV: Responsabilisation du responsable de traitement et risk based approach

Principe d'accountability

60. La CPVP apprécie l'ancrage du principe de responsabilisation des responsables de traitement (accountability) imposant à ceux-ci la mise en place de mesures préventives qui ont pour objectif d'éviter toute atteinte éventuelle à la protection des données[8]. Cependant, la CPVP estime que le principe ne devrait pas viser les seuls responsables de traitement mais également les sous-traitants dès lors que les mécanismes listés de mise en œuvre de ce principe de responsabilisation concernent également ce dernier.

[8] Voir points 83 et 84 de l'avis 35/2012.

61. Si la CPVP plaide pour un système d'obligations cohérentes et basées sur l'appréciation concrète du risque réel induit par les traitements réalisés, elle estime qu'une approche fondée sur les risques ne devrait avoir ni pour objectif ni pour conséquence d'entamer la substance même de la responsabilisation (accountability) des acteurs. Les responsables et sous-traitants doivent toujours pouvoir être à même de démontrer le respect de leurs obligations et cela, à l'égard de n'importe quel traitement, quels que soit la nature de celui-ci, le contexte dans lequel il est opéré ou les risques liés à celui-ci.

62. L'approche par les risques permet une *adaptation d*es obligations. Elle ne convient dès lors pas à toutes les obligations pesant sur le responsable de traitement et le sous-traitant. Si le responsable de traitement peut adapter, par exemple, la sécurité du traitement en fonction des risques (au vu de la multitude des solutions disponibles relatives à la sécurité), il ne lui est par contre pas possible de moduler son obligation de désigner un représentant ou de documenter les traitements qu'il opère. Pour ce type d'obligation, les responsables et sous-traitants ont besoin de sécurité juridique et de pouvoir déterminer facilement s'ils sont soumis ou non à l'obligation en question. La CPVP estime à cet égard que la position du Conseil entraine parfois une insécurité juridique, notamment lorsqu'elle conduit le responsable de traitement à ne pas pouvoir déterminer de manière certaine s'il est soumis ou non à une obligation juridique donnée.

Article 23 - Protection des données dès la conception et protection des données par défaut (Privacy by design and by default)

63. La CPVP a déjà exprimé son soutien pour l'insertion de ces principes de « privacy by design » et de « privacy by default ». Néanmoins, la CPVP a également déjà souligné le fait que ces principes devraient également être mis en œuvre par les concepteurs de produits ou de logiciels dès lors qu'ils sont responsables de la conception des systèmes de traitement[9]. Par conséquent, la CPVP soutient la référence faite par le Conseil au considérant 61 à la nécessité d'encourager l'application des principes de « Privacy by Design » et « Privacy by default » par ces concepteurs.

Article 25 - Le représentant

64. La CPVP souligne à nouveau la nécessité de clarifier le rôle du représentant[10]. Il semble acquis par les 3 institutions qu'il sera un point de contact au sein de l'Union pour les autorités de protection de données[11].

---

[9] Point 87 de l'Avis 35/2012.

[10] Voir point 89 de l'Avis 35/2012.

[11] Voir notamment le considérant 63 et les articles 53.1c du PE, de la COM (53.1a du Conseil), 25.3a du Conseil et 29 (du PE et de la COM).

65. Cependant, son rôle en termes de responsabilité juridique reste flou. L'article 78 relatif aux sanctions, tel qu'actuellement formulé dans les positions du PE et de la COM, fait référence au fait que les sanctions sont applicables au représentant. Le Considérant 63 du Conseil indique également que le représentant doit pouvoir être soumis à des mesures d'exécution (« enforcement actions ») lorsque le responsable de traitement ne respecte pas ses obligations. Cependant aucune institution ne vise directement le représentant à l'article 79 relatif aux sanctions administratives.

66. Par ailleurs, l'article 78 permet aux États membres, de prévoir des sanctions (notamment pénales). En ne stipulant pas clairement le fait que les obligations juridiques du responsable du traitement incombent également au représentant, la mise en place d'une responsabilité pénale directe peut poser problème. On ne peut en effet être pénalement responsable pour les fautes d'autrui.

67. La CPVP attire également l'attention sur le fait que lors de ce choix (de permettre ou de ne pas permettre de sanctionner le représentant), il faudra nécessairement prendre en considération les conséquences pratiques de ce choix. Ainsi, les risques liés à cette fonction pourraient freiner la désignation de représentants.

68. Concernant les exceptions à l'obligation de désigner un représentant (article 25.2.), la CPVP souscrit à la position du Conseil qui supprime l'exception qui vise l'hypothèse où le responsable du traitement est établi dans un pays tiers assurant un niveau de protection adéquat (article 25.2. a)[12]. Quant à l'exception relative aux risques (art. 25.2.b), la CPVP soutient la proposition du PE qui se réfère au nombre de personnes concernées visées et à la nature des données concernées[13].

Article 26 - Responsable de traitement et sous-traitant

69. La CPVP soutient la position du Conseil aux paragraphes 1A et 2A de l'article 26 qui vise à encadrer juridiquement la sous-traitance ultérieure (le fait pour un sous-traitant de lui-même sous-traiter une partie de ses activités). Sur ce point, la position du PE se limite à permettre au responsable de traitement et au sous-traitant de convenir contractuellement des conditions de la sous-traitance ultérieure ; l'accord préalable du responsable de traitement n'est donné que comme une possibilité pouvant être convenue. La CPVP estime toutefois que si un sous-traitant pouvait, aux termes du projet de Règlement, décider seul de faire appel à un sous-traitant ultérieur, sans transparence ni accord préalable du

[12] Voir points 91 de l'avis 35/2012.

[13] La CPVP avait déjà justifié son scepticisme à l'égard du critère du nombre d'employés présenté par la COM (point 92 de l'avis 35/2012) et elle estime également que le critère des risques du Conseil est trop flou pour apporter une sécurité juridique aux responsables de traitement.

responsable de traitement, cette décision devrait entrainer sa requalification en responsable de traitement. En effet, c'est une décision importante relative au traitement de données et elle ne peut appartenir qu'au responsable de traitement (qui par ailleurs est tenu de choisir des sous-traitants présentant certaines garanties[14]).

70. La position de la COM est plus stricte car elle impose l'accord préalable du responsable du traitement, sans toutefois indiquer si l'accord peut être généralement donné ou si celui-ci doit être spécifique, à chaque nouvelle sous-traitance ultérieure. Si elle a l'avantage de laisser le contrôle de cette question au responsable de traitement, l'inconvénient de cette position est qu'elle implique le risque d'une interprétation stricte (accord nécessairement spécifique), ce qui serait impraticable pour certains services, tel qu'en matière de cloud computing.

71. C'est pourquoi, la position du Conseil est certainement la plus équilibrée car elle permet d'éviter la confusion des rôles de chacun tout en permettant une certaine flexibilité pour les parties contractantes. La sous-traitance ultérieure ne pourra avoir lieu qu'en pleine transparence à l'égard du responsable de traitement et avec son autorisation. En fonction des circonstances de l'espèce, par exemple de la sensibilité du secteur concerné, l'accord pourra soit être spécifique, soit général. S'il est généralement donné, le responsable de traitement a toujours l'occasion d'objecter à un changement. Par ailleurs, le Conseil prévoit que le sous-traitant ultérieur devra être tenu des mêmes obligations contractuelles que le sous-traitant initial. C'est un point décisif. Il est également prévu que le sous-traitant principal reste responsable à l'égard du responsable de traitement pour le non-respect des garanties contractuelles par le sous-traitant ultérieur.

72. Ces conditions sont celles qui aujourd'hui, figurent déjà dans les clauses contractuelles type 2010/87/UE adoptées par la COM et validées par les États membres au sein du Comité 31 et davantage développées par le Groupe de l'article 29[15].

73. Si la sous-traitance ultérieure était plutôt rare jusqu'il y a quelques années, elle tend à présent à se développer considérablement. Partant, la CPVP est d'avis que pour que le projet de Règlement réponde adéquatement aux développements technologiques, il est essentiel qu'il encadre ces activités.

Article 28- Documentation

Qui doit documenter ?

[14] Voir l'art. 26.1.

[15] Voir WP196 sur le cloud computing et WP195 sur les BCR sous-traitants.

74. Comme précédemment indiqué[16], la CPVP est favorable à l'obligation de documentation interne en lieu et place de la déclaration préalable de traitements, pour autant que l'intérêt particulier de cette déclaration - soit l'obligation pour le déclarant de se poser les questions pertinentes au regard des principes de protection des données concernant ses traitements – demeure.

75. La CPVP soutient la position du Conseil qui vise à distinguer la documentation réalisée par le responsable de traitement de celle réalisée par le sous-traitant. Cette distinction permet d'éviter pour une grande partie une duplication de l'exercice.

Contenu de la documentation ?

76. Pour ce qui concerne le contenu de la documentation, la CPVP soutiendrait une position intermédiaire à celles proposées actuellement par les 3 institutions. Plutôt que d'imposer un contenu minimaliste tel que formulé par le PE ou une documentation systématiquement extensive, comme le proposent la COM et le Conseil, la CPVP suggère d'introduire une distinction entre des éléments de base qui devront toujours être documentés et d'autres informations pour lesquelles le responsable du traitement ou le sous-traitant seront autorisés à ne pas documenter dans la mesure où ils peuvent motiver, sur la base d'un fondement raisonnable, la raison pour laquelle telle documentation est impossible en pratique.

77. La CPVP est d'avis que les éléments essentiels suivants doivent figurer dans la documentation : données de contact du responsable du traitement ainsi que de la personne qui peut concrètement être contactée par la personne concernée pour l'exercice de ses droits ainsi que l'identité des sous-traitants, du représentant éventuel, du délégué à la protection des données (DPO) et une description succincte des traitements (reprenant les finalités de ceux-ci, les catégories de données et les destinataires).

78. Par ailleurs, dès lors que la CPVP estime qu'il n'est pas toujours possible pour le responsable du traitement de déterminer au préalable la durée de conservation des données qu'il appliquera, la CPVP soutient la position du Conseil qui vise à ne prévoir cette information que lorsque cela est possible, le cas échéant en faisant référence à des paramètres (tels le délai de prescription, l'échéance du contrat) plutôt qu'une durée quantifiée.

Les exceptions à l'obligation de documentation

[16] Point 61 avis 10/2014.

79. En ce qui concerne les exceptions à la documentation, la CPVP estime que les exceptions proposées par la COM sont trop larges dès lors que bon nombre d'entreprises emploient moins de 250 personnes. La proposition du Conseil qui prévoit la combinaison de ce critère avec une approche sur les risques est quant à elle trop floue car elle ne permettra pas aux acteurs de savoir clairement s'ils sont soumis ou non à l'obligation de documentation (voy. supra le point 62). Par ailleurs, l'exercice de la démonstration de l'absence de risques devra nécessairement être documenté afin de pouvoir justifier à l'autorité de protection des données (ci-après « la DPA ») la raison pour laquelle le traitement n'est pas documenté. La CPVP se demande dès lors dans quelle mesure le fait de devoir documenter l'absence de risque - et donc la justification de l'application de l'exception - n'entraine finalement pas plus de difficultés que de simplement documenter le traitement. En clair, est-ce que les conditions pour pouvoir bénéficier de l'exception ne sont pas plus complexes (et entrainant une insécurité juridique) que celles qui consistent à satisfaire à l'obligation ? Par ailleurs, les exceptions susmentionnées ne devraient pas s'appliquer aux "données à caractère personnel sensibles".

Article 30 - Sécurité

A qui incombe l'obligation de sécurité ?

80. La CPVP apprécie que les 3 institutions s'accordent pour désormais imposer les obligations en matière de sécurité également directement au sous-traitant (article 30.1)[17].

Contenu de la politique de sécurité

81. Par ailleurs, la CPVP salue la position du PE quant aux précisions apportées au contenu de la politique de sécurité (art. 30.1a).

Articles 31 et 32 - Notification des violations de sécurité

Notification aux DPA

82. La CPVP soutient la position du Conseil qui vise à limiter les notifications d'atteintes à la sécurité aux cas pouvant présenter des risques importants pour les droits et liberté des individus. Comme déjà énoncé dans un précédent avis[18], il faut avant tout éviter une notification excessive de petites violations aux DPA et prévoir que seules les violations ayant de graves conséquences ou concernant un grand nombre de personnes doivent être notifiées.

Notification aux personnes concernées

[17] Dans la pratique, cela correspond à l'article 16, § 4 de la loi belge relative à la protection des données.

[18] Point 109 de l'avis 35/2012.

83. Par contre, pour ce qui concerne la notification des atteintes à la sécurité aux personnes concernées, la CPVP estime qu'il serait préférable d'utiliser les critères déjà exploités dans la directive ePrivacy[19] L'existence de critères différents pour le secteur des communications électroniques pourrait entrainer également des difficultés de mise en œuvre. Ces critères ont par ailleurs déjà fait l'objet d'analyses et de clarification de la part de l'ENISA et du Groupe de l'article 29 (WP 213)[20].

Article 33 - Analyse d'impact relative à la protection des données (PIA)

Quels sont les traitements soumis au PIA ? Que couvre-t-il ?

84. La CPVP est favorable à l'instrument *« Analyse d'impact relatif à la protection des données »* pour autant que celui-ci porte sur des traitements adéquatement identifiés comme particulièrement « risqués » et pour autant que le PIA soit effectif, concret et réalisé de la manière la plus impartiale possible[21].

85. La CPVP soutient les positions du PE et du Conseil qui visent *à ne pas* limiter l'analyse aux impacts strictement liés à la protection des données mais plus globalement aux droits et libertés des individus.

86. Elle accueille également favorablement le principe du « lifecycle data protection management » développée par le PE ainsi que celui d'une évaluation périodique de l'analyse d'impact (article 33a. du PE).

87. La CPVP estime que, s'il faut naturellement éviter qu'un même traitement fasse l'objet d'une analyse d'impact à la fois par le responsable et le sous-traitant, l'intervention du sous-traitant est cependant parfois cruciale dès lors qu'il peut avoir connaissance d'éléments techniques déterminants. La CPVP soutient dès lors les positions de la COM et du PE qui prévoient la contribution du sous-traitant.

Exception

88. Enfin, concernant l'exemption relative au secteur public, la CPVP accueille favorablement la proposition du Conseil à l'article 33.5 qui vise à renvoyer, non pas uniquement aux traitements effectués dans le cadre de la législation européenne mais également à celle des États membres[22]. La CPVP soutient le principe d'exempter de l'obligation des PIA les

---

[19] « En cas de violation de nature à affecter les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier ».

[20] Recommendation for a methodology of the assessment of severity of personal data breaches: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity

[21] Point 67 de l'avis 10/2014.

[22] Point 116 de l'avis 35/2012.

traitements se fondant sur une législation nationale mais uniquement dans la mesure où celle-ci aurait déjà fait l'objet d'un avis obligatoire par la DPA concernée[23] (voir l'article 52.1.f de la COM et du PE, ainsi que l'article 53.1c.aa du Conseil[24]).

Article 34 - Autorisation et consultation préalables des DPA

89. La CPVP soutient la position du Conseil à l'article 34.7a qui vise à permettre aux États membres de maintenir un système d'autorisations préalables pour les traitements réalisés pour des tâches d'intérêt public, notamment dans le cadre de la protection sociale et de la santé publique. Ce paragraphe permet le maintien du système belge de Comités sectoriels, mis en place pour la protection des données à caractère personnel dans le cadre du secteur public, ce que la CPVP avait déjà souhaité dans ses précédents avis[25].

Articles 35 à 37 - Le délégué à la protection des données (DPO)

90. S'agissant du DPO, la CPVP s'est jusqu'ici opposée à sa désignation obligatoire et ce, quelles que soient les hypothèses dans lesquelles tant la COM que le PE ont prévu que cette désignation devait intervenir. Subsidiairement, la CPVP a jugé jusqu'ici que les cas dans lesquels cette nomination est obligatoire étaient, pour certains à tout le moins, dépourvus de pertinence (points 126 et s. de l'avis 35/2012 et 71 et suivants de l'avis 10/2014).

91. La CPVP confirme sa position antérieure et renvoie à ses avis précédents. Elle ajoute qu'il est essentiel que le DPO dispose de compétences pluridisciplinaires, tant juridiques que techniques. Le seul bagage juridique en matière de protection des données personnelles est insuffisant.

Article 38 - Codes de conduite

92. La proposition du Conseil dépasse le simple encouragement des codes de conduite et de l'émission d'avis par les DPA (positions de la COM et du PE), et prévoit des conséquences juridiques à l'approbation des codes de conduite.

93. Ainsi, le Conseil prévoit que les codes de conduite approuvés peuvent être considérés comme des garanties appropriées (adequate safeguards) pour le transfert de données hors de l'Union européenne. Si les parties au trilogue s'engagent effectivement dans cette voie visant à permettre l'utilisation des codes de conduite sectoriels comme outil de transferts de données, la CPVP soutiendrait également la position du Conseil qui vise à

---

[23] *Ibidem*.

[24] Dans le cadre de cette consultation, la DPA compétente déterminera si un PIA est nécessaire et utile ainsi que la manière dont il doit être réalisé.

[25] Points 120 et s. de l'avis 35/2015 ainsi que les points 68 et s. de l'avis 10/2014.

conditionner cette reconnaissance au fait que ces outils impliquent des engagements juridiquement contraignants et exécutables par les personnes concernées[26].

94. Le Conseil prévoit également que l'adhésion à un code de conduite approuvé sera un facteur qui devra nécessairement être pris en considération par la DPA lorsqu'elle décidera du montant de la sanction qui sera imposée à la suite d'une violation. La CPVP se demande si l'objectif visé ici est de considérer cette adhésion comme un facteur pouvant réduire le montant de la sanction, ou si au contraire, il s'agit là d'un facteur aggravant[27]. En tout état de cause, la CPVP est opposée à l'idée même que l'adhésion à un code de conduite soit un facteur nécessairement/systématiquement pris en considération lors de l'évaluation du montant des sanctions. Les autorités devraient rester libres de prendre ou non en considération cette adhésion.

95. La CPVP soutient également l'idée que l'adhésion à un code de conduite n'établit pas en soi le respect du règlement (voir l'article 22.2b du Conseil) et que les compétences de contrôle et d'investigation des DPA demeurent intactes (voir l'article 38.1b et 38a.1 du Conseil).

96. En outre, si le Règlement devait permettre l'approbation des codes de conduite, il faudrait nécessairement prévoir des mesures de publicité des codes approuvés (38.5a du Conseil).

97. Enfin, la CPVP avait déjà indiqué qu'il ne devrait pas être de la compétence de la COM mais bien du Comité européen de la protection des données (ci-après « l'EDPB ») de constater qu'un code de conduite est d'applicabilité générale sur le territoire de l'Union (article 38.4)[28]. La CPVP accueille dès lors favorablement l'intervention prévue de l'EDPB par le PE et le Conseil. Cependant, dans ces deux textes, l'EDPB n'a qu'un rôle d'avis et l'approbation européenne des codes de conduite est laissée à la compétence de la COM. La CPVP estime que, dans l'hypothèse où l'EDPB aurait la possibilité d'adopter des décisions contraignantes (ce qui est désormais proposé par le PE et le Conseil et ce que soutient la CPVP – voy. infra points 140 et 144), l'EDPB devrait recevoir également cette compétence d'approbation européenne des codes de conduite.

---

[26] Pour le surplus, voir le point 120 du présent avis.

[27] En effet, au lieu de vouloir alléger les sanctions au titre de récompense à l'adhésion à un code de conduite, on pourrait éventuellement considérer comme étant que le fait pour un responsable de traitement de ne pas respecter pas le règlement malgré cette adhésion soit considéré comme un facteur aggravant.

[28] Point 135 de l'avis 35/2012.

Article 39 – Certification

98. Le Conseil ainsi que le PE proposent un *corpus* plus abouti de règles relatives à la certification.

99. Une différence entre les deux propositions concerne la nature de l'entité en charge de la délivrance des certifications. Le PE propose que seules les DPA soient en charge de cette responsabilité alors que le Conseil prévoit, outre la certification par les DPA, la possibilité que des organismes privés[29] puissent également s'en charger. La CPVP considère que la possibilité pour les DPA de certifier des activités, des responsables de traitement ou des sous-traitants pourrait porter atteinte à son indépendance. Par conséquent, la CPVP soutient l'idée que seuls des organismes privés, accrédités par le secteur public, devraient pouvoir procéder à de la certification mais uniquement sur la base de critère de certification élaborés par les DPA.

100. Les propositions du Conseil et du PE prévoient également que la certification emporterait certaines conséquences juridiques concrètes. Ainsi, la certification serait considérée comme étant une garantie appropriée pour le transfert de données hors de l'Union européenne. En premier lieu, la CPVP s'interroge sur la manière dont la certification d'une entreprise établie en dehors de l'Union européenne pourrait concrètement être réalisée compte tenu de la distance géographique. Néanmoins, si le Règlement devait reconnaître la possibilité de reconnaître la certification comme outil de transfert international de données, la CPVP soutiendrait la position du Conseil qui vise à la conditionner au fait que ces outils soient combinés à des engagements juridiquement contraignants et exécutables par les personnes concernées[30]. Ces conditions sont systématiquement prévues actuellement dans les contrats de transfert de données ainsi que dans les règles d'entreprise contraignantes (Binding Corporate Rules - BCR). Il est essentiel qu'elles soient également présentes dans tout nouvel outil de transfert de données afin de ne pas affaiblir le niveau de protection actuellement offert par les garanties appropriées existantes.

101. La seconde conséquence juridique serait un impact quant au nombre d'hypothèses dans lesquelles le traitement serait administrativement sanctionné (79.2b du PE) ou sur le montant des sanctions (79.2a.j du Conseil). La CPVP renvoie ici à la position qu'elle adopte au point 94. .

---

[29] Ces organismes seraient accrédités, soit par les DPA, soit par les organismes nationaux d'accréditation visé par le Règlement 765/2008/EC.

[30] Voir également le point 116 de l'avis.

102. Une différence essentielle entre la proposition du PE et celle du Conseil sur la certification tient au fait que si le PE prévoit que seules les DPA sont habilitées à certifier, le Conseil souhaite permettre à des organismes de certification de proposer également leur service. En tout état de cause, il est essentiel que les *critères de certification* soient approuvés par les DPA (article 39.2a du Conseil) et rendus publics (39a.6 du Conseil). Comme élaboré au point 116 (infra) de cet avis, la CPVP estime qu'en matière de flux internationaux, les outils proposés doivent nécessairement être des outils de co-régulation et non de simple autorégulation.

103. Par ailleurs, la CPVP souscrit à l'idée d'un registre public des certificats délivrés et retirés (article 39.1h du PE et 39.5 du Conseil).

104. En outre, il est essentiel que la certification ne réduise aucunement les obligations des responsables de traitement et des sous-traitants (voir l'article 39.2 et 39a.4 du Conseil). Elle ne peut, à elle seule démontrer le respect du règlement (voir l'article 22.2b du Conseil) et les compétences de contrôle et d'investigation des DPA doivent demeurer intactes (voir l'article 39.2 et 39a.1 du Conseil).

105. Enfin, comme le PE a prévu que le respect de l'article 23 « data protection by design» peut être un critère de sélection des marchés publics (article 23.1a), la CPVP estimerait utile que la certification puisse également jouer ici un rôle important, dans la lignée des dispositions actuelles des directives 2004/17/CE et 2004/18/CE relatives aux procédures de passation de certains marchés publics.

Chapitre V : Flux transfrontières

Article 40 - Principes généraux pour les transferts

106. La CPVP soutient le maintien de l'article 40 (proposé par la COM et soutenu par le PE) car il permet de préciser qu'en matière de flux transfrontières, le nécessaire respect du chapitre V, n'exempte pas du respect des autres chapitres du règlement, notamment les principes de légitimité et de finalité.

107. Avant de pouvoir transférer les données à l'étranger, l'exportateur doit s'assurer que l'ensemble des dispositions légales sont respectées et notamment que la collecte initiale des données et sa communication à un tiers sont légitimes (respect de l'article 6 du règlement), que les données transférées sont proportionnelles et que le transfert est sécurisé.

108. Cet article 40 rappelle utilement ce principe et permet d'éviter la confusion fréquente que font les responsables de traitement et qui consiste à penser que l'existence d'une décision d'adéquation ou la mise en place de garanties appropriées suffisent pour envoyer des données librement à l'étranger sans avoir égard aux autres dispositions légales.

Article 41 – Adéquation

109. La CPVP soutient la position des 3 institutions qui consiste à clarifier les critères d'évaluation de l'adéquation des pays tiers mais également, et plus particulièrement, la position du Conseil qui tend à souligner le fait que la liste de critères proposée n'est pas exhaustive. En effet, si la clarification des critères peut augmenter la sécurité juridique, il ne faudrait pas limiter le champ de l'analyse dès lors que la directive 95/46/CE permet actuellement la prise en considération de l'ensemble des circonstances relatives au transfert.

Article 42 - Transferts de données au moyen de garanties appropriées

Suppression des autorisations pour BCR/clauses types

110. La CPVP soutient la volonté des 3 institutions de simplifier les obligations des entreprises en supprimant les exigences d'autorisations nationales lorsque des clauses types ou des règles d'entreprises contraignantes (BCR) sont utilisées.

Sort des autorisations délivrées pour les clauses contractuelles ad hoc et des décisions de la Commission européenne en matière de clauses contractuelles types

111. Quant au sort des autorisations nationales existantes et des décisions en matière de clauses contractuelles type, la CPVP soutient la proposition du Conseil qui vise à maintenir leurs effets tant qu'ils n'ont pas été modifiés, supprimés ou retirés. La CPVP tient à souligner les risques en termes d'insécurité juridique et de surcharge administrative de la position du PE sur ces points. En effet, le PE prévoit d'une part, que les décisions de la COM en matière de clauses contractuelles type ne demeurent valides que cinq années après l'entrée en vigueur du projet de Règlement et que, d'autre part, les autorisations prises en vertu de l'article 26.2 de la directive 95/46/CE (autorisations nationales de transferts de données sur la base de contrats ad hoc[31]) ne demeureront valides que deux années après l'entrée en vigueur du projet de Règlement.

112. La suppression automatique des décisions existantes de la COM en matière de clauses contractuelles types crée le risque que celles-ci ne soient pas remplacées à temps.

[31] L'invalidité des autorisations en matière de clauses types et de BCR n'aurait quant à elle que peu d'impact du fait que ces outils ne seraient de toute façon plus soumis à un quelconque régime d'autorisation.

Sans possibilité de conclure les contrats dans les temps, les entreprises pourraient être tentées de se référer aux exceptions (comme le consentement des individus), moins protectrices dès lors qu'elles n'apportent aucune garantie juridique une fois les données transférées.

113. On ne peut également envisager que l'ensemble des autorisations nationales délivrées depuis 1995 et qui concerneraient des contrats ad hoc toujours en vigueur aujourd'hui soient automatiquement invalidées 2 ans après l'entrée en vigueur du Règlement. Comme déjà indiqué dans son avis 10/2014 relatif à la position du Comité LIBE et du PE, la CPVP estime que cette position impliquera une surcharge administrative importante et non nécessaire tant pour les DPA européennes qui devront réévaluer l'ensemble des décisions déjà accordées, que pour les responsables de traitement[32].

Les BCR responsables de traitement

114. La CPVP soutient la reconnaissance explicite des BCR, et en particulier la précision par le Conseil des conditions auxquelles ils doivent satisfaire. Plus concrètement, le Conseil pallie les critiques précédemment formulées par la CPVP[33] en exigeant explicitement un système interne de traitement des plaintes des personnes concernées[34], la mise en place d'un programme de formation adéquat[35] ainsi que la transparence imposée à l'égard des DPA dans l'hypothèse d'un conflit entre une législation étrangère et les BCR[36]. La CPVP soutient également la référence plus explicite aux exigences en matière d'audits[37].

Référence aux BCR sous-traitants

115. La CPVP soutient les positions de la COM et du Conseil qui prévoient la possibilité pour les sociétés multinationales de mettre en place des BCR sous-traitants. Le PE choisit de supprimer cette possibilité et la CPVP s'y oppose. Sur ce point, la CPVP se réfère aux arguments qu'elle a développés dans son précédent avis 10/2014[38].

La Certification et les Codes de conduite

116. Si l'on devait ajouter la certification et les codes de conduite comme nouvelles formes de garanties appropriées autorisant les transferts à l'étranger en l'absence d'adéquation, la CPVP estime qu'il faudrait nécessairement opter pour un système de co-régulation (impliquant l'intervention des DPA) et non d'autorégulation pure. Par ailleurs, la

---

[32] Points 82 à 84 de l'avis 10/2014.

[33] Point 139 de l'avis 32/2012.

[34] Article 43. hh de la position du Conseil.

[35] Article 43.m de la position du Conseil.

[36] Article 43.l de la position du Conseil.

[37] Article 43.i de la position du Conseil.

[38] L'ensemble des arguments sont détaillés aux points 86 à 94 de l'avis 10/2014.

CPVP soutient également la position du Conseil qui vise à promouvoir des outils impliquant des engagements juridiquement contraignants et exécutables par les personnes concernées. Il serait en effet inconsidéré de reconnaître comme garantie appropriée des outils d'autorégulation n'impliquant aucune forme d'engagement juridique et aucun droit de recours pour les individus. Ceci entrainerait une protection insuffisante et un risque de désintérêt évident pour les BCR ou les clauses contractuelles dès lors que ces instruments sont plus contraignants et donc plus protecteurs.

Des outils pour le secteur public

117. La CPVP soutient les propositions du PE et du Conseil qui visent à supprimer la proposition de l'article 42.5 proposé par la COM, et cela, principalement du fait de son manque de clarté[39]. La CPVP soutient également la position du Conseil qui vise à reconnaître explicitement des outils encadrant les transferts internationaux de données réalisés par le secteur public[40]. Elle soutient également la position du Conseil qui vise à soumettre à autorisation nationale tout outil non contraignant utilisé par le secteur public[41].

Article 43.a du PE - Transferts et divulgations non autorisées par le droit de l'Union

118. La CPVP renvoie à ses positions développées aux points 95 à 102 de son avis 10/2014.

Article 44 - Les dérogations

119. La CPVP soutient la position du PE qui vise à supprimer la dérogation prévue à l'article 44.1.h. relative à la possibilité pour le responsable de traitement d'évaluer lui-même les circonstances relatives à un transfert et d'offrir les garanties appropriées nécessaires. La CPVP avait jugé que ce texte est en contradiction avec (et met en péril) le régime des clauses contractuelles "ad hoc" et des BCR qui impliquent nécessairement l'intervention de la DPA[42]. Par ailleurs, la CPVP réitère son avis selon lequel les dérogations prévues à l'article 44 doivent être interprétées de manière restrictive et ne peuvent porter sur des transferts massifs ou répétitifs de données, ni servir de base à des transferts de données qui ont lieu d'une manière telle qu'elle ne peut être considérée comme étant nécessaire et proportionnée dans une société démocratique[43].

---

[39] Pour plus de détail, voir le point 138 de l'avis 35/2012.

[40] Art. 42.2.oa de la position du Conseil.

[41] Article 42.2a.d de la position du Conseil.

[42] Point 140 de l'avis 35/2012.

[43] Point 103 de l'avis 10/2014.

Chapitre VI: les autorités de contrôle

120. Le Chapitre VI est entièrement consacré aux DPA. Leur statut, les règles relatives à leur établissement, leurs compétences, fonctions et pouvoirs sont, quel que soit le texte auquel on se réfère COM, PE ou Conseil, plus nombreux et bien davantage précisés que dans la directive 95/46/CE.

Article 47 - Indépendance des DPA

121. La CPVP soutient le renforcement de l'exigence d'indépendance des DPA voulu tant par la COM, le PE que le Conseil dans le prolongement des arrêts de la Cour de Justice de Luxembourg des dernières années (article 47).

122. La CPVP est d'avis que cette indépendance ne pourra être effective que si, comme mentionné à l'article 47.5, *"Each Member State (…) [ensures] that the supervisory authority is provided with the adequate human, technical and financial resources"*. La CPVP renvoie à cet égard à la résolution adoptée le 20 mai dernier par la Conférence européenne des autorités de protection des données réunies à Manchester.

Article 51 - Mécanisme du guichet unique ou principe "one-stop-shop"

123. Le Conseil a consacré de nombreuses réunions au principe de guichet unique, en particulier pour tenter de répondre à la demande des ministres d'y associer *la proximité*. La solution élaborée par le Conseil s'écarte très clairement des textes de la COM et du PE. De manière générale et même s'il ne répond pas à toutes ses attentes, en particulier à celle première, d'une véritable autorité européenne de protection des données, la CPVP peut, dans ses grandes lignes, adhérer au compromis obtenu par le Conseil.

124. Un constat important : le Conseil, tout comme la COM et le PE, reste d'avis que les traitements effectués par des autorités publiques relèvent exclusivement de la compétence de la DPA de l'État membre concerné. La CPVP soutient cette approche.

Traitement transnational (transnational processing) et DPA concernées

125. Le Conseil introduit la notion de "traitement transnational", tout en prévoyant plusieurs exceptions ou corrections importantes.

126. Un traitement peut être « transnational » pour plusieurs raisons. Tout d'abord, il peut s'agir d'un traitement opéré dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable de traitement ou sous-traitant dans l'Union[44].

[44] La CPVP ne comprend pas bien la définition. Il est question d'un "traitement dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant dans l'Union et où le responsable du traitement ou le sous-traitant a des établissements dans plusieurs États membres". Il lui semble que la deuxième partie de

Ensuite, ce peut être un traitement dans le cadre des activités d'un seul établissement d'un responsable de traitement ou d'un sous-traitant dans l'Union, qui affecte (ou affectera) probablement sensiblement des personnes concernées dans plusieurs États membres.

127. Lorsqu'il y a *traitement transnational*, plusieurs autorités de contrôle sont toujours impliquées. La procédure élaborée par le Conseil ajoute la notion d' "autorités de contrôle concernées". Une DPA peut être concernée pour plusieurs raisons : le responsable de traitement ou le sous-traitant est établi sur le territoire de son État membre, les personnes concernées qui sont (probablement) sensiblement affectées par le traitement résident dans son État membre ou la réclamation sous-jacente a été introduite auprès de cette DPA. Concrètement, cela signifie par exemple que l'autorité de contrôle chef de file est toujours une autorité de contrôle concernée.

Compétence de l'autorité de contrôle chef de file – l'établissement principal

128. Le Conseil prévoit que dans les cas transnationaux, est compétente l'autorité de contrôle chef de file (la "lead authority"), soit la DPA de l'établissement principal du responsable de traitement ou du sous-traitant. Celui-ci agit ainsi comme seul interlocuteur à l'égard du responsable de traitement ou du sous-traitant, ce qui ne veut pas dire qu'elle est compétente pour se prononcer systématiquement *seule* (sans droit de parole d'autres DPA) quant au fond de l'affaire (voir ci-après).

129. Dans la version du Conseil, la définition de l'établissement principal a été adaptée et est davantage détaillée que dans le texte du PE : la relation entre le responsable de traitement et le sous-traitant y a été réglée de manière moins stricte. La CPVP estime néanmoins que les adaptations apportées par le Conseil clarifient la situation.

130. En résumé, le texte du Conseil présume que le lieu de l'administration centrale est l'établissement principal tout en autorisant une preuve contraire à cet égard. L'"établissement du responsable du traitement dans l'Union qui prend les décisions quant à la finalité et aux moyens du traitement de données à caractère personnel et qui est également autorisé à exécuter ces décisions est ainsi qualifié *d'établissement principal*.

131. En ce qui concerne le sous-traitant, le Conseil a opté pour le critère du lieu de l'administration centrale. Lorsque ce dernier ne se trouve pas dans l'Union, il s'agit de l'établissement où les principales activités de traitement ont lieu.

---

cette phrase constitue une répétition inutile de la première partie. Ce qui est essentiel, c'est que le traitement ait lieu dans le cadre des activités d'établissements dans plusieurs États membres de l'Union.

132. La procédure à suivre à cet égard est celle de l'article 54*bis* (voir ci-après).

133. La CPVP soutient la démarche du Conseil consistant à prévoir une procédure destinée à trancher la question de savoir qui est l'autorité de contrôle chef de file. À cet effet, l'article 57, 3e alinéa proposé par le Conseil prévoit que le Comité européen de la protection des données (EDPB) adopte une décision contraignante "*lorsqu'il existe des points de vue divergents quant à l'autorité de contrôle concernée compétente pour l'établissement principal*". L'imprécision présente dans le texte du PE à ce niveau est ainsi levée. La manière dont la problématique peut ou doit être soumise à l'EDPB n'est toutefois plus réglée. La CPVP estime à cet égard qu'il faut éviter un formalisme excessif : une demande émanant d'une autorité de contrôle concernée doit pouvoir suffire. Il convient également de clarifier le moment à partir duquel le délai dans lequel l'EDPB doit se prononcer court (en principe, un mois à compter de la transmission de la question).

Maintien de la compétence de la DPA (locale) dans des cas locaux

134. Ce qui précède n'empêche pas le Conseil de procéder à une correction importante quant à la compétence de l'autorité de contrôle chef de file. En présence d'un traitement transnational (voy. ci-dessus) dont les conséquences se limitent toutefois à un seul État membre, soit parce que la question (« subject matter ») est exclusivement liée à cet État membre, soit parce qu'elle n'a de conséquences importantes que pour des personnes concernées dans cet État membre, la compétence revient alors en principe à la DPA de cet État. Il s'agit là des "cas locaux" pour lesquels la DPA locale est en principe compétente.

135. Une procédure spécifique de coopération est prévue à cet effet. Elle consiste à ce que la DPA locale informe immédiatement l'autorité de contrôle chef de file du cas, après quoi cette dernière doit décider si elle traitera ou non ce cas via le mécanisme de guichet unique. Un des critères à cet égard est l'existence ou non d'un établissement dans l'État membre de la DPA locale pour pouvoir garantir qu'une décision puisse réellement être exécutée.

136. La CPVP marque son accord à cet égard. Cette approche répond en effet aux cas qu'elle a précédemment évoqués pour illustrer sa préoccupation quant aux conséquences juridiques et pratiques d'une autorité compétente unique[45].

Procédure – codécision des DPA concernées avec un rôle renforcé de l'EDPB

[45] Au point 148 de l'avis n° 35/2012. Dans chacun des exemples cités, la solution proposée par le Conseil offre d'ailleurs une issue : sur la base du texte du Conseil, seul le contrôleur belge sera compétent aussi bien dans le cas d'écoute téléphonique par l'employeur belge que dans le cas de l'enregistrement de conversations entre les clients et les travailleurs d'un établissement belge ou dans le cas de faille de sécurité rendant publiques les données de citoyens belges.

137. La procédure pour les cas transnationaux a été adaptée par rapport au texte du PE. Principalement, un rôle plus important est attribué à l'EDPB.

138. Le texte du Conseil prévoit (à l'article 54*bis*) qu'il suffit qu'une DPA concernée formule une objection pertinente et motivée contre un projet de décision de l'autorité de contrôle chef de file pour que le cas soit soumis à la décision de l'EDPB[46] (et non plus uniquement à son *avis*, comme c'est le cas dans le texte du PE). Cela permet *de facto* à l'EDPB d'exercer un rôle de "chien de garde" européen.

139. La CPVP se réjouit du choix, par le Conseil, d'une procédure de *codécision* aux termes de laquelle l'autorité de contrôle chef de file ne peut pas, à elle seule, approuver et prendre des mesures pour lesquelles d'autres autorités de contrôle sont également compétentes[47].

140. Le Conseil ne charge pas à proprement parler l'EDPB de la surveillance des traitements transnationaux. Sa solution s'en approche toutefois, en renforçant son rôle en cas d'objection d'une DPA concernée. Pour pouvoir assumer ce rôle, le Conseil a donné à l'EDPB la forme d'une agence dotée de la personnalité juridique. Cela répond aux remarques précédemment formulées par la CPVP[48].

Chapitre VII. Coopération et cohérence

141. Comme indiqué ci-avant et au vu de la mondialisation croissante des traitements de données, la CPVP estime nécessaire de renforcer la coopération entre les DPA européennes[49].

Articles 55 et 56 – Assistance mutuelle et opérations conjointes des DPA

142. La préférence de la CPVP va au texte rédigé par le Conseil, du moins en ce qui concerne l'assistance mutuelle. Pour ce qui est des opérations communes (« joint operations of DPA's »), les 3 textes sont assez similaires. A noter que le Conseil a réglé la responsabilité d'éventuels dommages dans ces cas.

---

[46] Il est notamment prévu qu'une décision de l'autorité de contrôle chef de file (après concertation) et une décision du Comité européen de la protection des données (EDPB) soient contraignantes. En particulier, il est prévu que l'autorité de contrôle chef de file et les autorités de contrôle concernées soient sensées marquer leur accord sur la décision (le projet de décision) (voir l'article 54*bis*, alinéa 4 tel que proposé par le Conseil).

[47] Comme indiqué au point 111 de l'avis n° 10/2014.

[48] Voir notamment les remarques du point 113 de l'avis n°10/2014. En outre, la CPVP souligne qu'il faut également pouvoir interjeter appel contre les décisions du Comité européen de la protection des données.

[49] Voir le point 151 de l'avis n°35/2012.

Article 57 et s. – Mécanisme de cohérence (Consistency mechanism) et EDPB

143. Le contrôle de la cohérence[50] constitue un aspect spécifique. Celui-ci est repris pour veiller à une application uniforme (ou cohérente) du Règlement dans l'Union. Alors que le PE fait une distinction entre les questions d'application générale et d'application individuelle, cette distinction est remplacée dans le texte du Conseil par les questions sur lesquelles l'EDPB émet un avis et celles sur lesquelles il prend une décision. La CPVP marque clairement sa préférence pour le système élaboré par le Conseil.

144. En ce qui concerne l'EDPB lui-même, la CPVP constate qu'il a été fait droit à sa demande de lui attribuer la personnalité juridique ainsi que la compétence d'adopter des décisions contraignantes. Cette prise de décision au sein de l'EDPB dépend de sa compétence (distinction entre décisions contraignantes et avis).

145. Néanmoins, la CPVP remarque qu'il n'est pas clairement prévu *comment* l'EDPB accomplira toutes les tâches qui lui sont confiées par l'article 66. En outre, dans plusieurs cas, on attendra de l'EDPB qu'il rédige des directives aidant les DPA à appliquer le règlement. Le travail le plus important s'effectuera à cet effet au niveau du secrétariat de l'EDPB. La CPVP approuve la distinction claire prévue par le Conseil entre d'une part, les collaborateurs qui accomplissent les tâches qui sont attribuées à l'EDPB par le projet de Règlement et d'autre part, ceux qui accomplissent les tâches du Contrôleur européen de la protection des données (EDPS). D'un point de vue pratique, la CPVP s'inquiète du régime linguistique qui sera mis en place au sein de l'EDPB. Il est certes prévu que le secrétariat de l'EDPB sera responsable de la traduction des informations pertinentes, mais sans plus amples détails, notamment quant à la manière dont il sera tenu compte des délais dans lesquels l'EDPB est tenu d' intervenir.

Chapitre VIII – Recours, responsabilité et sanctions

146. Le Chapitre VIII a déjà été abordé précédemment par la CPVP, notamment en ce qui concerne les sanctions et la complexité des recours juridictionnels. Trois aspects majeurs sont examinés ci-après.

Recours - Recours effectif

147. Le Conseil a beaucoup travaillé pour assurer une bonne application du principe de proximité. Le texte élaboré implique que si la personne concernée introduit une réclamation et que celle-ci est rejetée ou révoquée, c'est la DPA auprès de laquelle la

[50] La CPVP fait remarquer que l'expression en néerlandais ("conformiteitstoetsing") ne couvre pas bien le sens visé. Par analogie avec le texte en français, il est préférable de parler d'un mécanisme de contrôle de la cohérence.

réclamation est introduite qui statue et qui notifie la personne concernée ou du moins la tient informée à ce sujet. Cela implique que la personne concernée qui n'est pas d'accord avec la décision peut intenter un recours contre (la décision de) cette DPA ("propre").

148. Cette solution s'applique également aux décisions prises par l'autorité de contrôle chef de file. La personne concernée qui souhaite intenter un recours contre la décision de l'autorité de contrôle chef de file ne doit ainsi pas s'adresser au tribunal de l'État membre où l'autorité de contrôle chef de file est établie. De cette manière, un droit à un recours effectif est garanti à la personne concernée[51].

149. Il en résulte que la personne concernée qui introduit une réclamation n'est plus (nécessairement) confrontée à une autorité de contrôle étrangère[52]. Si une personne concernée belge introduit une réclamation auprès de la CPVP, elle aura toujours affaire, en cas de rejet ou de révocation, à la CPVP et pourra intenter un recours contre la décision (de rejet ou de révocation) auprès d'un tribunal belge.

Tribunal compétent

150. Contrairement au PE, le Conseil a opté pour un régime alternatif. Il part du principe que le Règlement n° 1215/2012 est d'application dès lors que le traitement de données est généralement accessoire à d'autres relations. Si ce Règlement n'est pas valable/pas d'application, l'action peut, au choix, être intentée devant le tribunal de l'État membre où le responsable ou le sous-traitant a un établissement ou devant les tribunaux de l'État membre où la personne concernée a sa résidence ordinaire. La seule exception est la situation dans laquelle le responsable de traitement ou le sous-traitant est une autorité publique qui agit dans le cadre de ses compétences publiques.

Article 76 et s. – Représentation des personnes concernées (collective action)

151. La CPVP approuve la possibilité offerte d'intenter une certaine forme de *class action.* Cette possibilité est prévue aussi bien pour introduire une réclamation que pour intenter une action, tant à l'encontre d'une DPA que d'un responsable de traitement ou d'un sous-traitant.

Suspension des procédures

152. Bien que le projet de Règlement élaboré doive en principe donner lieu à une limitation du nombre de conflits de juridiction, ils ne peuvent probablement pas être

[51] Ce qui n'était pas aussi clair dans le texte du PE (voir le point 119 de l'avis n°10/2014).

[52] Comme remarqué précédemment par la CPVP au point 17 de l'avis n° 10/2014.

totalement évités. À cet égard, la CPVP marque son accord sur le règlement tel que repris à l'article 76*bis* du Conseil

Article 77 – Responsabilité

153. La question de la responsabilité a donné lieu à de très nombreuses discussions. Celles-ci ne concernent pas uniquement la question de savoir si la responsabilité est ou doit être objective, mais surtout si elle doit être ou non *solidaire*[53].

154. La CPVP estime que les principes de responsabilité quasi-objective et solidaire, tels que repris dans la proposition initiale de la COM, doivent être maintenus. Cela implique avant tout que le responsable de traitement et le sous-traitant ne peuvent se dégager de leur responsabilité que s'ils démontrent que le dommage ne peut leur être imputé. Dès que la responsabilité est établie, elle doit de préférence aussi être solidaire. Cela implique que la personne concernée peut s'adresser à chacune des parties responsables pour obtenir une indemnisation intégrale. Même si ce n'est pas toujours la meilleure solution, notamment lorsque le sous-traitant est économiquement beaucoup plus « fort » que le responsable de traitement, la CPVP estime qu'elle est celle qui sert le mieux les intérêts de la personne concernée[54].

155. La CPVP est d'avis qu'il convient procéder à une harmonisation européenne à ce niveau et ce afin, notamment, d'éviter que des responsables et/ou sous-traitants se délocalisent le cas échéant, par exemple pour avoir la possibilité d'échapper (encore) à leur responsabilité (forum shopping"). Dans cette optique, la CPVP soutient la proposition du Conseil.

Article 79 - Sanctions

156. La CPVP renvoie à ses remarques précédentes quant à l'opportunité d'attribuer aux DPA la compétence d'infliger des sanctions administratives[55]. À ce niveau, le texte tel que proposé par le Conseil semble offrir davantage de possibilités.

---

[53] La CPVP souligne qu'il faut d'abord poser la question de savoir dans quelle mesure on est (ou peut être) responsable. Cela implique également que l'on sache clairement ce que la personne concernée doit prouver et quelle preuve contraire la partie prétendue responsable peut fournir. Cela fait partie de la question de savoir si la responsabilité est objective ou quasi-objective. En deuxième instance, il y a la question de savoir qui, dans la mesure où il y a des parties responsables, paiera l'indemnisation. Cet aspect est envisagé avec le caractère solidaire ou *in solidum* de la responsabilité.

[54] La CPVP fait d'ailleurs remarquer que dans la plupart des cas en Belgique en ce moment, suite à l'incrimination de la plupart des infractions, il est question d'une responsabilité *in solidum* dans le chef du responsable et du sous-traitant. Cela donne en pratique le même résultat qu'avec la responsabilité solidaire.

[55] Voir les remarques des points 124 et 125 de l'avis n° 10/2014 qui renvoient aussi expressément aux remarques sur la proposition initiale de la COM aux points 154 à 163 de l'avis n° 35/2012.

157. Avant tout, le texte du Conseil prévoit la *possibilité* pour les DPA d'infliger une amende administrative (l'article 79a dispose en particulier ce qui suit : *"The supervisory authority may impose a fine …"*), de sorte qu'il n'y a pas d'obligation d'infliger des amendes administratives[56].

158. Il est également prévu que les États membres peuvent renoncer à déterminer des règles relatives aux amendes administratives si les infractions prévues (à l'article 79a, alinéas 1, 2 et 3) sont déjà soumises à des sanctions pénales à la date d'application du règlement (c'est-à-dire l'entrée en vigueur + 2 ans)[57].

159. Ces dispositions contribuent bien entendu au respect du principe "non bis in idem"[58].

La préférence pour des mesures administratives autres que des amendes

160. La CPVP estime qu'il doit être possible de lui attribuer la compétence d'imposer des mesures administratives (autres que des amendes) afin de garantir (la mise en) conformité avec les dispositions légales. Ou encore, la CPVP est plutôt favorable à des mesures alternatives (autres que des amendes) à la répression qui visent plutôt la mise en conformité. À ce niveau, le texte du Conseil répond le plus aux préoccupations de la CPVP. Le Conseil prévoit en effet que des amendes administratives soient le cas échéant infligées, en fonction des circonstances de chaque cas individuel, en plus ou au lieu des mesures visées à l'article 53, alinéa 1b, points a) à f). Elle confirme ainsi la priorité des compétences et/ou mesures de correction telles que les avertissements (que les traitements envisagés sont peut-être de nature à constituer une infraction au Règlement), les réprimandes, l'injonction au responsable de traitement ou au sous-traitant de respecter les requêtes de la personne concernée et l'injonction de suspendre le transfert vers un destinataire dans un pays tiers ou vers une organisation internationale. La CPVP renvoie à cet égard aux compétences et pouvoirs d'intervention tels qu'attribués en Belgique à la Commission de contrôle flamande (Vlaamse Toezichtcommissie – VTC) et à l'IBPT[59]. À cet égard, ce qui est toutefois important, c'est le fait que l'on prévoie une épée

---

[56] Auparavant déjà, la CPVP avait clairement marqué sa préférence pour la voie qu'avait empruntée le Conseil "*d'accorder aux autorités de protection des données la faculté (et non l'obligation) d'imposer des amendes administratives*" (point 125 de l'avis n° 10/2014).

[57] Cela devrait permettre au législateur belge de renoncer à infliger des amendes administratives dans les cas où une sanction pénale est déjà prévue.

[58] Voir à cet égard les remarques aux points 160 et 161 de l'avis n° 35/2012.

[59] Il s'agit de *l'arrêt ou de l'exécution de travaux, d'actes ou d'activités, immédiatement ou dans un délai fixé et/ou de l'interdiction de l'utilisation de bâtiments, d'installations, de machines, d'appareils et de tout ce qui se trouve dedans ou dessus* (article 12/1 du décret du 18 juillet 2008 *relatif à l'échange électronique de données administratives*, tel qu'inséré par l'article 3 du décret du 6 décembre 2013 *portant modification du décret du 18 juillet 2008 relatif à l'échange électronique de données administratives, en ce qui concerne l'établissement des compétences de contrôle et de maintien de la commission flamande de contrôle relatives à l'échange électronique de données administratives*).

de Damoclès qui veille à ce que les mesures infligées puissent être imposées. Cela peut se faire le cas échéant en prévoyant la possibilité d'imposer des amendes.

En cas d'amendes, l'exigence de marge d'appréciation pour les DPA

161. L'article 79, alinéa 2bis répond à la remarque antérieure de la CPVP selon laquelle, si des amendes administratives sont (doivent être) infligées, les DPA doivent disposer de la marge d'appréciation nécessaire. Cet article énumère les éléments dont il faut tenir compte dans les décisions relatives à l'imposition d'amendes administratives et sur leur portée.

Prise en compte de la situation spécifique du secteur public

162. Le texte du Conseil prévoit la possibilité de tenir compte des spécificités du secteur public lors de la mise ne œuvre du régime de sanctions (voir l'article 79, alinéa 3*ter*).

163. À noter toutefois que pour les infractions au projet de Règlement qui ne sont pas soumises aux amendes administratives, les États membres doivent fixer des règles relatives aux sanctions qui s'y rapportent (article 79*ter* du texte du Conseil).

Chapitre IX : Dispositions relatives à des situations particulières de traitement de données

164. Comme déjà indiqué, le chapitre IX concerne les différents secteurs qui font l'objet de divergences nationales et dont on admet que ces divergences sont justifiées par les différentes cultures et traditions juridiques, tels qu'en matière de liberté d'expression, de traitement de données de santé, de sécurité sociale et d'emploi. Pour cette raison, les États sont invités pour ces aspects à élaborer leurs propres législations nationales[60].

Article 80 - Transparence administrative et réutilisation des données du secteur public

165. Le Conseil insère une référence aux législations nationales en matière de transparence administrative et de réutilisation des données du secteur public (article 80a et 80 aa). Le PE prévoit également une référence à la transparence administrative

[60]Points 164 et s. de l'avis 35/2012.

(article 80a). Dans ces articles, il est fait référence au besoin de réconcilier le droit à la protection des données et la transparence administrative d'une part mais également de concilier le premier et le droit à la réutilisation des données du secteur public, d'autre part.

166. La CPVP souhaite préciser que l'on ne peut parler de *réconciliation* que lorsqu'il s'agit d'une relation entre deux droits fondamentaux (par ex. le droit à la transparence administrative et le droit à la protection des données), ce qui n'est pas le cas de la relation entre le droit à la protection des données et la réutilisation des données du secteur public. Le droit à la réutilisation des données du secteur public est de nature inférieure au droit à la protection des données. Ceci est confirmé par les articles 1.4 de la Directive 2003/98/CE[61] et 1 §2 c) quater inséré par la Directive 2013/37/UE[62] la modifiant. Par conséquent, la mise en œuvre du droit à la réutilisation des données du secteur public doit se faire dans le respect du droit à la protection des données.

167. De plus, la mise en forme de ces articles, telle qu'élaborée par le Conseil devrait être revue car elle donne à penser que la divulgation des données et la législation visée (transparence et réutilisation) ont pour objectif de réconcilier les droits en présence (« in order to reconcile ») alors que ce n'est pas le cas. Ces législations ont leur finalité propre. Dans ce sens, la formulation du PE à l'article 80a (« legislations …, which reconciles ») semble plus correcte juridiquement.

Article 80 b (Conseil) - Numéro de Registre national

168. La CPVP soutient la position du Conseil à l'article 80b qui vise à réintroduire l'article 8.7 de la directive 95/46/CE qui permet aux États membres de définir les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement. La CPVP avait déjà, dans ses avis antérieurs, souhaité cette réintroduction[63].

---

[61] La présente directive laisse intact et n'affecte en rien le niveau de protection des personnes à l'égard du traitement des données à caractère personnel garanti par les dispositions du droit communautaire et du droit national et, en particulier, ne modifie en rien les droits et obligations prévus dans la directive 95/46/CE.

[62] La directive « reuse » ne s'applique pas aux documents dont l'accès est exclu ou limité en application de règles d'accès pour des motifs de protection des données à caractère personnel, et aux parties de documents accessibles en vertu desdites règles qui contiennent des données à caractère personnel dont la réutilisation a été définie par la loi comme étant incompatible avec la législation concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel ».

[63] Points 169 à 171 de l'avis 35/2012 ainsi que les points 127 et 128 de l'avis 10/2014.

Article 83 - Les traitements de données à des fins de recherche historique, statistique et scientifique

Base de légitimité

169. Si la CPVP soutient l'article 9.2.i, elle a beaucoup plus de réserves à propos de l'article 6.2 qui semble permettre que des traitements de données "non-sensibles" puissent avoir lieu à des fins de recherche scientifique sans que le premier paragraphe de l'article 6 soit respecté. Il est pourtant essentiel, aux yeux de la CPVP, que tout projet de recherche passe par l'obligation de ce test de légitimité et cela afin d'éviter, par exemple, le développement de projets de recherche qui ne seraient pas éthiques[64].

Conditions de traitement

170. La CPVP soutient le texte de la COM qui vise à promouvoir l'usage de données anonymes ou codées en matière de recherche scientifique. Cette suggestion est parfaitement en ligne avec d'autres standards internationaux[65].

171. Le texte du PE reprend cette suggestion mais supprime la possibilité de faire usage de données directement identifiantes lorsqu'il est impossible de faire usage de données anonymes ou pseudonymisées (suppression de *« as long as these purpose can be fulfilled in this manner »*). Comme précédemment déjà souligné[66], cette suppression va trop loin car pour certaines recherches, l'utilisation de données directement identifiantes est nécessaire. On ne peut imaginer obliger tous les historiens à supprimer l'identité des personnes publiques ou à remplacer leur nom par des alias.

172. La CPVP préfèrerait que les conditions de traitement en matière de recherche scientifique, historique et statistique soient davantage harmonisées afin de faciliter le travail des scientifiques dont les projets dépassent de plus en plus souvent le cadre purement national. Il est important pour eux que l'on évite des divergences dues aux législations nationales. Cependant, aucune version proposée ne rencontre pour le moment pleinement les attentes de la CPVP (promotion de l'usage des données anonymes ou codées, évitement du consentement systématique pour les données sensibles,

---

[64] Voir également le point 178 de l'avis 35/2012.

[65] Par ailleurs, elle est également en ligne avec notre législation nationale, voir le Chapitre II de l'arrêté royal du 13/02/2001. Pour les références nationales étrangères et internationale, voir l'Art.40 de la loi fédérale allemande, l'article 46 de la loi fédérale autrichienne (DSG 2000), l'article 16 de la loi estonienne et l'article 3 de la Recommandation Rec (2006)4 du Conseil de l'Europe sur la recherche utilisant du matériel biologique d'origine humaine.

[66] Point 138 de l'avis 10/2014.

suppression de l'article 6.2 et pour ce qui concerne les exceptions, la CPVP renvoie à ses propositions émises dans l'avis 35/2012 (point 180). Tant que les conditions de traitement ne sont pas réglées de manière satisfaisantes, la CPVP aura une préférence pour une solution qui vise à laisser aux États membres le soin d'élaborer ces conditions de traitement.

Les exceptions aux droits des personnes concernées

173. La CPVP soutient l'intention du PE de prévoir les exceptions, ainsi que les garanties requises pour leur application, directement dans le projet de Règlement. Comme déjà expliqué[67], les conditions de traitement en matière de recherche historique, statistique et scientifique devraient être davantage harmonisées.

174. La CPVP ne soutient dès lors ni la position du Conseil qui laisse aux États membres le soin de prévoir les exceptions dans leur législation nationale, ni la position de la COM qui prévoit de régler cette question par la voie d'actes délégués[68].

175. Pour les détails techniques visant à l'amélioration de la proposition du PE, la CPVP se réfère à son précédent avis[69].

Délais de conservation

176. Tout comme le projet initial de la COM, le projet voté par le PE et celui du Conseil prévoient la possibilité de conserver les données plus longtemps à des fins de recherche historique, statistique et scientifique en ajoutant comme garantie additionnelle le fait que des mesures de sécurité et d'organisation soient prises. La CPVP accueille favorablement ces ajouts (la référence aux mesures de sécurité avait spécifiquement été suggérée par la CPVP dans son avis 35/2012[70]).

Chapitre X – Actes délégués et actes d'exécution

[67] Voir le point 172 du présent avis.
[68] Voir le point 180 de l'avis 35/2012.
[69] Points 139 et 140 de l'avis 10/2014.
[70] Point 179.

177. La CPVP a précédemment critiqué le nombre important d'actes délégués et d'actes d'exécution prévus dans la proposition de la COM[71]. Sur ce point, elle adhère à la proposition du Conseil dans laquelle les cas initialement prévus sont considérablement réduits. Le Conseil ne retient en effet qu'un seul acte délégué (article 39a, alinéa 7) et conserve des actes d'exécution dans 11 cas.

Chapitre XI – Dispositions finales

178. En ce qui concerne la relation avec la Directive ePrivacy - vie privée et communications électroniques 2002/58, la CPVP peut marquer son accord sur le premier alinéa de l'article 89. Pour le reste, il doit être clair que l'on doit procéder, au plus vite après l'entrée en vigueur de ce Règlement, à une adaptation de cette directive pour la mettre en conformité avec le Règlement. Il en va de même pour le Règlement n° 45/2001.

Conclusion

179. Comme mentionné en introduction, la CPVP exprime, aux termes de cet avis, son point de vue sur les 3 textes sur la table des négociations en vue du trilogue. Partant, cet avis est directement adressé à la COM , au PE et au Conseil ainsi qu'à tout autre «stakeholder » intéressé.

180. Pour différentes raisons explicitées dans ses avis précédents, la CPVP a d'emblée émis des doutes sur la nécessité de l'exercice initié par la COM en janvier 2012. Elle n'en a pas moins souhaité s'inscrire de manière constructive dans le débat en commentant tant la proposition de la COM (avis 35/2012) que la position du PE (avis 10/2014). La CPVP a, en outre, assisté le gouvernement belge en qualité d'expert lors des négociations aux DAPIX et COREPER.

181. Avec ce 3eme avis, la CPVP entend plus que jamais insister sur la nécessité d'adopter un *cadre simple et clair* pour l'ensemble des acteurs concernés (responsables de traitement, sous-traitants, DPA et personnes concernées). Les avantages et « simplifications » mises en avant pour justifier le choix d'un règlement ne se

[71] Voir à cet égard les remarques aux points 182 à 185 de l'avis n° 35/2012.

concrétiseront que si celui-ci offre un cadre règlementaire compréhensible, prévisible et applicable en pratique.

182. Cette qualité, la CPVP exige également de la retrouver au regard du *niveau de protection effective* que garantira le règlement. La CPVP ne s'oppose pas à l'introduction de nouveaux concepts tels que, pour n'en citer que deux, celui de « l'accountability » ou celui du « guichet unique » pour autant que le niveau de protection actuellement offert par la directive 95/46/CE soit, au minimum, préservé. Tout affaiblissement du niveau de protection serait inacceptable et la CPVP plaide pour sa part pour un renforcement de ce niveau de protection.

183. A cet égard, la CPVP souligne que là où la directive 95/46/CE le permettait, le législateur belge a parfois adopté un niveau de protection supérieur à celui prévu par la directive elle-même. La CPVP demeure préoccupée par le fait que l'adoption du Règlement ne permettrait plus ce niveau de protection supérieur et ce, nonobstant l'article 53 de la Charte des droits fondamentaux de l'Union.

184. Enfin, la CPVP insiste sur le rôle des DPA et sur la nécessité, outre celle d'adopter un cadre règlementaire de qualité, de prévoir pour elles des ressources adéquates et suffisantes pour mettre en pratique le Règlement à venir.

Pour l'Administrateur f.f., abs. Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere

Chef de section OMR f.f.