



Avis n° 168/2018 du 19 décembre 2018

Objet: Avis sur le projet d'arrêté du Gouvernement wallon relatif au contrôle des législations et réglementations relatives à la reconversion et au recyclage professionnels ainsi qu'à l'instauration d'amendes administratives applicables en cas d'infraction à ces législations et réglementations et sur le projet d'arrêté du gouvernement wallon relatif au contrôle des législations et réglementations relatives à la politique économique, à la politique de l'emploi et à la recherche scientifique ainsi qu'à l'instauration d'amendes administratives applicables en cas d'infraction à ces législations et réglementations (CO-A-2018-146-147)

L'Autorité de protection des données (ci-après l'Autorité);

Vu la loi du 3 décembre 2017 *relative à la loi portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26;

Vu la demande d'avis de M. Pierre-Yves Jeholet, Vice-Président du Gouvernement wallon et Ministre wallon de l'Economie, de l'Industrie, de la Recherche, de l'Innovation et du Numérique, reçue le 26 octobre 2018;

Vu le rapport de M. Willem Debeuckelaere ;

Émet, le 19 décembre 2018, l'avis suivant :

1. OBJET DE LA DEMANDE D'AVIS

1. Le Ministre wallon de l'Economie, de l'Industrie, de la Recherche, de l'Innovation, du Numérique, de l'Emploi et de la Formation (ci-après le demandeur) sollicite l'avis de l'Autorité concernant deux textes :
 - un projet d'arrêté relatif au contrôle des législations et réglementations relatives à la reconversion et au recyclage professionnels ainsi qu'à l'instauration d'amendes administratives applicables en cas d'infraction à ces législations et réglementations (ci-après, « *projet d'arrêté reconversion et recyclage* »);
 - un projet d'arrêté relatif au contrôle des législations et réglementations relatives à la politique économique, à la politique de l'emploi et à la recherche scientifique ainsi qu'à l'instauration d'amendes administratives applicables en cas d'infraction à ces législations et réglementations (ci-après, « *projet d'arrêté politique économique, emploi et recherche scientifique* »).

2. Ces deux textes ont en commun de traiter des pouvoirs d'investigations et enquêtes exercés par des agents régionaux afin de contrôler le respect des législations susmentionnées et infliger, le cas échéant, des amendes administratives. Ces projets d'arrêtés exécutent les deux projets de décrets de même nom, en cours de finalisation, sur lesquels l'Autorité a rendu l'avis n° 124/2017 le 7 novembre dernier.

3. Les avant-projets d'arrêtés soumis pour avis ont notamment pour but de :
 - désigner les services d'inspection de la direction générale opérationnelle de l'Economie, de l'Emploi et de la Recherche ;
 - déterminer les modalités de la méthode de priorétisation des contrôles et de fixation des amendes par échantillonnage-extrapolation, instituée par les avant-projets de décret (articles 35 à 37) ;

4. Les avants-projets modifient une série de textes réglementaires afin d'habiliter, dans chaque matière concernée, les inspecteurs du Département de l'Inspection, à procéder aux contrôles conformément aux avant-projets de décret. Dans ce cadre, une série de dispositions relatives à l'« *e-PV* » (le procès-verbal électronique), ont été introduites afin d'asseoir légalement les opérations de contrôle et leurs suites, effectuées en recourant à cet outil au niveau de la Région wallonne. Il est également prévu de créer par ces mêmes arrêtés une banque de données dite « *Amadeus* » définie comme « *la banque de données de l'administration compétente, qui contient les données relatives aux missions qui lui sont attribuées* » (article

1 8° *juncto* article 5 du projet d'arrêté économique, de l'emploi et recherche scientifique ; article 2 8° *juncto* article 6 du projet d'arrêté recyclage et reconversion).

2. EXAMEN DE LA DEMANDE D'AVIS

1. La banque de données « e-PV », la banque de données « Amadeus » et l'échange d'information entre ces banques de données

5. Les projets d'arrêtés spécifient les dispositions relatives à l'échange d'information entre la banque de données « e-PV », à savoir, la banque de données visée à l'article 100/6 du Code pénal social, d'une part, et d'autre part, la nouvelle banque de données « Amadeus », évoquée précédemment.

1.1 Références à la législation de protection des données personnelles

6. L'Autorité note qu'il est prévu que l'échange électronique d'informations via « l'e-PV, la banque de données e-PV, et banque de données Amadeus » se fasse conformément aux dispositions de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité sociale (ci-après, « loi BCSS ») (respectivement, les articles 5 § 2 et 6 § 2 des projets d'arrêtés). L'Autorité souligne que ces deux législations ne sont pas autosuffisantes et que le RGPD doit également être cité à titre de « *lex generalis* » en ce qui concerne la protection des données personnelles.
7. L'Autorité note en outre qu'à l'occasion de cet échange de données, il sera fait usage des « *numéros d'identification visés à l'article 8 § 1 de la loi BCSS* », c'est-à-dire, le numéro de RN (respectivement, articles 5 § 2 et 6 § 2 des projets d'arrêtés). L'Autorité attire l'attention du demandeur sur l'existence de règles relatives à l'utilisation de ce numéro, y compris des obligations d'autorisation préalable, en vertu de la loi du 8 août 1983 organisant un registre national des personnes physiques.

1.2 Légalité

a) Base légale de la banque de données « Amadeus »

8. Le demandeur n'a transmis aucun élément permettant de déterminer que la banque de données « Amadeus » aurait une autre base légale que les projets d'arrêtés d'application eux-mêmes, ce qui n'est pas admissible au regard de l'article 22 de la Constitution.
9. Selon les informations complémentaires transmises¹, le demandeur estime que cette banque de données trouve sa base légale dans les chapitres 6 des projets de décrets. L'Autorité ne partage pas ce point de vue. Les chapitres 6 des derniers projets de décrets transmis par le demandeur² ne contiennent qu'un principe général relatif à la désignation du responsable du traitement des données traitées dans le cadre de chaque décret respectif, ainsi que des dispositions spécifiques concernant la limitation des droits de protection des données (droit d'information, droit d'accès, droit de rectification, droit à la limitation du traitement). L'Autorité n'y voit aucun élément permettant de constituer la base légale de création d'une banque de données telle qu'« Amadeus », et invite dès lors très fortement le demandeur à revoir ses projets de décrets et d'arrêtés d'application sur ce point, afin de rencontrer les exigences de prévisibilité de l'article 22 de la Constitution.
10. De l'avis de l'Autorité, l'article 22 de la Constitution requiert une intervention légale formelle pour mettre en place et/ou encadrer des banques de données publiques d'une telle ampleur. La banque de données « Amadeus » contient des données à caractère personnel judiciaires au sens de l'article 10 du RGPD et de l'article 10 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel³, ce qui implique en outre que des garanties appropriées pour les droits et libertés

¹ Email du demandeur du 10 décembre 2018.

² Projets de décrets « finaux » transmis par le demandeur le 28 novembre 2018.

³ Art. 10. § 1er. de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel : « En exécution de l'article 10 du Règlement, le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions pénales ou aux mesures de sûreté connexes est effectué :
 1° par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige; ou
 2° par des avocats ou d'autres conseils juridiques, pour autant que la défense de leurs clients l'exige; ou
 3° par d'autres personnes lorsque le traitement est nécessaire pour des motifs d'intérêt public important pour l'accomplissement de tâches d'intérêt général confiées par ou en vertu d'une loi, d'un décret, d'une ordonnance ou du droit de l'Union européenne; ou
 4° pour les nécessités de la recherche scientifique, historique ou statistique ou à des fins d'archives; ou
 5° si la personne concernée a autorisé explicitement et par écrit le traitement de ces données à caractère personnel pour une finalité ou plusieurs finalités spécifiques et si leur traitement est limité à ces finalités; ou
 6° si le traitement porte sur des données à caractère personnel manifestement rendues publiques par la personne concernée, de sa propre initiative, pour une finalité ou plusieurs finalités spécifiques et si leur traitement est limité à ces finalités.

des personnes concernées soient prévues, comme une base légale adéquate (voir Avis n° 12/2018 de la Commission de la protection de la vie privée du 7 février 2018 sur l'avant-projet de loi portant l'introduction du procès-verbal électronique pour les services d'inspection du Service public fédéral Economie, PME, Classes moyennes et Energie et modifiant le Code pénal social , p. 4 § 7).

11. La nécessité d'une législation claire fondant la base de données « *Amadeus* » est notamment illustrée par le fait que les catégories de données traitées et les finalités envisagées pour la banque de données « *Amadeus* » selon les projets d'arrêtés sont très similaires à celles retenues par le législateur fédéral en ce qui concerne la banque de données « *Ginaa* », à savoir, « *la banque de données de l'administration compétente, qui contient les données relatives aux missions qui lui sont attribuées [...]* » dans le cadre du Code pénal social (article 16 19° du Code pénal social). Or, cette base de données « *Ginaa* » a fait l'objet d'un ancrage légal explicite à l'article 100/11 du Code pénal social. (Pour une comparaison des finalités et données traitées dans « *Ginaa* » avec « *Amadeus* », voir sous les titres « finalité » § 19 « proportionnalité » § 24).

b) Protocole relatif aux données transférées par des institutions fédérales le cas échéant

12. L'Autorité comprend que le demandeur, autorité régionale, entend utiliser des données issues de la banque de données fédérale « *e-PV* ». Selon les explications complémentaires du demandeur, certaines de ces données seront d'ailleurs intégrées dans la banque de données « *Amadeus* »⁴. Dans cette mesure, l'Autorité attire l'attention du demandeur sur les conditions imposées par l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, en cas de transfert de données à caractère personnel de l'autorité fédérale à toute autre autorité publique, lorsque ce transfert est fondé sur le nécessaire respect d'une obligation légale ou sur la nécessaire exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique (articles 6.1.c ou 6.1.e du RGPD). Dans un tel cas, les autorités concernées doivent conclure un protocole d'échange de données, adopté après les avis respectifs du délégué à la protection des données de l'autorité publique fédérale détenteur des données à caractère

§ 2. Le responsable du traitement et, le cas échéant, le sous-traitant établissent une liste des catégories de personnes, ayant accès aux données à caractère personnel avec une description de leur fonction par rapport au traitement des données visées. Cette liste est tenue à la disposition de l'autorité de contrôle compétente. Le responsable du traitement et, le cas échéant, le sous-traitant veillent à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées. »

⁴ Email du demandeur à l'Autorité du 10 décembre 2018.

personnel et du destinataire. Ce protocole doit aussi être publié sur le site internet des responsables du traitement concernés (article 20 de la loi du 30 juillet 2018 précitée).

1.3 Responsable de traitement

13. Selon les décrets de base en projet, le responsable des traitement des données à caractère personnel envisagés dans le cadre des traitements concernés est « *le département de l'Inspection de la Direction générale opérationnelle de l'Economie, de l'Emploi et de la Recherche du Service public de Wallonie* » (articles 38 des décrets de base). Selon les projets d'arrêtés, « *le responsable du traitement des données à caractère personnel, au sens de la réglementation en matière de protection des données à caractère personnel est le Directeur Général de la Direction générale opérationnelle Economie, Emploi et Recherche du Service public de Wallonie* » (respectivement, articles 18 et 19 des projets d'arrêtés). L'Autorité recommande d'uniformiser la désignation : soit un département, soit une fonction de direction. L'Autorité se demande d'ailleurs quelle est la valeur ajoutée d'une réitération de ce principe dans les arrêtés d'application.

14. L'Autorité note qu'en ce qui concerne la banque de données « *Amadeus* », les projets d'arrêtés spécifient que le Directeur général de la Direction générale opérationnelle Economie, Emploi et Recherche du Service public de Wallonie est le responsable du traitement au sens de l'article 4.7 du RGPD (selon - respectivement - les articles 8 et 9 des projets d'arrêtés). L'Autorité en prend acte, sous réserve de légalité de cette base de données « *Amadeus* », comme observé ci-dessus. Il ne serait bien entendu pas nécessaire d'ajouter une telle précision dans les arrêtés d'application si la base de données « *Amadeus* » était créée par les décrets de base : sauf spécification contraire, cette base de données serait alors réglementée par le responsable de traitement désigné de manière générale dans les articles 38 des décrets de base.

15. En ce qui concerne la banque de données « *e-PV* », l'Autorité conseille de nuancer le principe général formulé aux articles 18 et 19 des projets d'arrêtés, désignant le « *Directeur Général de la Direction générale opérationnelle Economie, Emploi et Recherche du Service public de Wallonie* » comme responsable de traitement. Si le demandeur conserve cette désignation dans les arrêtés, contrairement à l'avis de l'Autorité, alors, l'Autorité invite le demandeur à clarifier que ces dispositions générales ne modifient en rien les règles édictées au niveau fédéral en ce qui concerne le responsable de traitement de la base de données e-PV, à savoir, « *l'Etat belge, représenté par le ministre compétent pour l'emploi, par le ministre compétent pour les affaires sociales et par le ministre compétent pour la justice, est responsable pour le traitement des données [...]* » (article 100/6 du Code pénal social). Une

telle précision ne serait bien entendu pas nécessaire si le demandeur se contentait de désigner le responsable de traitement dans les décrets de base, comme le recommande l'Autorité, ce qui n'empêcherait pas le demandeur de prévoir dans les arrêtés d'application un renvoi aux dispositions correspondantes (articles 38 des décrets de base) pour plus de clarté concernant le responsable de traitement.

1.4 Finalités déterminées et explicites

16. Les finalités d'un traitement de données doivent être déterminées et explicites, en application de l'article 5.1.b du RGPD.
17. Les avant-projets d'arrêtés imposent un strict respect de la finalité pour laquelle ces banques de données peuvent être utilisées, à savoir respectivement, les finalités décrites à l'article 100/6 du Code pénal social pour ce qui est d'e-PV, et les finalités reprises respectivement aux articles 8 et 9 des projets d'arrêtés, pour ce qui est d'« *Amadeus* » (sous réserve de base légale adéquate).
18. Ainsi, selon les projets d'arrêtés, les finalités d'« *Amadeus* » sont triples :

« 1° la collecte de l'information qui est utile pour permettre à l'administration compétente d'exercer les missions qui lui sont attribuées dans ou en vertu du décret du [...] (date) ;

2° la collecte de l'information relative à la poursuite des infractions qui est utile pour permettre aux inspecteurs d'exercer leurs missions légales relatives à la politique économique, à la politique de l'emploi et à la recherche scientifique ;

3° la collecte de l'information relative à la poursuite des infractions qui est utile pour permettre aux inspecteurs de combattre de manière adéquate les infractions relatives à la politique économique, à la politique de l'emploi et à la recherche scientifique ».

19. Selon les explications complémentaires du demandeur, il semble que cette base de données serve essentiellement à déclencher des procédures d'amendes administratives⁵. L'Autorité en prend acte mais note que l'intitulé des finalités semble permettre de nombreuses autres

⁵ « *AMADEUS n'est pas un doublon de la base de données e-PV. En effet, bien que les données reprises dans les pro-jusitita soient en partie encodées dans l'application, elles sont en réalité les éléments déclencheurs d'une procédure de traitement de ceux-ci, procédure visant à infliger une amende administrative dans les cas où l'analyse des documents et la procédure contradictoire mise en place permettraient au fonctionnaire sanctionnateur de prendre une telle décision* », informations complémentaires fournies par le demandeur à l'Autorité le 10 décembre 2018.

finalités, définies de manière fonctionnelle par rapport aux missions de l'administration compétente, à l'instar de la base de données « *Ginaa* » prévue dans le Code pénal social, où les modalités d'échanges avec les données de l'« e-PV » sont d'ailleurs également réglementées (Article 100/11 du Code pénal social⁶).

20. L'Autorité estime toutefois que ces finalités sont suffisamment déterminées et explicites.

1.5 Proportionnalité

21. Les données personnelles traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, en application de l'article 5.1.d du RGPD. Ce principe vaut tant pour les catégories de données à caractère personnel traitées que pour la manière dont elles sont traitées (condition d'accès, mesures de sécurité et méthodologie de traitement de données).

a) Catégories de données à caractère personnel traitées et personnes concernées

22. Les projets de décrets finalisés tels que transmis au Secrétariat de l'Autorité ont précisé de manière exhaustive les catégories de données appelées à être traitées dans le cadre de procès-verbaux, comme l'avait recommandé l'Autorité dans son avis 124/2018 du 7 novembre 2018 (article 19 de ces projets de décrets⁷). En ce qui concerne les traitements de données effectués dans le cadre de procès-verbaux constatant une infraction aux législations et réglementations visées dans les décrets et leurs arrêtés d'application, l'Autorité estime donc que les catégories de données concernées sont suffisamment précisées dans les décrets de base, pour autant que leur texte soit maintenu sur ce point.

23. Quant aux catégories de données traitées dans le cadre de la banque de données « *Amadeus* » - sous réserve de base légale - elles y sont qualifiées de données « *sociales* à

⁶ Pour une liste des finalités de cette base de données « *Ginaa* », voir l'article 100/11 du Code pénal social : « *Le stockage et le fait de tenir à jour les données visées à l'alinéa 3 poursuivent les objectifs suivants : 1° la collecte de l'information qui est utile pour permettre à l'administration compétente d'exercer les missions qui lui sont attribuées dans ou en vertu du Livre Ier; 2° la collecte de l'information relative à la poursuite des infractions qui est utile pour permettre aux acteurs de la lutte contre le travail illégal et la fraude sociale d'exercer leurs missions légales; 3° la collecte de l'information relative à la poursuite des infractions qui est utile pour permettre aux acteurs de la lutte contre le travail illégal et la fraude sociale de combattre de manière adéquate le travail illégal et la fraude sociale; 4° l'élaboration de statistiques internes et externes.* ».

⁷ Articles 19 des projets de décrets (version communiquée par le demandeur le 18 novembre 2018) : « *Tout procès-verbal constatant une infraction aux législations et réglementations visées à l'article 3 ainsi qu'aux dispositions du présent décret contient les données suivantes : 1° l'identité de l'inspecteur verbalisant ; 2° la disposition en vertu de laquelle l'inspecteur verbalisant est compétent pour agir ; 3° le lieu et la date de l'infraction ; 4° l'identité de l'auteur présumé et des personnes intéressées ; 5° la disposition légale violée ; 6° un exposé succinct des faits en rapport avec les infractions commises ; 7° les dates et lieu de rédaction du procès-verbal, le lien éventuel avec d'autres procès-verbaux, et, le cas échéant, l'inventaire des annexes* ».

caractère personnel au sens de l'article 2, al. 1^{er}, 6° de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale » (articles 8 et 9 des avant-projets d'arrêtés).

24. Ces données sont définies comme étant les « *données déterminées par le Gouvernement* » à propos de :

« 1° *toute personne suspectée d'être auteur ou co-auteur d'une infraction* ;
 2° *toute personne à qui une amende administrative peut être infligée* ;
 3° *tout travailleur ou personne qui est concerné ou considéré comme étant concerné par une infraction* » (articles 8 et 9 des avant-projets d'arrêtés)⁸.

25. Il s'agit donc de données personnelles relatives à des condamnations pénales et à des infractions visées à l'article 10 du RGPD. Il incombe au responsable de traitement de cette future banque de données de réaliser une analyse de l'impact des traitements de données personnelles envisagés, conformément à l'article 35.2 (a) du RGPD, lequel impose la réalisation d'une telle analyse préalablement à tout traitement de données qui implique le traitement à large échelle de telles données.

26. Il incombe au responsable du traitement de transmettre cette analyse d'impact pour consultation à l'Autorité de protection des données si les conditions de l'article 36.1 du RGPD sont réunies.

27. L'Autorité estime donc que le traitement envisagé répond au prescrit de l'article 5.1.d du RGPD en ce qui concerne la délimitation des catégories de données traitées et les personnes concernées par la banque de données « *e-PV* », mais réserve ses commentaires en ce qui concerne la banque de données « *Amadeus* » en l'absence d'une base légale, et en l'absence d'une analyse d'impact réalisée à ce sujet au stade législatif et/ou préalablement au traitement⁹.

28. Enfin, dans la mesure où certaines données « *e-PV* » seront reprises dans la banque de données « *Amadeus* » selon les explications complémentaires du demandeur¹⁰, l'Autorité

⁸ L'Autorité note que les données traitées sont similaires à celles énoncées pour la banque de données « *Ginaa* », laquelle contient, au niveau fédéral, « *les données déterminées par le Roi à propos de : 1° toute personne suspectée d'être (co)auteur d'une infraction; 2° toute personne à qui une amende administrative peut être infligée; 3° tout travailleur ou personne qui est concerné ou considéré comme étant concerné par une infraction.* » (article 100/11 § 3 du Code pénal social).

⁹ Article 23 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel : « *En exécution de l'article 35.10 du Règlement, une analyse d'impact spécifique de protection des données est effectuée avant l'activité de traitement, même si une analyse d'impact générale relative à la protection des données a déjà été réalisée dans le cadre de l'adoption de la base légale* ».

¹⁰ Email du demandeur à l'Autorité du 10 décembre 2018.

recommande également de préciser quelles catégories de données « *e-PV* » seront reprises dans la Banque de données « *Amadeus* ».

b) Autorisations préalables des autorités publiques ayant accès à « Amadeus »

29. Les avant-projet d'arrêtés se réfèrent à des « *autorisations* » d'accès à la banque de données « *Amadeus* » sans préciser sous quelles conditions et modalités ces autorisations sont accordées. Article 10 des projets d'arrêtés disposent en effet : « *Chaque instance qui est autorisée à accéder [à la banque de données « e-PV »¹¹ et] à la banque de données « Amadeus » établit une liste mise à jour régulièrement des personnes qu'elle a désignées afin d'exercer ce droit d'accès* ».
30. L'Autorité invite le demandeur à prévoir les conditions de telles autorisations préalables explicitement dans le décret, ou à tout le moins, faire référence aux dispositions pertinentes dans d'autres législations, afin de respecter le prescrit de l'article 22 de la Constitution, pour autant, bien entendu, que la banque de données « *Amadeus* » soit créée de manière légitime, sur pied d'une base légale adéquate.
31. A cet effet, le demandeur pourra notamment s'inspirer des conditions d'accès aux banques de données fédérales « *Ginaa* » ou « *e-PV* » comme explicité ci-dessous.
32. Ainsi par exemple, au niveau fédéral, l'autorisation préalable de la chambre sécurité sociale et santé du comité de sécurité de l'information conditionne l'accès des autorités publiques à la banque de données fédérale « *Ginaa* », dont la banque de données « *Amadeus* » semble fortement inspirée, comme indiqué précédemment. Cela est précisé de manière explicite dans les dispositions du Code pénal social relatives à « *Ginaa* »¹².
33. De même, il appartient au demandeur de préciser si une autorisation de la « *Commission Wallonie-Bruxelles de contrôle d'échange de données* » est requise préalablement aux échanges de données envisagés dans le cadre de la base de données « *Amadeus* ». Selon

¹¹ Les conditions d'accès à la banque de données « *e-PV* » sont définies dans le Code pénal social par référence à l'autorisation de la chambre sécurité sociale et santé du Comité de sécurité de l'information (article 100/10 § 1) : « *Sans préjudice des articles 54 et 55 et moyennant l'autorisation de [la chambre sécurité sociale et santé du comité de sécurité de l'information], les catégories de fonctionnaires habilités par le Roi des services d'inspection sociale fédéraux désignés par le Roi ont accès aux données suivantes de la banque de données e-PV [...]* ».

¹² Article 100/12 § 3 du Code pénal social, tel que modifié par l'article 58 de la loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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

l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française - portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, l'intervention préalable de la « *Commission Wallonie-Bruxelles de contrôle d'échange de données* », définie comme un « *organe indépendant chargé de régler les relations entre la Banque-Carrefour d'échange de données, les utilisateurs, les sources authentiques de données, les banques de données issues de sources authentiques et les autorités publiques, ainsi qu'entre les sources authentiques de données et les banques de données issues de sources authentiques elles-mêmes* » (article 2.6 de l'accord de coopération)¹³.

34. Or, dans ses explications complémentaires, le demandeur explicite que « *Amadeus est une application informatique permettant la gestion des dossiers devant être instruits en amendes administratives. Plus précisément, il s'agit d'un outil informatique dont les fonctionnalités principales sont l'aide au traitement des dossiers, la génération de courriers, l'élaboration de rapports statistiques, le recours aux sources de données authentiques. Cet outil dispose effectivement d'une base de données quant aux dossiers qui y sont gérés.* »¹⁴ Ce recours à des sources authentiques semble donc à première vue justifier une intervention de la Commission Wallonie-Bruxelles, sous réserve de précisions du demandeur à ce sujet. Il y a également lieu d'être attentif aux éventuelles autorisations requises par les échanges de données envisagé aux articles 23 des projets de décrets¹⁵.
35. Afin d'éviter toute confusion, à toutes fins utiles, l'Autorité souligne que les conditions d'autorisation préalable d'accès des Autorités publiques à « *Amadeus* », qu'il y a lieu de préciser, n'ont *a priori* rien à voir avec les conditions d'accès des citoyens concernés aux données traitées par ces mêmes autorités : ce dernier point fait l'objet de certaines dispositions du chapitre 6 des Décrets de base, qui ne constituent pas en la matière une base légale définissant les conditions d'accès à la base de données pour les autorités publiques concernées.

¹³ A la connaissance de l'Autorité, la Commission Wallonie-Bruxelles de contrôle des échanges de données n'a pas d'existence effective. Au sujet de cette Commission et de son rôle, voir l'avis n° 34/2014 de la CPVP du 30 avril 2014 concernant un projet d'accord de coopération entre la Région wallonne et la Communauté française portant exécution de l'Accord de Coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative.

¹⁴ Email du demandeur à l'Autorité du 10 décembre 2018.

¹⁵ L'article 23 des projets de décrets prévoit que « les inspecteurs communiquent les renseignements recueillis lors de leur inspection aux institutions publiques et aux institutions coopérantes de sécurité sociale, aux inspecteurs des autres services d'inspection, ainsi qu'à tous les autres fonctionnaires chargés du contrôle d'autres législations ou en application d'une autre législation, si ces renseignements peuvent intéresser ces derniers dans l'exercice du contrôle dont ils sont chargés ou en application d'une autre législation ».

c) Désignation des catégories d'agent ayant accès à « Amadeus »

36. L'Autorité note que selon les projets d'arrêtés, une stricte gestion des accès à la banque de données « Amadeus » (et à la banque de données « e-PV ») est imposée à chaque instance qui est autorisée à y accéder: une liste mise à jour régulièrement des personnes qu'elle a désignées afin d'exercer ce « droit d'accès »¹⁶, doit être tenue par « chaque instance qui est autorisée à accéder à la banque de données « Amadeus » (et « e-PV ») (article 10 des projets d'arrêtés).
37. L'Autorité souligne que cette liste doit être tenue à sa disposition à la demande, en vertu de l'article 10 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, laquelle impose une telle obligation au responsable du traitement (ou sous-traitant) de données à caractère personnel relatives aux condamnations pénales et aux infractions pénales (telles que les données « e-PV » contenues dans « Amadeus »¹⁷).
38. L'Autorité recommande en outre que cette liste soit être déterminée par arrêté, à l'instar de la banque de données « e-PV », pour laquelle les catégories de fonctionnaires qui ont accès aux données sont habilités par le roi à avoir accès à un certain nombre de données bien déterminé, listées de manière exhaustive dans le Code pénal social (article 100/10 du Code pénal social). Des conditions d'accès spécifiques sont déterminées pour l'accès à l'entièreté de l'e-PV (notamment l'exigence d'un intérêt à consulter ces données), et une autorisation expresse de l'autorité judiciaire est requise lorsque les données reprises dans l'e-PV ont été établies durant l'exécution de devoirs prescrits par l'autorité judiciaire.
39. Il semble que ces conditions d'accès sont à tout le moins en partie pertinentes pour « Amadeus » qui contient certaines données des « e-PVs ». Certes, selon les explications complémentaires du demandeur, « Amadeus » n'est pas un doublon d'e-PV mais les données reprises dans les pro-justitia sont en partie encodées dans l'application¹⁸.

¹⁶ En ce qui concerne la formulation de l'article 10 des projets d'arrêtés, l'Autorité se demande dans quelle mesure la référence à un « droit d'accès » des autorités aux banques de données ne porte pas à confusion par rapport aux droits d'accès des citoyens à leurs données personnelles tel que visé à l'article 40 des décrets de base.

¹⁷ Email du demandeur à l'Autorité du 10 décembre 2018.

¹⁸ Explications complémentaires du demandeur dd. 10-12-2018 : « AMADEUS n'est pas un doublon de la base de données e-PV. En effet, bien que les données reprises dans les pro-justitia soient en partie encodées dans l'application, elles sont en réalité les éléments déclencheurs d'une procédure de traitement de ceux-ci, procédure visant à infliger une amende administrative dans les cas où l'analyse des documents et la procédure contradictoire mise en place permettraient au fonctionnaire sanctionnateur de prendre une telle décision. ».

40. Dans cette mesure, l'Autorité recommande donc que le demandeur envisage de préciser - s'il y a lieu - les éventuels niveaux d'accès autorisés à la banque de données « *Amadeus* » en fonction du besoin d'en connaître des catégories d'agents concernés, selon les catégories de données traitées.

d) Mesures de sécurité (confidentialité et gestion des accès)

41. Toutes les personnes qui ont accès à la banque de données Amadeus (et à la banque de données « *e-PV* ») sont en outre tenues de « *prendre les mesures nécessaires afin de garantir le caractère confidentiel des données à caractère personnel qui sont contenues dans ces banques de données* », et sont tenues de garantir que ces données seront uniquement utilisées en vue des finalités annoncées à l'article 9 pour ce qui concerne la banque de données « *Amadeus* » (et à l'article 100/6 du Code pénal social pour ce qui concerne la banque de données « *e-PV* »). Cette disposition répond aux obligations de confidentialité imposées à l'article 10 § 2 de la loi précitée du 30 juillet 2018, laquelle impose au responsable de traitement et à son sous-traitant de veiller à ce que les personnes désignées pour traiter de telles données soient tenues au respect de leur confidentialité par une obligation légale, statutaire ou contractuelle.
42. Les projets d'arrêtés stipulent que toute violation du caractère confidentiel des données « *e-PV* » ou « *Amadeus* », qualifié de « *secret professionnel* », sera en outre punie conformément à l'article 458 du Code pénal (article 10 § 3 des projets d'arrêtés). L'Autorité en prend note. Cette disposition rencontre l'obligation faite au responsable de traitement à l'article 24 du RGPD de prendre toutes les mesures techniques et organisationnelles nécessaires pour assurer la sécurité des données, d'autant que le traitement de données à caractère personnel sensibles, dont celles relatives à des condamnations pénales (article 10 RGPD), sont de nature à justifier des mesures de sécurité plus strictes. L'Autorité se réfère à ce titre aux « *mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel* » figurant sur son site web¹⁹.
43. L'Autorité relève toutefois qu'au-delà de la définition des personnes désignées pour accéder à la base de données « *Amadeus* », aucune disposition ne garantit qu'un contrôle des accès (« *loggings* ») soit effectué, alors que selon les informations complémentaires fournies par le

¹⁹ <http://www.privacycommission.be/fr/static/pdf/mesures-de-reference-vs-01.pdf>

demandeur, il semble qu'un tel contrôle ait bien lieu²⁰. Un tel contrôle est une mesure de sécurité indispensable, selon une jurisprudence constante de l'Autorité. Il y a lieu de le prévoir explicitement dans les Décrets de base, ou de renvoyer à la législation pertinente organisant ce contrôle par le Service public de Wallonie, le cas échéant.

e) **Méthodologie des contrôles effectués**

44. Les projets d'arrêtés précisent la « *méthodologie particulière de contrôle* » des législations visées par le projet d'arrêté (respectivement aux articles 16/17 - 17/18, et suivants des projets d'arrêtés).
45. La méthodologie vise à déterminer les priorités du département de l'Inspection chargée du contrôle « *en recourant à des techniques d'analyse statistiques telles que la comparaison des données, l'exploration des données et l'analyse de banques de données internes et externes* » (Ibid).
46. Les principes de base de ces « *méthodes particulières de contrôle* » sont définies dans le chapitre homonyme des projets de décrets (articles 35 et 36 du Chapitre V de ces décrets de base). Selon ces projets de décrets, l'échantillonnage peut également servir à extrapoler les résultats d'un contrôle réalisé sur un échantillon représentatif, à l'ensemble des éléments ayant constitué la base de l'échantillon, et ce, lorsque les législations et réglementations contrôlées le prévoient expressément, selon des modalités déterminées par le Gouvernement (articles 35 et 36 des décrets de base). Dans l'exposé des motifs des décrets de base, le demandeur se réfère à des mécanismes similaires utilisés dans le cadre de l'assurance obligatoire soins de santé et indemnités²¹, et à la validation de ce système par le Conseil d'Etat dans son arrêt 227.073 du 9 avril 2014. L'Autorité en prend note.

²⁰ Informations complémentaires du demandeur à l'Autorité, le 10 décembre 2018 : « *La gestion des utilisateurs est réalisée en interne. Seuls les agents autorisés pourront y avoir accès moyennant des identifiants et mots de passe délivrés par l'administrateur de l'application et selon les règles établies et contrôlées par le Département des Technologies de l'information et de la communication du SPW. L'utilisation des données à caractères personnels utiles pour le traitement des dossiers est quant à elle réglementée par le chapitre 6 des Décrets.* »

²¹ Loi du 14 juillet 1994 relative à l'assurance-maladie invalidité telle que modifiée par l'article 31 de la loi du 18 décembre 2016 : « § 2/1. Pour constater les infractions visées à l'article 73bis et calculer la valeur des prestations indûment remboursées par l'assurance obligatoire soins de santé, le personnel d'inspection visé au § 1er peut entre autres utiliser la méthode de vérification par échantillonnage et extrapolation. Cette méthode consiste à :
 1° établir la base de sondage en identifiant et en définissant un ensemble de cas indépendants qui seront examinés;
 2° effectuer un tirage aléatoire dans cette base de sondage pour constituer un échantillon et documenter la méthode de tirage;
 3° analyser les cas dans cet échantillon et calculer dans l'échantillon le pourcentage des montants indûment remboursés par l'assurance de santé obligatoire;
 4° calculer la valeur en dessous de laquelle le pourcentage de la population que l'on cherche à estimer, a une probabilité inférieure à 2.5 % de se trouver;
 5° utiliser cette valeur pour calculer le montant à récupérer pour toutes les prestations de la base de sondage. »

47. L'Autorité comprend que cette méthode vise à un gain de temps pour l'Inspection concernée²² ainsi qu'un traitement équitable entre les administrés de petite taille et les grandes structures où « *le contrôle ne permettra jamais de vérifier la correction de tous les éléments à contrôler* » (Exposé des motifs des décrets de base tels que communiqués à l'Autorité préalablement à son avis n° 124/2018 du 7 novembre 2018, p. 10). Les méthodes utilisées sont détaillées aux articles 21 et suivantes des projets d'arrêtés, où sont définies les notions statistiques utilisées pour chaque législation concernée. L'Autorité rappelle à toutes fins utiles que cette méthodologie doit aboutir à minimiser les résultats faussement positifs. L'Autorité renvoie à cet égard aux recommandations du rapport « *Big Data* » publié par la Commission vie privée en 2017²³.
48. Sans préjuger du succès de la méthode statistique envisagée dans des cas concrets qui lui seraient éventuellement soumis, l'Autorité note que des garanties sont prévues en faveur des droits et libertés des personnes concernées. En effet, en ce qui concerne la technique d'échantillonnage, « *l'inspecteur explique le choix et le contenu de la méthode qu'il a utilisée dans son rapport d'inspection* » (respectivement, articles 17 et 18 des projets d'arrêtés). L'Autorité note également que les entreprises concernées par le contrôle peuvent renverser la présomption découlant des « *extrapolations* », par exemple « *en établissant la validité de tout ou partie du pourcentage de la subvention incriminée* » (articles 23, 29 du projet d'arrêté politique économique, emploi et recherche scientifique).
49. Enfin, l'Autorité rappelle que le responsable de traitement est responsable d'assurer la qualité des données personnelles faisant l'objet d'un contrôle. Il est en effet tenu de prendre « *toutes les mesures raisonnables* » pour que les données à caractère personnel qui sont « *inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder* » (article 5.1.d *juncto* article 5.2 du RGPD). En aucun cas, cette responsabilité ne peut être assumée à titre individuel par l'un ou l'autre agent de la fonction publique tel qu'un inspecteur. L'Autorité s'interroge dès lors sur la portée des dispositions insérées respectivement aux articles 17.2 et 18.1 des projets d'arrêtés : « *avant le contrôle des dossiers individuels, l'inspecteur procède à l'examen de la complétude des bases de données existantes et à l'élimination des données erronées, redondantes ou incertaines* ». A cet égard, l'Autorité invite le demandeur à revoir ces dispositions dans la mesure où elles mettent à charge des inspecteurs la qualité des données sur base desquelles sont effectuées les contrôles. De plus, l'« *examen de la complétude des bases de données existantes* »,

²² Informations complémentaires communiquées par le demandeur le 13 novembre 2018 (note au gouvernement wallon du 22 octobre 2018, « *projet d'arrêté portant exécution du décret du [...] relatif au contrôle des législations et réglementations relatives à la politique économique, à la politique scientifique ainsi qu'à l'instauration d'amendes administratives applicables en cas d'infraction à ces législations et réglementations* », première lecture, p. 2).

²³ Ce rapport est disponible via le lien suivant : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Rapport_Big_Data_2017.pdf.

l' « *élimination des données erronées, redondantes ou incertaines* » préalablement à un contrôle semble à première vue une tâche fort hasardeuse, sauf à démontrer qu'un inspecteur dispose à titre individuel des ressources nécessaires pour ce faire. Tout au plus l'inspecteur pourrait-il être tenu de mettre en œuvre les meilleurs moyens à sa disposition pour ce faire, sans que cette obligation ne décharge le responsable de traitement de veiller à la qualité des données de manière structurelle et organisée dès la conception du traitement de données concerné (ex. base de données « *Amadeus* »), en vertu de l'article 25 du RGPD *juncto* les articles 5.1.d et 52 du RGPD.

PAR CES MOTIFS,

L'Autorité émet un avis défavorable, compte tenu des remarques suivantes :

- Considérants 9 et suivants : prévoir une base légale décrétable pour la base de données « *Amadeus* » ;
- Considérant 28 : préciser quelles catégories de données « *e-PV* » seront reprises dans la Banque de données « *Amadeus* » ;
- Considérants 38 et 40: déterminer par arrêté la liste des catégories de fonctionnaires qui ont accès à « *Amadeus* » et déterminer s'il y a lieu les éventuels niveaux d'accès en fonction du besoin d'en connaître des agents concernées, selon les catégories de données traitées ;
- Considérant 43 : prévoir un contrôle des accès via « *loggings* » ;
- Considérant 49 : revoir les articles 17.2 et 18.1 des projets d'arrêtés de manière à ne pas faire porter aux inspecteurs à titre individuel la charge de la qualité des données utilisées pour l'inspection, alors que le responsable du traitement doit veiller à la qualité des données dès la conception du traitement de données concerné (ex. base de données « *Amadeus* ») en vertu de l'article de l'article 25 du RGPD *juncto* les articles 5.1.d et 52 du RGPD.

L'Autorité émet pour le surplus un avis favorable, à condition de prendre en compte les remarques formulées aux paragraphes suivants :

- Considérant 6: faire référence au RGPD en complément de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

- Considérants 13 et 14 : uniformiser la désignation du responsable de traitement et supprimer les répétitions inutiles des dispositions y relatives dans les projets d'arrêté ;
- Considérants 25 et 26 : réaliser une analyse d'impact relative à la banque de données « *Amadeus* » conformément à l'article 35.2 (a) du RGPD et transmettre cette analyse d'impact pour consultation à l'Autorité si les conditions de l'article 36.1 du RGPD sont réunies ;
- Considérants 29 à 35 : préciser les autorisations nécessaires pour l'accès à « *Amadeus* » par les instances visées à l'article 10 des projets d'arrêté ;

Tenir compte des suggestions suivantes :

- Considérant 7 : tenir compte des règles relatives à l'utilisation du numéro de registre national lors de l'échange de données entre l'« *e-PV* », la banque de données « *e-PV* » et la banque de données « *Amadeus* » ;
- Considérant 12 : tenir compte de l'obligation de conclure un protocole en vertu de l'article 20 de la loi précitée du 30 juillet 2018 en cas de transfert de données à caractère personnel de l'autorité fédérale à toute autre autorité publique, lorsque ce transfert est fondé sur le nécessaire respect d'une obligation légale ou sur la nécessaire exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ;
- Considérant 47 : la méthode statistique de détermination des priorités du contrôle et de détermination des amendes administratives doit aboutir à minimiser les résultats faussement positifs.

L'Administrateur f.f.,

Le Président

(sé) An Machtens

(sé) Willem Debeuckelaere