



Avis n° 08/2014 du 5 février 2014

Objet: Demande d'avis concernant un avant-projet d'ordonnance portant création et organisation d'un intégrateur de services régional (CO-A-2013-036)

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 la demande d'avis de la Ministre des Travaux publics et des Transports, de l'Informatique et du Port de Bruxelles la Région de Bruxelles-Capitale reçue le 10/07/2013;

Vu le rapport de Monsieur Stefan Verschuere, Vice-Président, et de Madame Mireille Salmon;

Émet, le 5 février 2014, l'avis suivant :

I. CONTEXTE ET OBJET DE LA DEMANDE

1. Malgré la disponibilité de moyens informatiques pour échanger des données électroniques entre administrations, il est encore très fréquent que les citoyens et les entreprises doivent fournir à une administration des données qui sont déjà détenues par une autre administration qui a la charge légale de leur collecte et de leur mise à jour. Ainsi, par exemple, on demande encore aux citoyens et aux entreprises de compléter de nombreux formulaires avec l'adresse de leur domicile ou de leur siège social alors que ces informations se retrouvent de façon tout à fait officielle dans le Registre National ou dans la Banque Carrefour des Entreprises.
2. Cherchant, entre autres, à améliorer cette situation, les entités fédérées ont signé en 2001 un accord de coopération dit «*e-Government*»¹ - visant à mettre en place des services électroniques basés sur les attentes des citoyens et des entreprises et s'appuyant sur des sources authentiques - et un «*transaction engine*» (moteur de transactions). Cet accord de coopération a été renouvelé en 2005 et en 2012 avec un accent particulier mis sur la collecte unique et la réutilisation maximale des données numériques.
3. Depuis lors d'autres initiatives réglementaires ont accru la nécessité de mettre en place les échanges électroniques entre administrations et les sources authentiques.
4. Ainsi, la Directive «*Services*»² visant - à faciliter la liberté d'établissement, la liberté de prestation de services au sein de l'UE et la suppression des discriminations entre les prestataires belges et étrangers - prévoit la mise en place d'échanges électroniques entre les États membres de l'Union Européenne en s'appuyant sur les systèmes d'information de ceux-ci, entre autres, pour s'assurer que les prestataires sont valablement agréés dans leur pays d'origine. Cette Directive impose également aux États membres de simplifier toutes les procédures engagées dans la création et la réalisation d'une activité de service (simplification administrative).
5. La Directive INSPIRE³ vise, quant à elle, la mise en place d'une infrastructure d'information géographique en Europe qui nécessite également l'identification de sources authentiques

¹ Accord de coopération entre l'État fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Commission communautaire flamande, la Commission communautaire française et la Commission communautaire commune concernant la construction et l'exploitation d'une e-plate-forme commune, http://www.awt.be/contenu/tel/gov/accord_cooperation_e-gov.pdf

² Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur, *J.O.*, L 376, 27 décembre 2006

³ Directive 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE), *J.O.*, L 108, 25 avril 2007

dans le domaine cartographique ainsi que des services permettant leur visualisation et leur téléchargement.

6. On peut encore citer, la Directive PSI (Public Sector Information)⁴ qui ambitionne d'assurer une transparence et une concurrence équitable pour l'accès aux données détenues par les autorités publiques.
7. Cependant, les échanges de données électroniques doivent être effectués dans le respect de la législation relative à la protection des données à caractère personnel. À cet égard, la Commission de la protection de la vie privée a déjà publié trois recommandations qui fixent un cadre spécifique destiné aux intégrateurs de services et aux tiers de confiance⁵.
8. Au niveau fédéral, la Banque Carrefour de la Sécurité Sociale joue le rôle d'intégrateur de services dans le domaine social⁶, tandis que la plate-forme eHealth l'exerce dans le domaine de la santé⁷. Ces deux organismes ont un fondement légal. FedICT exerce la mission d'intégrateur de services fédéral pour tous les autres domaines⁸.
9. Au niveau de la Région flamande, le décret du 13 juillet 2012 a confié au DAB Informatie Vlaanderen la mission d'intégrateur de services régional flamand répondant ainsi à la demande pressante de la Commission de donner un fondement légal à la plate-forme d'échanges électroniques de données Magda⁹.
10. Au niveau de la Région wallonne et de la Communauté française, un décret¹⁰ confie à la Banque-carrefour d'échanges de données la mission d'intégrateur de services régional et communautaire¹¹.

⁴ adoptée en 2003 et transposée par l'ordonnance du 6 mars 2008 portant transposition de la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *M.B.*, 8 avril 2008

⁵ Recommandation n° 03/2009 du 1^{er} juillet 2009 concernant les intégrateurs dans le secteur public ; Recommandation n°02/2010 du 31 mars 2010 concernant le rôle de protection de la vie privée des Trusted Third Parties (TTP ou tiers de confiance) lors de l'échange de données ; Recommandation n° 09/2012 du 23 mai 2012 relative aux sources authentiques de données dans le secteur public

⁶ Voy. loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, *M.B.*, 22 février 1990

⁷ Voy. loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions, *M.B.*, 13 octobre 2008

⁸ Voy. loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, *M.B.*, 29 août 2012

⁹ Voy. à ce sujet, l'avis n° 18/2011 du 7 septembre 2011 concernant l'avant-projet de décret relatif à l'institution et à l'organisation d'un intégrateur de services flamand ; voy. également, l'avis n° 11/2009 du 29 avril 2009 concernant le projet d'arrêté du Gouvernement flamand portant exécution du décret du 18 juillet 2008 relatif à l'échange électronique de données administratives et l'avis n° 01/2008 du 16 janvier 2008 relatif au projet de décret relatif à l'échange électronique de données administratives

¹⁰ Décret de la Région wallonne du 10 juillet 2013 portant assentiment à 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, *M.B.*, 23 juillet 2013 ; Décret de la Communauté française du 4

11. En Région de Bruxelles-Capitale, le Centre d'informatique pour la Région Bruxelloise (CIRB) joue déjà le rôle d'intégrateur de services régional par la mise en place, entre autres, d'une plateforme d'échanges qui permet actuellement à l'administration de la Région de Bruxelles-Capitale d'obtenir des données à caractère personnel du niveau fédéral notamment pour octroyer automatiquement des exonérations à des taxes régionales et pour lutter contre la fraude chez les chauffeurs de taxi. Il a également développé diverses plates-formes dont l'objectif premier est de faciliter les démarches pour le citoyen ou l'entrepreneur en privilégiant la dématérialisation des procédures administratives. Il s'agit en particulier du guichet électronique IRISbox, de NOVA, de BO_Secrétariat et de TutelleXchange. Il représente également la Région de Bruxelles-Capitale dans le Comité Général de Coordination de la Banque Carrefour de la Sécurité Sociale.
12. Eu égard à ce qui précède, il convenait de donner un fondement légal au CIRB afin de clarifier la situation pour tous les acteurs régionaux et ainsi répondre aux exigences de la Commission. En effet, l'institution à laquelle cette mission est confiée doit offrir des garanties sur le plan de la stabilité, de la permanence et de l'indépendance. Seule une norme législative peut offrir de telles garanties.
13. C'est pourquoi, la Ministre des Travaux publics et des Transports, de l'informatique et du Port de Bruxelles de la Région de Bruxelles-Capitale a sollicité le 10 juillet 2013 l'avis de la Commission concernant un avant-projet d'ordonnance portant création et organisation d'un intégrateur de services régional. Celui-ci serait chargé de la mise en place et de l'exploitation d'une infrastructure facilitant les échanges électroniques de données entre les Institutions publiques qui dépendent de la Région de Bruxelles-Capitale entre elles (dénommés services publics participants) et avec d'autres intégrateurs de services en vue de réduire les démarches et les charges administratives au bénéfice des citoyens et des entreprises. Le projet favorise notamment la collecte et l'accès coordonné aux données authentiques et partant aux sources authentiques.
14. Lors de sa séance du 4 septembre 2013, la Commission a analysé un premier avant-projet d'ordonnance portant création et organisation d'un intégrateur de service bruxellois.

juillet 2013 portant assentiment à 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, *M.B.*, 23 juillet 2013

¹¹ Voy. à ce sujet, l'avis n° 29/2012 du 12 septembre 2012 concernant un projet d'accord de coopération 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

15. Considérant la nécessité d'encadrer les flux et traitements de données effectués par les autorités et institutions bruxelloises, la Commission a toutefois considéré que les limites du champ d'application de cette ordonnance en avant-projet constituait un problème fondamental. Il apparaissait en effet que les flux et traitements effectués par les institutions communautaires de Bruxelles-Capitale demeuraient dépourvus de tout encadrement, de même que les flux et traitements de données à caractère personnel utiles ou nécessaires à la collaboration entre les institutions des différents niveaux de pouvoir bruxellois.
16. Une réunion au sein de la Commission a eu lieu le 15 janvier 2014 avec le cabinet du demandeur où des solutions ont été proposées et débattues.
17. Un nouvel avant-projet d'ordonnance a été communiqué à la Commission le 21 janvier 2014 afin de satisfaire aux critiques émises et de concrétiser les solutions envisagées. C'est sur cet avant-projet que la Commission rend le présent avis. Un projet d'accord de coopération entre la Région de Bruxelles-Capitale et la Commission Communautaire commune portant sur la désignation d'un intégrateur de services commun pour l'échange électronique de données a été également communiqué à la Commission.

II. EXAMEN DE LA DEMANDE

A.1. Remarques préliminaires quant à l'initiative

18. Du point de vue de la protection des données à caractère personnel dans le cadre d'un échange électronique, l'initiative doit être encouragée. Actuellement, on peut en effet parler d'absence de contrôle approfondi de l'échange électronique de données entre les autorités publiques de la Région de Bruxelles-Capitale.
19. Au sein de la Commission, il n'existe en effet pas de comité sectoriel spécifique compétent pour se prononcer sur le caractère autorisé ou non d'un échange électronique de données envisagé entre les autorités publiques de la Région de Bruxelles-Capitale (système d'autorisation). Cela ne signifie toutefois pas que les services concernés peuvent agir librement. Ils doivent, quoi qu'il en soit, respecter la LVP¹². La protection de la vie privée, et

¹² Ceci concerne notamment la base légale nécessaire à tout traitement de données par un service public. En effet, il résulte des textes européens et de la jurisprudence de la Cour européenne des droits, de l'homme (arrêt Rotaru du 4 mai 2000) qu'une loi réglementant le traitement de données à caractère personnel doit fixer :

- Le genre d'informations pouvant être consignées.
- Les catégories de personnes à propos desquelles on peut collecter des informations.
- Les circonstances dans lesquelles les traitements de données peuvent intervenir.
- Les personnes qui ont le droit de consulter les informations enregistrées.

en particulier des traitements de données à caractère personnel, implique en effet qu'il faut vérifier au cas par cas si les finalités pour lesquelles on souhaite obtenir des données sont compatibles avec celles pour lesquelles les données ont été initialement collectées et si les données dont la communication est demandée sont proportionnelles à la lumière de la finalité. La Commission a également eu l'occasion de le rappeler dans ses avis 01/2008¹³ du 16 janvier 2008 et 29/2012 du 12 septembre 2012¹⁴.

20. Certes, la LVP offre aux instances concernées la possibilité de recueillir l'avis de la Commission concernant un échange électronique de données envisagé, mais un avis n'a toutefois pas la même valeur juridique qu'une décision d'autorisation.
21. Afin de compenser cette lacune dans la législation relative à la protection des données à caractère personnel, l'avant-projet d'ordonnance prévoit la création d'une « *commission de contrôle bruxelloise pour l'échange électronique des données* » dont le rôle sera de régler « *tout échange de données issu de source authentiques de données, de banque de données issues de sources authentiques ou de sources authentiques externes et tous autres flux de données, dans les limites des compétences de la Région de Bruxelles-Capitale* » (article 3 de l'avant-projet d'ordonnance). Ces transferts de données seront opérés par l'intermédiaire de l' « *intégréateur de services régional* ». Par analogie avec les comités sectoriels institués au sein de la Commission, la « *commission de contrôle bruxelloise pour l'échange électronique des données* » délivrera une autorisation pour « *toute communication électronique de données à caractère personnel par l'intégréateur de services régional ou à l'intégréateur de services régional requiert une autorisation préalable, à moins que cette communication électronique ne soit autorisée ou soit exemptée d'autorisation par ou en vertu d'une disposition légale* » (article 32, §1^{er}, al.2). Dans ce cadre, elle devra nécessairement veiller à ce que la LVP soit respectée et appliquée par cette instance. En effet, selon la cour constitutionnelle, la loi du 8 décembre 1992 est « *la réglementation fédérale générale qui a valeur de réglementation minimale pour toute la matière* »¹⁵.
22. Dans la mesure où cet avant-projet d'ordonnance permet de remédier à une lacune ayant des répercussions considérables pour le traitement de données à caractère personnel, cette initiative, et particulièrement les objectifs qu'elle poursuit, ne peut donc être accueillie que favorablement.

-
- La limite de conservation des données.

¹³ *Op.cit.*

¹⁴ *Op.cit.*

¹⁵ C.C., arrêt n° 162/2004, du 20 octobre 2004, B.5.2; arrêt n° 16/2005, du 19 janvier 2005, B.5.2 et arrêt n° 15/2008, du 14 février 2008

B. Analyse de l'avant-projet d'ordonnance à la lumière de la LVP

B.1. Principes de base de l'échange électronique de données administratives

23. L'article 5 de l'avant-projet d'ordonnance prévoit en son § 1^{er} que « *sans préjudice des sources authentiques reconnues à d'autres niveaux de pouvoirs, le Gouvernement de la Région de Bruxelles-Capitale, sur proposition de l'intégrateur de services régional incluant l'avis du service compétent pour la simplification administrative, désigne par arrêté les sources authentiques régionales et les services publics participants chargés de leur collecte, leur mise à jour et leur mise à disposition* ».
24. L'article 5 précise que lors de la désignation de la source authentique, l'arrêté de désignation indique pour chaque source authentique:
- l'identité du gestionnaire de la source authentique chargé de la collecte et du stockage des données authentiques;
 - les modalités selon lesquelles seront tenues à jour et rendues accessibles les données dont l'enregistrement est confié au gestionnaire de la source authentique, outre les obligations auxquelles il est tenu en vertu de la loi;
 - la ou les finalité(s) poursuivie(s) par la source authentique dans la collecte des données qu'elle traite;
 - la liste des données contenues dans la source authentique.
25. L'article 5, § 2 précise que seul le décret pourra établir les banques de données issues de sources authentiques. La Commission constate que cette initiative respecte l'article 22 de la Constitution.
26. Le principe de la "**source authentique**" est intimement lié à celui de la **collecte unique** de données introduit par l'article 5, §3 de l'avant-projet d'ordonnance.
27. La Commission rappelle qu'à cet égard, elle a adopté le 23 mai 2012 une recommandation n°09/2012¹⁶ relative aux sources authentiques de données dans le secteur public contenant les lignes directrices en matière et suggère dès lors au demandeur de s'y référer.
28. Ces deux principes consistent donc à collecter de manière unique des données auprès de citoyens et d'entreprises¹⁷ pour ensuite stocker ces données dans des sources authentiques,

¹⁶ *op.cit*

gérées par des autorités publiques, et les rendre accessibles à d'autres instances (publiques). Le but est d'éviter qu'une autorité ne réclame une donnée à des citoyens / entreprises alors que cette information a déjà été communiquée et est déjà connue d'une autre instance publique¹⁸. Obligation est faite, dans ce cas, de consulter directement la source authentique. Cela s'inscrit également dans le cadre de la simplification administrative.

29. L'exposé des motifs rappelle très justement que « *la collecte unique des données authentiques et l'accès coordonné à ces dernières (...) occupent une place centrale dans le fonctionnement de l'intégrateur de services régional* ».

30. Les sources authentiques occupent en effet, avec les intégrateurs de services¹⁹, une position cruciale dans le contexte de l'e-gouvernement belge et de sa réglementation²⁰.

31. La Commission estime que, vu leur position clé, les sources authentiques ont potentiellement un impact important sur la protection de la vie privée et des données à caractère personnel de chaque citoyen et que lors des traitements de données intervenant dans le cadre d'une source authentique, il convient donc de veiller à ce que la LVP soit rigoureusement respectée. La Commission a en effet toujours insisté dans sa jurisprudence sur le principe selon lequel les données doivent en principe toujours être réclamée auprès de la source authentique. À cet égard, l'utilisation et l'exploitation des sources authentiques constitue une condition essentielle à la garantie d'une protection effective des données à caractère personnel.

32. La Commission rappelle également que la source authentique doit – éventuellement avec l'intervention de l'intégrateur de services régional – garantir le respect du **principe de proportionnalité**. Il est en effet uniquement permis de collecter/conserver/transmettre des données pertinentes et non excessives.²¹ L'avant-projet d'ordonnance précise à plusieurs

¹⁷ Par souci d'exhaustivité, la Commission attire l'attention sur le fait qu'il existe également des sources authentiques contenant des informations créées par les pouvoirs publics eux-mêmes et qui ne sont donc pas réclamées auprès des citoyens/entreprises.

¹⁸ Voy. la recommandation d'initiative n° 09/2012 du 23 mai 2012 relative aux sources authentiques de données dans le secteur public, www.privacycommission.be

¹⁹ Voy. recommandation d'initiative n° 03/2009 du 1er juillet 2009 concernant les intégrateurs dans le secteur public, www.privacycommission.be

²⁰ À titre d'exemple :

- article 2, 2°, articles 3 et 4 du décret flamand du 18 juillet 2008 *relatif à l'échange électronique de données administratives* ;
- article 3, § 1^{er}, (b), deuxième alinéa de l'accord de coopération du 28 septembre 2006 qui reconnaît le principe de la collecte unique et de la réutilisation maximale des données en utilisant des sources authentiques de données (Accord de coopération entre l'État fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Commission communautaire française et la Commission communautaire commune *concernant les principes pour un e-gouvernement intégré et la construction, l'utilisation et la gestion de développements et de services d'un e-gouvernement intégré* (M.B. 19/10/2006).

²¹ Point 13 et sv., recommandation d'initiative n° 09/2012 du 23 mai 2012, op. cit.

reprises que les traitements de données se feront conformément à la loi vie privée. On peut dès lors en déduire que le principe de proportionnalité sera garanti.

33. La Commission estime par ailleurs que **l'exactitude des données** contenues dans une source authentique est fondamentale. Si la source authentique contient des données inexactes, ces dernières seront rapidement diffusées et "contamineront" toutes sortes de traitements de données dans le secteur public. Ce phénomène est également appelé "diffusion de la pollution"²². À cet égard, une mise à jour continue est nécessaire. Toutefois, la Commission rappelle qu'une donnée n'est exacte que dans un contexte de collecte ou d'utilisation spécifique et qu'il convient alors que le cadastre (inventaire) des données mises à disposition informe aussi sur ce contexte conditionnant l'exactitude des données²³.

34. Afin d'assurer la qualité des données, l'avant-projet d'ordonnance prévoit :

- à l'article 5, § 3, al. 1^{er} que « *les services publics participants qui sont autorisés à consulter des données authentiques via l'intégrateur de services régional ne peuvent plus réclamer directement ces données à d'autres services publics participants ou à des citoyens, entreprises, organismes ou institutions* »;
- à l'article 5, § 3, al. 2 une obligation d'utilisation stipulant que « *dès qu'une donnée est accessible par le biais de l'intégrateur de services, les services publics participants sont obligés de passer par lui pour une telle utilisation sauf exception fixée par ou en vertu d'une loi ou d'un arrêté* ». Ce qui constitue une garantie d'une bonne qualité de données ;
- à l'article 7, § 1^{er} que « *le service public participant gestionnaire de sources authentiques ou de banque de données issues de sources authentiques assure à tout moment, entre autres, la qualité des données ainsi que leur sécurité, tant au niveau technique qu'organisationnel, nécessaires au respect de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* » ;
- la tenue d'un historique des données, pour autant que cela soit nécessaire eu égard aux finalités avancées (art. 7, § 1^{er}) ;
- une obligation pour l'utilisateur qui a un doute fondé sur l'exactitude des données qu'il a réclamées auprès d'une source authentique de signaler l'inexactitude constatée (art. 7, §2) ;
- à l'article 21, § 1^{er}, le droit pour toute personne d'obtenir sans frais la rectification de toute donnée inexacte qui la concerne.

²² G. Overkleeft-Verburg, "Basisregistraties en rechtsbescherming. Over de dualisering van de bestuurlijke rechtsbetrekking", Nederlands Tijdschrift voor Bestuursrecht 2009, p. 80

²³ À titre d'exemple, certains traitements nécessitent la connaissance de la composition de famille au 1er janvier de l'année. Cette donnée est à conserver sans être mise à jour, même si la composition de famille change en cours d'année.

35. La Commission regrette toutefois que la mise en place d'un principe de labélisation afin de garantir la qualité des sources authentiques ne soit pas prévu dans l'avant-projet d'ordonnance.²⁴
36. Par ailleurs, la Commission conseille d'effectuer des "cross-controls" (croisement avec d'autres banques de données) afin de détecter les erreurs éventuelles²⁵. Il s'agit bien de vérifier l'exactitude de données considérées individuellement et non le rapprochement de fichiers.
37. La Commission prend acte qu'un droit d'accès électronique par la personne concernée est prévu à l'article 6 de l'avant-projet d'ordonnance et ce, sans préjudice des articles 10 et 12 LVP.
38. Par ailleurs, la Commission rappelle que lorsqu'une décision administrative est prise à l'égard d'un citoyen, l'instance qui la prend doit toujours indiquer à la personne concernée sur quelles données elle s'est basée, où celles-ci ont été réclamées et auprès de qui le citoyen peut exercer ses droits. De cette manière, le citoyen a encore la possibilité, le cas échéant, de prouver que certaines données ne sont pas (plus) correctes²⁶.
39. La Commission rappelle également l'article 12^{bis} de la LVP, sur la base duquel « *une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut en principe être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité* »²⁷.
40. L'article 9 de l'avant-projet d'ordonnance précise que l'intégrateur de services régional « *promeut une politique de **sécurité** coordonnée pour le réseau* ». La Commission se doit de souligner l'importance d'une politique de sécurité de l'information adéquate pour chaque source authentique, ceci sans préjudice des responsabilités propres à chaque acteur du réseau. À cet égard, elle renvoie tout d'abord à l'article 16 LVP ainsi qu'à ses « *Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel* »²⁸. Ensuite, elle attire l'attention sur sa recommandation n° 01/2008 du 24

²⁴ Voy. n° 29/2012 du 12 septembre 2012 point 57, *op. cit.*

²⁵ Voy. la recommandation d'initiative n° 09/2012 du 23 mai 2012, *op. cit.* (point 10)

²⁶ Recommandation n° 09/2012 du 23 mai 2012, *op. cit.*

²⁷ La personne concernée doit pouvoir communiquer son point de vue avant qu'une décision définitive ne soit prise.

²⁸ Accessibles à l'adresse suivante :

http://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel.pdf

septembre 2008 relative à la gestion des accès et des utilisateurs dans le secteur public et sur le principe des « cercles de confiance » exposé aux points 13-15 de sa recommandation n° 03/2009 du 1^{er} juillet 2009 concernant les intégrateurs dans le secteur public. Enfin, la Commission attire l'attention sur sa Recommandation d'initiative n° 01/2013 du 21 janvier 2013 relative aux mesures de sécurité à respecter afin de prévenir les fuites de données²⁹

41. La Commission prend également acte du fait que l'intégrateur de service régional et chaque service participant désignera un conseiller en sécurité.
42. La Commission insiste enfin sur le fait qu'une source authentique doit définir des responsabilités claires à tous niveaux (exactitude des données, sécurité, transparence, délais de conservation, etc.). À cet effet, il faut élaborer les procédures et les Service Level Agreements³⁰ nécessaires et intégrer des mécanismes de contrôle afin de vérifier si les procédures mises en place sont respectées.
43. La source authentique doit ainsi remplir à chacune des phases (collecte, validation ; gestion; mise à disposition) un rôle actif et de coordination, et ce également pour les (aspects des) phases pour lesquelles elle n'est pas elle-même directement ou complètement responsable.³¹

B.2. L'intégrateur de services régional

44. L'article 8 de l'avant-projet d'ordonnance désigne le Centre informatique pour la Région Bruxelloise (CIRB)³² comme intégrateur de services régional.
45. Il est déduit de l'exposé des motifs et du commentaire des articles que l'intégrateur de services régional a pour **but de simplifier et d'optimiser les échanges de données entre les différents acteurs publics** (services publics participants et autres intégrateurs de services), en mettant particulièrement l'accent sur l'utilisation des données authentiques dans le réseau. À cette fin, il assurera surtout **un rôle d'intégrateur de services, mais aussi de tiers de confiance.**

²⁹ Accessible à l'adresse suivante : http://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2013_0.pdf

³⁰ Voy. à ce sujet : la Recommandation n°09/2012, *op.cit.*

³¹ Recommandation n° 09/2012 du 23 mai 2012, *op. cit.*

³² Ordonnance du 20 mai 1999 portant sur la réorganisation du Centre d'informatique pour la Région bruxelloise, *M.B.*, 29 juillet 1999

46. Le champ d'application de l'intégrateur de services régional comprend « *tous les services décentralisés personnalisés, les établissements publics, les entreprises publiques, les organes et les personnes morales de droit public, qui ont été créés par ou qui dépendent de la Région de Bruxelles-Capitale, les intercommunales de la Région de Bruxelles-Capitale* » (article 3, §1^{er}, al. 2 de l'avant-projet d'ordonnance).
47. Cette délimitation ne pouvant bien évidemment pas porter préjudice à la répartition des compétences fixée dans la loi spéciale de réformes institutionnelles du 8 août 1980³³, il est très justement précisé à l'alinéa 3 de l'article 8 de l'avant-projet d'ordonnance que **l'intégrateur de services régional intervient « par défaut, et sans préjudice à une réglementation qui imposerait le recours à un autre intégrateur de services ».**
48. S'il est fondamental de rappeler que l'intégrateur de service intervient « *par défaut, et sans préjudice à une réglementation qui imposerait le recours à un autre intégrateur de services*», la Commission estime qu'il n'est pas nécessaire de préciser son champ d'application au risque de ne pas pouvoir viser l'ensemble des situations variées dans lesquelles il est susceptible d'intervenir. En effet, le « champ d'application » de l'intégrateur de service doit se déduire des missions et compétences qui sont les siennes. Au même titre, la Commission suggère d'abandonner la référence à un réseau dont l'étendue et le déroulement paraissent difficilement maîtrisables.
49. Cependant et vu le contexte juridique complexe, certains domaines de compétences de différents intégrateurs de services dans le secteur public vont inévitablement s'effleurer, voire même se chevaucher sur certains points³⁴.
50. C'est pourquoi la Commission juge utile de rappeler que dans une telle situation, la pratique administrative idoine est de toujours veiller que les données puissent être mises à disposition des utilisateurs (fonctionnaires, citoyens, ...) de manière intégrée. Un intégrateur de services a en effet essentiellement pour but d'offrir à ses clients, en l'occurrence les services publics, des services intégrés afin que chaque client ne doive pas lui-même intégrer des services provenant de différents fournisseurs de services. Il est évident que tant du point de vue de l'efficacité que du point de vue de la sécurité de l'information, **la Commission recommande³⁵ qu'un service public ne doive recourir qu'à un seul intégrateur de services.** De cette manière, le client n'est confronté qu'à un seul système

³³ loi spéciale du 8 août 1980 de réforme institutionnelles, *M.B.*, 15 août 1980

³⁴ Voy. point 52 de la Recommandation n°03/2009, *op. cit.*

³⁵ La Commission constate que la création de différents intégrateurs de services va inmanquablement créer des problèmes de coordination. La Commission adoptera une recommandation à ce sujet afin de garantir la sécurité de l'information et le respect de la vie privée.

de gestion des utilisateurs et des accès, un seul ensemble de spécifications techniques, etc.³⁶

51. La Commission plaide dès lors pour que les intégrateurs de services concluent les accords nécessaires afin que des clients ayant recours à un intégrateur de services déterminé puissent être servis par des fournisseurs de services associés à un autre intégrateur de services. Cela éviterait en outre de nombreuses discussions inutiles concernant la répartition des tâches entre intégrateurs de services et on pourrait consacrer de façon optimale l'énergie à un bon service aux clients et à leurs utilisateurs, c'est-à-dire les citoyens et les entreprises, notamment dans le cadre des cercles de confiance³⁷.
52. Dans un même temps, la Commission rappelle que le principe, pour chaque service public, de ne recourir qu'à un seul intégrateur de services ne porte pas préjudice aux répartitions légales de compétences entre services ou niveaux publics. Étant donné ce contexte juridique complexe, il ne sera pas toujours évident, dans la pratique, de demander aux services publics de ne recourir qu'à un seul intégrateur de services. Pour de tels cas, la Commission propose les solutions suivantes :
- on pourrait opter pour **reprendre dans l'administration des intégrateurs fédéraux aussi bien des représentants du niveau fédéral que du niveau régional**. Du point de vue de l'efficacité et de la sécurité, une telle approche est recommandée plutôt que le recours d'un service public à plusieurs intégrateurs de services ;
 - si toutefois, il y avait quand même un recours à plusieurs intégrateurs – ce qui, comme précisé, ne recueille pas la préférence de la Commission- on peut, selon la nature du projet d'intégration à réaliser, **concevoir une collaboration *ad hoc* entre l'intégrateur de services régional et les autres intégrateurs de services** où seul un de ces intégrateurs peut intervenir, ou encore mettre en place une collaboration entre un de ces intégrateurs et d'autres instances (locales), toujours en respectant le principe des "**cercles de confiance**".³⁸
53. L'article 9 de l'avant-projet d'ordonnance définit les missions de intégrateur de services régional en s'inspirant de l'article 2^{bis} de la loi banque-carrefour de la sécurité sociale³⁹ et de

³⁶ Voy. point 29 de l'Avis n° 18/2011 du 7 septembre 2011 concernant l'avant-projet de décret relatif à l'institution et à l'organisation d'un intégrateur de services flamand

³⁷ Voy. point 31 de l'Avis n° 18/2011, *op.cit.* ; Recommandation n°02/2010 du 31 mars 2010 concernant le rôle de protection de la vie privée des Trusted Third Parties (TTP ou tiers de confiance) lors de l'échange de données, *op. cit.*

³⁸ Ces solutions ont également été proposées à la Région Flamande (point 32 de l'Avis n° 18/2011, *op. cit.*) et à la Région wallonne et la Communauté française (point 85 de l'Avis n° 29/2012, *op. cit.*)

³⁹ loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque-carrefour de la sécurité sociale, *M.B.*, 22 février 1990

l'article 4 du décret du 13 juillet 2012 portant création et organisation d'un intégrateur de services flamand⁴⁰.

54. Ainsi, les missions suivantes sont prévues :

- l'élaboration des modes de contrôle technique et organisationnel des droits d'accès aux banques de données ainsi que la banque de règles⁴¹ ;
- la promotion et la surveillance de l'homogénéité des droits d'accès aux banques de données ;
- l'élaboration des modalités techniques visant à développer les canaux d'accès de la manière la plus efficace et la plus fiable possible ;
- l'élaboration, selon les normes, des standards techniques et fonctionnels, de l'architecture de base et des modalités techniques relatives à la communication entre les banques de données ou les sources authentiques;
- la promotion d'une politique de sécurité coordonnée pour le réseau ;
- l'organisation de la collaboration avec les autres intégrateurs de service ;
- la création et la gestion d'un répertoire de références et d'une banque de règles qui stipule qui a accès, à quelles conditions et pour quelles données déterminées.

55. Concernant cette toute dernière mission, la Commission constate que l'avant-projet d'ordonnance prévoit que l'intégrateur de services arrête :

- a) qui effectue quels authentications, vérifications et contrôles, à l'aide de quels moyens, et qui en assume la responsabilité;
- b) la manière dont les résultats des authentications, les vérifications et les contrôles exécutés font l'objet d'un échange et d'une conservation électroniques sécurisés entre les parties concernées;
- c) qui tient à jour des loggings déterminés.

56. Les articles 14 à 20 organisent le fonctionnement de l'intégrateur de services régional.

57. La Commission prend acte que lors de l'intégration de services, l'intégrateur de services régional doit respecter les éventuelles autorisations qui accordent à un utilisateur un accès à des données à caractère personnel. La Commission se permet de préciser qu'une autorisation définit aussi bien les finalités pour lesquelles elle est accordée que les données auxquelles l'instance habilitée peut accéder.⁴²

⁴⁰ M.B., 1 août 2012

⁴¹ « ensemble des règles fixant pour la banque de données ou la source authentique, les conditions de consultation ou de communication des données, créée et gérée par l'intégrateur de services » art. 2, al. 1, 9° de l'avant-projet d'ordonnance

⁴² avis n° 29/2012 du 12 septembre 2012, *op.cit.*

58. Enfin, l'article 10 de l'avant-projet d'ordonnance stipule que « *pour le traitement des données en application de la présente ordonnance et de ses arrêtés d'exécution, [le numéro d'identification du Registre national sera utilisé]...»*.
59. Dans un souci de conformité à la loi, la Commission attire l'attention sur le fait que cela n'est possible que dans la mesure où toutes les parties concernées ont été dûment autorisées à cet effet par le Comité sectoriel du Registre national⁴³.

B.3. Comité de coordination

60. L'article 26 de l'avant-projet d'ordonnance prévoit la création d'un comité de coordination constitué des représentants des services publics participants parmi les fonctions dirigeantes et des fonctionnaires dirigeants de l'intégrateur de services régional et du représentant du service compétent pour la simplification administrative.
61. L'article 29 de l'avant-projet d'ordonnance énumère les missions du comité de coordination.
62. À ce sujet, la Commission attire l'attention sur le risque qui consisterait à doter ce comité de pouvoirs contraignants. Ces compétences importantes doivent être confiées à la commission de contrôle bruxelloise dont les décisions devraient être précédées d'une consultation du comité de coordination ou même formées sur la base de propositions de ce dernier.

B.4. Protection des données

B.4.1. Principe général de l'autorisation pour toutes communications de données à l'intervention ou non de l'intégrateur de service

63. Ce principe général est prévu par l'article 12 de l'avant-projet d'ordonnance qui prévoit en effet que « *toute communication à caractère personnel par l'intégrateur de services régional ou à l'intégrateur de services régional requiert une autorisation préalable, à moins que cette communication électronique ne soit autorisée ou soit exemptée d'autorisation par ou en vertu d'une disposition légale,»*.

B.4.2. Obligation de confidentialité

⁴³ Art. 5 loi du 8 août 1983 organisant un registre national des personnes physiques, *M.B.*, 21 avril 1984

64. La Commission constate que cette obligation de confidentialité (secret professionnel) est bel et bien instaurée par l'article 22 de l'avant-projet d'ordonnance.

B.4.3. Conseiller en sécurité de l'information

65. Le conseiller en sécurité de l'information se doit d'être l'instigateur et le moteur de la politique de sécurité de l'information. C'est à lui qu'est confiée la mise en œuvre de la politique de sécurité. C'est donc lui qui fait des propositions, qui fixent les objectifs à atteindre, qui suit et conseille les différentes personnes qui interviennent lors de la mise en place du système de sécurisation. Il analyse et étudie les incidents de sécurité et propose des mesures d'amélioration. Il s'assure encore que personne n'est confronté à des intérêts contradictoires et il endosse la fonction de principal interlocuteur dans toutes les questions qui concernent la sécurité. Il rapporte directement à la direction et bénéficie de moyens suffisants, tant en argent, qu'en personnel ou en matériel et équipement, pour pouvoir exécuter correctement sa mission.
66. La Commission estime également que toute instance qui gère une source authentique de données contenant des données à caractère personnel, toute instance qui reçoit ou échange des données à caractère personnel électroniques, et toute entité qui traite des données à caractère personnel doit désigner un conseiller en sécurité.
67. La Commission constate que l'obligation de désigner un conseiller en sécurité de l'information est prévue à l'article 24 de l'avant-projet d'ordonnance.

B.4.4. La Commission de contrôle bruxelloise

68. À la lecture du considérant B.21 de l'arrêt n° 15/2008 du 14 février 2008 de la Cour constitutionnelle et au regard des compétences implicites visées à l'article 10 de la loi spéciale⁴⁴, la **compétence des Régions et Communautés** d'installer une autorité de contrôle de l'échange des données au sein de leur propre administration ne fait aucun doute.
69. La Commission prend acte que l'article 31 crée auprès du Parlement de la Région de Bruxelles-Capitale une commission de contrôle bruxelloise indépendante pour l'échange électronique de données de sources authentiques régionales de données et de banques de données issues de sources authentiques régionales mais également, pour le traitement et

⁴⁴ *op. cit.*

l'échange d'images dans le cadre de la mutualisation des services régionaux, notamment, en matière de vidéosurveillance et ce, sans préjudice aux compétences de la Commission de la protection de la vie privée en la matière.

70. Les articles relatifs à la composition de la commission de contrôle bruxelloise semblent avoir largement été inspirés du Décret flamand du 18 juillet 2008 relatif à l'échange électronique de données administratives.
71. La commission de contrôle bruxelloise *« se compose de six membres effectifs et six membres suppléants. La durée de leur mandat est de cinq ans et est renouvelable. Après concertation avec la Commission de la protection de la vie privée, le Parlement de la Région de Bruxelles-Capitale désigne parmi les membres effectifs et suppléants de cette commission, trois membres de la commission de contrôle bruxelloise, dont le président, le vice-président, ainsi qu'un suppléant pour chacun d'eux. Les trois autres membres de la commission de contrôle sont respectivement un juriste, un informaticien et une personne pouvant justifier d'une expérience professionnelle dans la gestion de données à caractère personnel. Ils sont désignés par le Parlement de la Région de Bruxelles-Capitale, qui nomme aussi un suppléant pour chacun d'eux. Le président et le vice-président de la commission de contrôle appartiennent à des rôles linguistiques différents. Un tiers (1/3) des membres de la commission de contrôle appartient au groupe linguistique le moins important »*.
72. La Commission estime qu'il serait nécessaire de préciser que la répartition linguistique des membres prévue est également applicable aux membres issus de la Commission et aux membres désignés par le Parlement de la Région de Bruxelles-Capitale. Cela permettrait de garantir le même équilibre linguistique entre les membres issus de la Commission et ceux désignés par le Parlement de la Région de Bruxelles-Capitale.
73. Les articles 32 et suivants de l'avant-projet d'ordonnance donnent à la commission de contrôle bruxelloise une **compétence d'avis, de recommandation, d'autorisation et d'investigation**.
74. La Commission constate également qu'il est prévu à l'article 32, § 3 de l'avant-projet que la commission de contrôle bruxelloise peut différer un avis, une recommandation ou une autorisation à l'avis préalable de la Commission de la protection de la vie privée à la demande de son président.

75. La Commission prend enfin acte du fait que la sanction consistant à mettre fin au flux de données lorsque le bénéficiaire d'une autorisation ne remplit pas ses obligations (retrait d'une autorisation) est prévue à l'article 37.

PAR CES MOTIFS,

La Commission

émet un avis favorable sur l'avant-projet **à condition de** prendre en compte les différentes remarques formulées dans le présent avis.

l'Administrateur f.f.,

Le Vice-Président,

(Sé.) Patrick Van Wouwe

(Sé.) Stefan Verschuere