Recommandation n° 03/2009 du 1er juillet 2009

Objet : recommandation d'initiative concernant les intégrateurs dans le secteur public (A/2007/043)

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 la "LVP"), en particulier l'article 31 ;

Vu les avis n° 01/2008 et 41/2008 que la Commission a émis concernant respectivement le projet de décret relatif à l'échange électronique de données administratives et l'avant-projet de loi relative à l'institution et à l'organisation d'un Intégrateur de Services fédéral ;

Vu le rapport du Président ;

Émet, le 1er juillet 2009, la recommandation suivante :

I. OBJET DE LA RECOMMANDATION

1. Le mot intégration est un terme générique. Utilisé dans le cadre du traitement de données à caractère personnel, ce terme peut couvrir des significations divergentes dont les conséquences pour la vie privée varient fortement.

2. Ainsi, la Commission distingue les formes suivantes d'intégration :

- l'intégration de données à caractère personnel : l'agrégation de données à caractère personnel provenant de plusieurs sources authentiques et leur enregistrement dans une banque de données intégrées distincte, en vue de leur communication à des tiers ;

- l'intégration de services : l'harmonisation de services électroniques partiels en un ensemble cohérent de services électroniques en vue de le proposer à des tiers ;

- l'intégration d'infrastructure : la simple utilisation d'une infrastructure commune pour des traitements de données à caractère personnel sans aucune forme d'intégration de données à caractère personnel ou d'intégration de services (par exemple l'utilisation commune de serveurs, de lignes, de logiciels) ;

- l'intégration de présentation : un simple accès intégré à des données à caractère personnel ou à des services via un seul point de contact électronique, sans aucune forme d'intégration de données à caractère personnel ou d'intégration de services (par exemple un portail, un téléphone vert).

3. Cette recommandation traite de l'intégration de services et de l'intégration de données à caractère personnel (ci-après intégration de données) dans le secteur public. Leur impact sur le traitement de données à caractère personnel est en effet celui qui risque le plus de menacer la vie privée.

4. Ces formes d'intégration seront confrontées ci-après aux principes de la LVP – loyauté, licéité et finalité, proportionnalité, exactitude et précision, transparence, sécurité, droits de la personne concernée, obligation de déclaration – en vue de fixer un certain nombre de règles pratiques qui doivent être respectées dans ce cadre. En tout cas, on espère que les instances chargées d'une intégration de services ou de données à caractère personnel dans le secteur public disposent

toujours d'une réglementation légale explicite en la matière qui réponde aux dispositions de la présente recommandation.

II. INTÉGRATION DE SERVICES OU INTÉGRATION DE DONNÉES ?

5. Lorsque plusieurs alternatives offrant un niveau d'efficacité similaire existent concernant le traitement de données à caractère personnel, il faut opter pour celle qui est la moins menaçante pour la vie privée.

6. Si, pour l'exécution de certaines tâches, il est nécessaire de disposer de données provenant de plusieurs sources, la mise à disposition de ces données au moyen d'une intégration de services constitue dans la plupart des cas une option moins menaçante pour la vie privée qu'au moyen d'une intégration de données à caractère personnel.

7. Dans le cas d'une intégration de services, les données ne sont agrégées que temporairement, à savoir au moment de l'offre du service intégré (concrètement : au moment où l'on interpelle le service concernant une personne déterminée ou un groupe de personnes déterminé). Un tel service n'exige pas l'agrégation permanente de données, ni leur enregistrement intégré à plus long terme. Généralement, les données sont directement obtenues auprès de différentes banques de données fiables, sous la responsabilité d'une entité déterminée, ce qu'on appelle des sources authentiques.

8. Un avantage incontestable d'une telle méthode réside dans le fait que l'on évite la circulation inutile de copies de fichiers de données dans lesquels sont enregistrées des données à caractère personnel qui ne sont pas ou pas régulièrement mises à jour et qui, par conséquent, contiennent des informations dépassées – donc des erreurs –, ce qui doit être évité à la lumière de l'article 4, § 1, 4° de la LVP. Cela réduit en outre le risque d'un accès illégitime aux données à caractère personnel étant donné que celles-ci ne sont pas reprises inutilement en plusieurs copies à plusieurs endroits.

9. Celui qui propose une intégration de services interviendra souvent en tant que "trusted third party" (ci-après TTP, tiers de confiance). Une TTP est "*an entity trusted by multiple other entities within a specific context and which is alien to their internal relationship*"[1]. Une TTP est donc une entité indépendante de confiance qui offre des services qui accroissent la fiabilité de l'échange électronique de données et de l'enregistrement de données et qui n'a elle-même aucune mission ou aucun intérêt en matière de traitement réel de fond de données à caractère personnel intégrées.

[1] P. 16 du "Consultation paper" du 23/11/2005 "on Common Terminological Framework for Interoperable Electronic Identity Management".

Sa raison d'être doit être l'agrégation temporaire de données au profit de tiers en veillant à ce que tant la LVP que les éventuelles autorisations des comités sectoriels compétents soient respectées. Par exemple, lorsqu'une autorisation prescrit que seul un résultat peut être communiqué à l'instance habilitée - comme un revenu supérieur ou inférieur à un certain montant – mais pas les données en elles-mêmes, la TTP se chargera du calcul éventuel et transmettra le résultat.

10. Dans le cas d'une intégration de données, une nouvelle banque de données est créée, dans laquelle sont agrégées et conservées de manière permanente des informations provenant de plusieurs sources. Il s'agit donc d'une concentration d'informations à un seul endroit. En dépit du fait que cela puisse être justifié à la lumière de la finalité pour laquelle ces données ont été agrégées, il est évident qu'un incident de sécurité concernant une telle banque de données aura un impact bien plus important sur la vie privée qu'un incident concernant une des sources d'où les données ont été tirées.

11. Du point de vue de la LVP, une intégration de services est dès lors préférable à une intégration de données. Cette dernière n'est acceptable que si elle est nécessaire **et** si la fonctionnalité souhaitée ne peut pas être réalisée avec une efficacité équivalente au moyen d'une intégration de services. Concrètement, cela signifie qu'une intégration de données n'est permise que dans la mesure où le responsable du traitement dispose soit d'une base légale, soit d'un intérêt légitime qui ne peut raisonnablement pas être réalisé avec une efficacité équivalente via une intégration de services. Le terme "raisonnablement" suppose une pondération de toutes les facettes du processus : ce qui est nécessaire, qui a quoi, ce qui peut être fourni et sous quelle forme, ce qui est techniquement possible, quels sont les risques en matière de sécurité, quelles sont les implications budgétaires, … , donc, en fait, un contrôle par rapport notamment aux articles 4, 5 et 16, § 4 de la LVP.

12. Le fait qu'une intégration de services ne soit pas une option à un moment donné et donc que l'on procède à une intégration de données n'exclut pas qu'une intégration de services devienne réalisable à un moment donné et que la méthode doive être adaptée en conséquence. À la lumière de cet élément, il est dès lors recommandé qu'en cas d'intégration de données, l'on évalue périodiquement si celle-ci est encore justifiée compte tenu de l'évolution des paramètres sous-jacents.

III. CERCLES DE CONFIANCE

13. Comme déjà indiqué ci-dessus, il faut veiller à ce qu'aucune menace pour la protection de la vie privée ne survienne en raison de l'agrégation ou de la copie inutile de données à caractère personnel.

14. En ayant recours à un système coordonné et modulaire de gestion des utilisateurs, des accès et des loggings avec un enregistrement décentralisé des données, grâce auquel plusieurs parties peuvent profiter des modules de gestion des accès électroniques, des sources authentiques et des systèmes de logging de chacune, ce principe peut être garanti au maximum en ce qui concerne la consultation de banques de données. C'en est fini des multiples contrôles identiques et enregistrements des loggings.

15. Un tel accord de coopération est souvent défini en tant que "cercles de confiance". Ceux-ci sont réalisés au moyen d'une répartition des tâches entre les instances concernées qui concluent des accords clairs sur :

- qui effectue quelles authentifications, quelles vérifications et quels contrôles à l'aide de quels moyens et qui en est responsable ;
- la manière dont les résultats des authentifications, vérifications et contrôles effectués sont échangés de manière sûre par voie électronique entre les instances concernées ;
- qui tient à jour quels loggings ;
- la manière dont on veille à ce que puisse avoir lieu, lors d'un examen effectué à l'initiative d'un organe de contrôle ou à l'occasion d'une plainte, un traçage complet de la personne physique qui a utilisé quel service ou quelle transaction concernant quel citoyen ou quelle entreprise, quand, via quel canal et pour quelles finalités.

IV. INTÉGRATION DE SERVICES ET LVP

4.1. Loyauté, licéité et finalité

16. La Commission précise que le traitement de données au moyen d'une intégration de services dans le secteur public n'est permis que lorsqu'il a lieu dans un ou plusieurs cas repris à l'article 5, premier alinéa de la LVP.

17. Travailler via un intégrateur de services peut avoir une incidence positive sur la protection de la vie privée. Si ce service est bien organisé, les utilisateurs n'ont pas ou peu de marge pour éventuellement abuser de l'autorisation qui leur octroie par exemple un accès à une source authentique de données. Travailler avec des répertoires de référence (voir point 25) peut contribuer à éviter des consultations illicites.

18. Vu son impact, l'intégration de services doit être considérée comme une finalité distincte et pas simplement comme la dérivée d'une autre finalité ou inhérente à celle-ci. La finalité "intégration de services" est en effet le critère à l'aide duquel tous les aspects de ce processus d'intégration doivent être évalués, notamment en ce qui concerne leur lien avec la finalité, leur proportionnalité, leur sécurité. Ce contrôle exige que la finalité "intégration de services" soit clairement définie et délimitée (déterminée). Le domaine couvert par l'intégrateur de services constitue dans ce contexte un facteur non négligeable. Lorsque par exemple des données sensibles (articles 6 à 9) sont filtrées, il faudra vérifier si les conditions connexes spécifiques sont remplies à cet effet.

19. La plus-value de l'intégration de services est proportionnelle aux services qu'elle englobe de manière à ce qu'ils ne doivent pas être interpellés séparément. Il faut donc savoir quels services sont inclus comme par exemple l'accès à quelle source authentique de données, à quelle sorte de transactions, etc. Une communication claire à cet égard par l'intégrateur de services est donc indispensable.

20. En outre, l'offre du service intégré suppose que les différents processus partiels soient harmonisés. Leur coordination (= orchestration) implique la conclusion d'accords précis sur l'exécution des diverses tâches comme par exemple le temps de traitement consenti d'une demande, la transmission en temps utile d'informations sur l'état de la demande, etc. Ces accords sont concrétisés dans les *service level agreements* que l'intégrateur de services conclut à ce sujet. Ce sont des accords entre le(s) prestataire(s) de certains services et l'utilisateur ou les utilisateurs de ces services ; ces accords définissent les services à fournir et leur niveau de qualité ainsi que les droits et obligations des deux parties à cet égard.

21. Pour le citoyen, une intégration de services ne sera pas toujours transparente. Il est donc primordial que l'intégrateur de services indique clairement qui est le responsable du traitement, où il est possible d'exercer ses droit d'accès, de rectification et de suppression (plus de détails sont disponibles à la rubrique 4.6., point 41 et suivants). Il faut à tout prix éviter que le citoyen soit découragé d'exercer ses droits parce qu'il lui est impossible d'identifier le(s) bon(s) interlocuteur(s).

4.2. Proportionnalité

22. Le champ d'action d'un intégrateur de services doit être clairement délimité et être suffisamment homogène afin qu'un utilisateur potentiel dispose d'un interlocuteur clair pour un domaine spécifique et qu'une application univoque de normes et de mesures de sécurité et de protection de la vie privée soit garantie (voir également point 34).

23. Une intégration de services vise à ne plus enregistrer de données à caractère personnel ou à ne pas les enregistrer plus longtemps que cela est nécessaire à la fourniture de services intégrés ou à d'autres finalités qui y sont liées, par exemple la reconstitution d'une transaction en cas de plainte. Ce principe s'applique aussi bien aux données à caractère personnel fournies qu'aux données à caractère personnel nécessaires à cette reconstitution.

24. Concrètement, cela signifie que l'on a recours à une série de sources authentiques qui sont mises en relation de manière conviviale pour l'utilisateur, de manière à obtenir des avantages équivalents à ceux d'un enregistrement de données centralisé sans que celui-ci ait effectivement lieu.

25. Une intégration de services peut parfois être utilement soutenue par la gestion d'un répertoire de référence. Un tel répertoire peut constituer la base de l'organisation de l'échange électronique de données et peut se composer de tableaux reliés entre eux, dont :

- un tableau de services et d'informations disponibles qui mentionne quels services ou quelles informations sont disponibles auprès d'un acteur concernant les différentes sortes de dossiers (le tableau "quoi-où") ;

- un tableau d'utilisateurs et d'applications ayant reçu un accès qui contient une liste des utilisateurs et des applications auxquels un accès peut être accordé mais également les instruments et règles d'authentification ainsi que les profils d'accès[2] (le tableau "qui reçoit quoi") ;

- un répertoire de personnes qui indique quelles personnes, en quelle qualité, possèdent des dossiers auprès de quels acteurs concernant quelles périodes (le tableau "qui-où-comment-quand") ;

[2] Le profil d'accès détermine à quelle sorte d'information ou de service on peut recourir et pendant quelle période, en fonction de la qualité sous laquelle une personne ou une entreprise est enregistrée.

- un tableau d'inscription qui mentionne quels utilisateurs et applications souhaitent obtenir quels services automatiques dans quels cas, pour quelles personnes et en quelle qualité.

26. Ce répertoire de référence peut être élaboré en tenant compte des principes des cercles de confiance mentionnés au point 15, de manière à ce que certaines parties puissent être décentralisées, en particulier lorsqu'on peut déduire des données qui y sont reprises des informations qui sont spécialement protégées par ou en vertu de la LVP.

27. L'intégrateur de services ne peut traiter que des données à caractère personnel qui sont pertinentes et non excessives pour les utilisateurs du service intégré (application de l'article 4 de la LVP). Cela signifie que :

- aucune donnée à laquelle les utilisateurs ne peuvent accéder ne peut leur être transmise, compte tenu aussi bien des modalités des éventuelles autorisations que des finalités ;

- l'intégrateur de services lui-même ne peut collecter que les données à caractère personnel qui sont nécessaires pour pouvoir fournir aux utilisateurs leurs informations et effectuer un audit complet.

28. Lors de l'intégration de services, l'intégrateur de services doit respecter les éventuelles autorisations qui accordent à un utilisateur un accès à des données à caractère personnel. Une autorisation définit aussi bien les finalités pour lesquelles elle est accordée que les données auxquelles l'instance habilitée peut accéder. Elle peut également encore contenir d'autres modalités :

> *Par exemple* : il peut être pertinent pour un utilisateur de savoir si le revenu d'une personne est ou non supérieur à un certain montant. Il n'a toutefois pas besoin de connaître le montant exact pour pouvoir réaliser ses finalités. Dans ce cas, l'autorisation stipulera généralement que seule une réponse de type oui/non peut lui être communiquée. L'intégrateur de services devra veiller à ce que seule la réponse soit transmise à l'utilisateur, pas les données sous-jacentes.

29. Ignorer des autorisations expose aussi bien l'intégrateur de services que l'utilisateur à des sanctions (article 39 de la LVP). L'intégrateur de services doit donc prendre des mesures afin d'empêcher cela. Si une autorisation a été délivrée, l'intégrateur de services sait clairement ce qui doit être garanti. C'est moins évident lorsque des données peuvent être réclamées auprès de tiers pour lesquelles aucune exigence d'autorisation n'est d'application. Dans ce cas, l'intégrateur de services devra vérifier si les données demandées sont pertinentes et non excessives en vue de la

finalité pour laquelle un utilisateur fait appel à ses services. L'absence d'une autorisation ne dispense pas l'intégrateur de services de l'obligation de respecter les articles de la LVP.

4.3. Exactitude et précision

30. L'intégration de services permet de mettre à disposition de l'utilisateur de ces services un certain nombre de données, généralement après un contrôle préalable de la finalité (déterminée, explicite et légitime) et de la proportionnalité des données par un comité sectoriel ou comparable.

31. Sur la base de ces données, cet utilisateur prend des décisions ou entreprend des actions à l'égard de personnes déterminées. Dans ce cadre, il importe, aussi bien pour l'utilisateur que pour les personnes concernées, que les données sur la base desquelles on agit soient correctes. Des données erronées peuvent conduire à ce qu'une personne concernée voie un de ses droits ignoré tandis que l'utilisateur sera confronté de son côté à des contestations de ses décisions qui auraient pu être évitées (frais, travail supplémentaire).

32. Actuellement, en application de l'article 4, § 1, 4° de la LVP, chaque responsable du traitement est en tout cas obligé de veiller à ce que les données traitées soient exactes. L'intégrateur de services doit développer des systèmes dans lesquels l'information du fait qu'une donnée déterminée est inexacte est immédiatement transmise au fournisseur de la donnée afin que ce dernier puisse immédiatement faire le nécessaire pour la rectifier. Cela n'empêche pas de recommander que l'intégrateur de services conclue préalablement à cet égard des accords clairs avec les fournisseurs des services partiels dans un *service level agreement*. Vis-à-vis des utilisateurs, cela présente l'avantage qu'ils peuvent être informés de manière précise quant à la qualité des données et des services fournis de manière à pouvoir faire une évaluation des conséquences de l'intégration de services pour leurs activités.

4.4. Transparence

33. Il est recommandé que l'intégrateur de services publie des informations claires concernant toutes les facettes de son fonctionnement, de manière à ce que chacun ait la possibilité de vérifier la régularité de son intervention. Cela signifie tout d'abord qu'il doit définir et expliquer le but de l'intégration de services. Cette finalité est en effet le critère sur la base duquel on établit si son traitement est réellement lié à la finalité. Cela implique notamment qu'il doit indiquer clairement quels services il agrège, quels traitements il exécute et selon quels *service level agreements* il fonctionne.

34. Le champ d'action d'un intégrateur de services doit également être clairement délimité afin d'éviter le chevauchement des champs d'action d'intégrateurs de services. C'est crucial parce que :

- il doit être clair, tant pour les utilisateurs que pour les non-initiés, via quel intégrateur de services et selon quelles règles, notamment en matière de sécurité, il faut travailler ;

- il faut exclure le "shopping" entre les intégrateurs de services. Un tel phénomène serait en effet néfaste à terme pour la sécurité de l'information. Afin de pouvoir économiser sur les dépenses pour la sécurité de l'information par exemple, un utilisateur sera tenté de s'engager avec l'intégrateur qui pose le moins d'exigences à cet égard. Conséquence : un nivellement de la sécurité par le bas plutôt que par le haut ;

- il est exclu que des intégrateurs de services prennent simultanément sur le même terrain des initiatives qui pourraient dès lors semer la confusion.

35. Grâce à l'intégration de services, l'utilisateur a, moyennant l'autorisation requise, accès aux données à caractère personnel dont il a besoin pour exécuter ses tâches – sans intervention du citoyen concerné. Le citoyen ne peut toutefois pas être relégué au rang d'objet passif de cette évolution. Afin d'éviter cela, il est recommandé que l'utilisateur communique au citoyen sur quelles données il base une décision ou une action afin que le citoyen puisse contrôler si l'on a travaillé avec des données correctes. Il s'agit d'une nécessité absolue pour que ce dernier puisse pleinement exercer son droit de rectification. À cet égard, il est également précisé que les autorisations d'échange de données sont publiques. En ce qui concerne les comités sectoriels au sein de la Commission, elles sont publiées sur son site Internet, de manière à ce que chaque citoyen puisse contrôler qui a été autorisé à accéder à quelles données, provenant de quelles sources authentiques et pour quelles raisons.

36. Dans ce cadre, la Commission plaide pour que l'on veille à ce que le citoyen puisse recevoir un relevé des informations suivantes : quelles données ont été consultées par qui, en ayant recours à un intégrateur de services. Cela peut se faire conformément aux principes susmentionnés des cercles de confiance. Le fait de savoir que le citoyen, qui est le mieux placé pour détecter quand ses données ont été consultées à tort, dispose d'un tel droit de consultation ne peut qu'influencer positivement l'utilisation correcte des autorisations octroyées.

37. On peut également recommander qu'un intégrateur de services soit cogéré par des représentants des personnes concernées, lorsque cela est possible. Un intégrateur de services veillera surtout aux besoins des utilisateurs. La gestion de l'intégrateur de services par une entité

qui, de par la nature de sa composition, veillera aux intérêts des personnes concernées, garantit que les intérêts de ces dernières ne soient pas perdus de vue.

4.5. Sécurité

38. Garantir la sécurité implique que des mesures structurelles, organisationnelles, juridiques, personnelles, techniques et physiques soient prises pour que le risque de non-respect de la LVP soit minimalisé. Ces mesures doivent donc permettre concrètement que l'intégrateur de services :

- garantisse de façon raisonnable que les données à caractère personnel qui sont traitées pour l'intégration de services ne soient pas traitées pour d'autres finalités (article 4 de la LVP – voir également la rubrique 4.1.) ;

- garantisse de façon raisonnable l'intégrité, l'authenticité, la disponibilité et la confidentialité des données à caractère personnel qu'il traite et conclue à cet effet des accords avec les différentes parties intervenantes dans l'ensemble de la chaîne de services (*service level agreements*) ;

- assure le contrôle préventif de la légitimité et de la proportionnalité de l'intégration de services (article 4 de la LVP – voir également les points 28-29) ;

- garantisse que les données à caractère personnel ne puissent pas être modifiées ou détruites indûment lors du traitement (article 16 de la LVP) ;

- garantisse l'auditabilité (qui, quoi, quand, au sujet de qui et pourquoi) du traitement des données à caractère personnel dans l'ensemble de la chaîne de services et conclue à cet effet des accords avec les différentes parties intervenantes dans l'ensemble de la chaîne de services ;

- n'exporte pas vers des pays tiers sans niveau de protection adéquat (article 21 de la LVP) ;

- élabore les mesures de sécurité selon le principe des "cercles de confiance" (voir points 13-15).

39. Il est recommandé que l'intégrateur de services dispose d'un service interne de sécurité de l'information ayant une fonction de stimulation, de coordination et éventuellement de contrôle à l'égard des prestataires de services partiels et des utilisateurs de services intégrés. Cela ne dispense

ni les prestataires ni les utilisateurs de l'obligation de disposer d'une propre politique de sécurité de l'information et éventuellement d'un service de sécurité de l'information. Ces services seront en effet les interlocuteurs par excellence du service de sécurité de l'intégrateur de services. Ils devront vérifier, en concertation, la manière dont on peut garantir une sécurité maximale. Dans un premier temps, l'on veillera à ce que tous les participants atteignent un niveau de sécurité acceptable afin de l'affiner ensuite progressivement et donc de l'améliorer. L'on peut, dans ce contexte, s'inspirer du cadre de référence de la série de normes ISO 27000 (exigences de sécurité à l'égard du personnel, de la gestion des processus de communication et de service, de la sécurité des accès, du développement et de l'entretien de systèmes, du management de la continuité, de l'organisation de la sécurité, etc.).

40. Le respect des exigences de sécurité par l'intégrateur de services et les utilisateurs de services intégrés pourrait être évalué annuellement au moyen d'une check-list à compléter concernant des normes minimales de sécurité, approuvée par un organe de contrôle externe, de préférence un comité sectoriel de la Commission ou un organe d'autorisation comparable. Il y a en effet des limites aux exigences qu'un intégrateur de services peut imposer aux prestataires de services partiels et aux utilisateurs de services intégrés. Les normes minimales de sécurité et leur contrôle externe constituent donc un instrument adéquat pour garantir un respect approprié en la matière. Le comité pourrait faire dépendre la prolongation du bénéfice d'une autorisation d'efforts complémentaires à fournir par une personne concernée au niveau de la sécurité.

4.6. Droits de la personne concernée

41. L'article 10 de la LVP accorde au citoyen le droit de consulter ses données auprès du responsable du traitement. Lorsque le citoyen est confronté à une décision ou à une action d'un utilisateur d'une intégration de services, il n'est pas toujours évident pour lui de savoir à qui il devra s'adresser pour consulter ses données et pour pouvoir exercer réellement ce droit.

42. L'information correcte du citoyen implique donc que l'utilisateur de l'intégration de services mentionne non seulement les données sur lesquelles il se base, mais également qui sont les responsables du traitement concernés. D'une part, cela permet au citoyen d'évaluer la fiabilité de la décision de l'utilisateur et d'autre part, il sait à quel responsable du traitement il doit s'adresser.

43. Ce dernier élément est non seulement important en vue de l'exercice du droit de consultation mais aussi en vue du droit de rectification gratuite de données à caractère personnel inexactes et/ou du droit de suppression gratuite d'une donnée à caractère personnel "*qui, compte tenu du but du traitement, est incomplète ou non pertinente ou dont l'enregistrement, la communication ou la*

conservation sont interdits ou encore qui a été conservée au-delà de la période autorisée" (article 12 de la LVP).

44. On peut préciser à cet égard que le droit de rectification dans le chef du citoyen apporte en fait une plus-value pour l'intégration de services. En effet, la rectification de données inexactes profite finalement à tous les utilisateurs de l'intégration de services.

V. INTÉGRATION DE DONNÉES ET LVP

5.1. Loyauté, licéité et finalité

45. La Commission souligne que l'intégration de données dans le secteur public n'est permise que lorsqu'elle est utile pour une ou plusieurs situations reprises à l'article 5, premier alinéa de la LVP **et**, comme déjà indiqué aux points 10 à 12, que la fonctionnalité souhaitée ne peut pas être fournie avec une même efficacité au moyen de l'intégration de services. Du point de vue de la LVP, l'intégration de données est seulement justifiée si une alternative plus favorable au respect de la vie privée, comme l'intégration de services, n'est pas réalisable.

46. L'intégration de données est une finalité distincte et pas simplement la dérivée d'une autre finalité ou inhérente à celle-ci. La finalité "intégration de données" est en effet le critère au moyen duquel tous les aspects de ce processus sont évalués au niveau de leur conformité avec la LVP (finalité, proportionnalité, sécurité, etc.). Ce contrôle requiert que la finalité "intégration de données" soit clairement définie et délimitée (déterminée). Le domaine couvert par l'intégrateur de données constitue dans ce contexte un facteur non négligeable. Lorsque par exemple des données sensibles (articles 6 à 9) sont intégrées, il faudra vérifier si les conditions connexes spécifiques sont remplies à cet effet.

47. Les données qui sont intégrées doivent être définies clairement. L'on ne peut se contenter d'une désignation vague et générale, faute de quoi un contrôle sérieux de leur proportionnalité est exclu, entraînant le risque évident que des données non pertinentes soient reprises. Cela rejoint d'ailleurs le concept du droit de tout citoyen de savoir quelles données un certain responsable du traitement traite à son sujet (article 10 de la LVP).

48. L'intégrateur de données doit indiquer clairement qui est le responsable du traitement auprès duquel un citoyen peut exercer son droit d'accès, de rectification et de suppression (voir rubrique 4.6.). Il faut éviter à tout prix que le citoyen soit découragé d'exercer ses droits parce qu'il lui est impossible d'identifier le bon interlocuteur.

49. Les données sont agrégées par l'intégrateur de données et le responsable du traitement en vue d'une finalité déterminée. La mesure dans laquelle de telles données intégrées peuvent être transmises à un tiers ou à un utilisateur dépend de la mesure dans laquelle la finalité pour laquelle ce dernier souhaite ces données est compatible avec la finalité de l'intégrateur en question. Cette compatibilité est appréciée en tenant compte des prévisions raisonnables ou des dispositions réglementaires en la matière (article 4, § 1, 2° de la LVP).

5.2. Proportionnalité

50. Dans certains cas, on sera contraint de procéder à une intégration de données pour réaliser une action déterminée ou une finalité, par exemple pour produire des statistiques. Ces données intégrées doivent être traitées conformément à la LVP. Cela signifie que si, pour la réalisation de la finalité, il n'est pas requis qu'un lien puisse être établi avec une personne physique déterminée, seul un enregistrement de ces données sous forme anonyme ou du moins sous forme codée est justifié. Ce n'est que lorsque la finalité requiert de pouvoir retrouver un individu que les données intégrées peuvent être enregistrées sous une forme permettant ce lien.

51. Ces principes s'appliquent également à l'envoi de données intégrées. Il faut donner la priorité à un envoi sous forme anonyme ou codée. Un envoi non codé n'est permis que pour autant que l'on démontre que l'utilisateur ne peut pas réaliser sa finalité au moyen de données anonymes.

52. Un certain nombre de principes avancés au regard de la problématique de la proportionnalité dans le volet relatif à l'intégration de services doivent être appliqués par analogie à l'intégration de données :

- la nécessité de délimiter clairement et de façon suffisamment homogène le champ d'application d'un intégrateur de données ;

- la gestion de loggings selon le principe des "cercles de confiance" ;

- on ne peut agréger que des données à caractère personnel qui sont pertinentes et non excessives pour les utilisateurs des données intégrées, rendant nécessaire un contrôle des données par rapport à la finalité ;

- dans le prolongement, des mesures appropriées doivent être prises pour qu'un utilisateur ne reçoive que des données concernant des personnes pour lesquelles ces données sont

pertinentes et non excessives à la lumière de la finalité poursuivie par l'utilisateur en question ;

- le respect des autorisations accordées par un comité sectoriel de la Commission ou un organe comparable.

5.3. Exactitude et précision

53. Tout comme pour un intégrateur de services, il est recommandé qu'un intégrateur de données conclue, avec les fournisseurs de données faisant l'objet de l'intégration, des "*service level agreements*" relatifs à l'exactitude et à la précision des données à caractère personnel fournies. En effet, la qualité des données intégrées en dépend. Cela implique par exemple des accords concernant le timing selon lequel des modifications ou rectifications de données doivent être signalées à l'intégrateur par les fournisseurs. Des données dépassées réduisent en effet la qualité des données intégrées. Pour les utilisateurs, il s'agit d'ailleurs d'informations pertinentes pour évaluer leur impact sur leurs activités.

54. Cependant, si la qualité des données fournies est bonne mais que leur intégration n'est pas réalisée avec soin, le résultat et donc l'exactitude des données intégrées sont médiocres, avec toutes les conséquences qui en découlent pour les utilisateurs. Par exemple, un utilisateur refuse injustement une intervention pour un citoyen parce que certaines données intégrées concernent une autre personne. L'intégrateur de données doit donc prendre des mesures pour veiller à ce que les données agrégées concernent une seule et même personne. Procéder à cette agrégation de données au moyen du numéro d'identification du Registre national pourrait par exemple constituer une de ces mesures.

5.4. Transparence

55. Vu l'impact sur la vie privée de l'intégration de données, une transparence maximale doit être assurée. Il est recommandé que l'intégrateur de données publie des informations claires concernant toutes les facettes de son fonctionnement, de manière à ce que chacun ait la possibilité de vérifier la régularité de son intervention.

56. Outre la communication d'informations publiques, cette transparence peut être réalisée en associant des représentants des personnes concernées à la gestion ou au contrôle de l'intégrateur de données. La Commission se réfère à cet égard aux suggestions qu'elle a formulées à ce sujet

dans le chapitre sur l'intégration de services et qu'elle rappelle ici brièvement, à savoir qu'il faut fournir des informations sur :

- la finalité de l'intégration de données ;
- le champ d'application de l'intégration de données ;
- les utilisateurs des données intégrées ;
- le responsable du traitement auprès duquel les droits d'accès, de rectification et de suppression peuvent être exercés.

5.5. Sécurité et droits de la personne concernée

57. La Commission se réfère aux règles pratiques qu'elle a élaborées à cet égard concernant l'intégration de services (voir point 38 et suivants).

Pour l'Administrateur e.c., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere