



Comité sectoriel du Registre national

Délibération RN n°43/ du 21 septembre 2011

Objet : demande formulée par l'AGIV, Agentschap voor Geografische Informatie Vlaanderen (Agence de l'Information géographique de la Flandre), afin d'accéder à une information du Registre national et d'utiliser le numéro d'identification de ce registre en vue de la gestion des accès et des utilisateurs d'applications et de services Web (RN/MA/2011/178)

Le Comité sectoriel du Registre national (ci-après "le Comité");

Vu la loi du 8 août 1983 *organisant un Registre national des personnes physiques* (ci-après la "LRN") ;

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 *bis* ;

Vu l'arrêté royal du 17 décembre 2003 *fixant les modalités relatives à la composition et au fonctionnement de certains Comités sectoriels institués au sein de la Commission de la protection de la vie privée* ;

Vu la demande de l'agence autonomisée externe "Agentschap voor Geografische Informatie Vlaanderen", reçue le 7/06/2011 ;

Vu les informations complémentaires reçues par courrier le 17/06/2011 ;

Vu la demande d'avis technique et juridique adressée au Service public fédéral Intérieur en date du 10/08/2011 ;

Vu le rapport de la Présidente ;

Émet, après délibération, la décision suivante, le 21/09/2011 :

I. OBJET DE LA DEMANDE

1. La demande vise à ce que l'agence autonomisée externe "Agentschap voor Geografische Informatie Vlaanderen", ci-après le demandeur, soit autorisée à :

- accéder à l'information mentionnée à l'article 3, premier alinéa, 1° de la LRN ;
- utiliser le numéro d'identification du Registre national ;

en vue de l'organisation et de l'élaboration de la gestion des accès et des utilisateurs.

II. EXAMEN DE LA DEMANDE

A. LÉGISLATION APPLICABLE

A.1. Loi du 8 août 1983 (LRN)

2. Conformément à l'article 5, premier alinéa, 2° et à l'article 8 de la LRN, l'autorisation d'accéder aux informations du Registre national ou d'en obtenir communication et d'utiliser le numéro d'identification de ce registre est accordée par le Comité aux "*organismes publics ou privés de droit belge pour les informations nécessaires à l'accomplissement de tâches d'intérêt général qui leur sont confiées par ou en vertu d'une loi, d'un décret ou d'une ordonnance ou de tâches reconnues explicitement comme telles par le comité sectoriel précité*".

3. Le demandeur est une agence autonomisée externe, créée par le décret du 7 mai 2004 portant création de l'agence autonomisée externe de droit public "*Agentschap voor Geografische Informatie Vlaanderen*" (*Agence de l'Information géographique de la Flandre*).

4. L'article 11 du *décret cadre politique administrative* du 18 juillet 2003 prévoit la possibilité de créer des agences autonomisées externes dotées de la personnalité juridique. Les agences autonomisées externes prennent les décisions en toute autonomie. Elles ne relèvent pas de l'autorité hiérarchique du ministre. Au niveau politique, le ministre reste toutefois le responsable final. D'un point de vue juridique, il s'agit d'une décentralisation fonctionnelle où un service indépendant se voit confier une tâche spécialisée et déterminée d'intérêt général déterminée (Parlement flamand, législature 2002-2003; document n° 1612, n° 1, p. 7) [traduction libre réalisée par le secrétariat de la Commission, en l'absence d'une traduction officielle].

5. Cette tâche est définie à l'article 4 du décret du 7 mai 2004 qui stipule que sa mission consiste à *optimiser l'utilisation des informations géographiques en Flandre*.

6. Le demandeur entre dès lors en ligne de compte pour bénéficier d'une autorisation sur la base de l'article 5, premier alinéa, 2° et de l'article 8 de la LRN.

A.2. Loi du 8 décembre 1992 (LVP)

7. En vertu de l'article 4 de la LVP, les informations et le numéro d'identification du Registre national constituent des données à caractère personnel dont le traitement n'est autorisé que pour des finalités déterminées, explicites et légitimes. Les données à caractère personnel doivent en outre être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

B. FINALITÉS

8. L'article 5 du décret du 7 mai 2004 énumère les tâches qui sont confiées au demandeur en vue de l'accomplissement de la mission dont il est chargé. Il est explicitement prévu que cet ensemble de tâches ne porte pas préjudice aux missions qui sont dévolues au demandeur en vertu d'autres décrets, comme le décret GDI, le décret GRB, le décret CRAB et le décret KLIP¹.

9. En vue d'exécuter les tâches qui lui sont confiées dans le décret, le demandeur a développé plusieurs applications et services Web. Il s'agit plus particulièrement d'applications et de services Web destinés à :

- la gestion décentralisée via le "Loket voor Authentieke Registratie" (LARA), guichet pour l'enregistrement authentique d'adresses par des agents d'administrations locales, en application des articles 17 et 22 du décret CRAB ;
- la gestion décentralisée d'informations sur les câbles et canalisations par les gestionnaires de câbles et de canalisations et l'introduction de demandes de plans par des entrepreneurs dans le cadre du décret KLIP (application KLIP) ;

¹ Le décret GDI : décret du 20 février 2009 *relatif à la " Geografische Data-Infrastructuur Vlaanderen "* (*l'infrastructure de données géographiques de la Flandre*) ; le décret GRB : décret du 16 avril 2004 *relatif au "Grootschalig Referentie Bestand (GRB)"* (*Base de données des références à grande échelle*) ; le décret KLIP : décret du 14 mars 2008 *portant la libération et l'échange d'informations sur les câbles et canalisations souterrains (Décret KLIP)* ; le décret CRAB *relatif au Fichier central d'Adresses de Référence*.

- la gestion décentralisée via le LARA de données GRB par des cogestionnaires GRB, à savoir des gestionnaires du domaine public (application de l'article 13 du décret GRB) ;
- la consultation et le chargement de données disponibles dans la GDI, Geografische Data-Infrastructuur (Infrastructure de données géographiques) à l'aide des services de consultation et de l'application de chargement qui seront mis à disposition de différents groupes cibles via le portail GDI-Vlaanderen, en application de diverses dispositions du décret GDI.

10. Ceci requiert, dans le chef du demandeur, qu'il mette au point une gestion des accès et des utilisateurs performante afin de garantir d'une part que seules des personnes dûment identifiées obtiennent un accès et d'autre part que l'étendue de l'accès de ces dernières soit limitée en fonction de leur qualité.

11. À cet égard, la demande précise que :

- les personnes qui souhaitent accéder à une des applications susmentionnées s'identifient et s'authentifient à l'aide soit de la carte d'identité électronique (eID), soit du token fédéral ;
- l'on utilise le Federal Authentication Service qui est mis à disposition par Fedict ;
- en cas d'identification et d'authentification réussies, Fedict fournit le nom, le prénom et le numéro d'identification de la personne concernée au demandeur qui enregistre ces données avec des informations que la personne concernée a fournies lors de son enregistrement ;
- lorsque l'accès à une application déterminée est limité aux personnes ayant une certaine qualité, par exemple des agents locaux ou des entrepreneurs, l'Access Control Management de l'Autorité flamande sera sollicité, via le service Web afin de contrôler ces attributs supplémentaires.

12. En vue de l'organisation et de l'harmonisation de ces étapes, le demandeur souhaite disposer d'un accès et utiliser le numéro d'identification.

13. Le Comité estime que la finalité susmentionnée qui est poursuivie est déterminée, explicite et légitime au sens de l'article 4, § 1, 2^o de la LVP et de l'article 5, deuxième alinéa de la LRN.

C. PROPORTIONNALITÉ

C.1. Quant aux données

14. Le demandeur souhaite obtenir un accès à l'information mentionnée à l'article 3, premier alinéa, 1° de la LRN, à savoir les nom et prénoms.

15. Le Comité déduit de la demande que le demandeur ne vise pas un accès physique proprement dit au Registre national mais souhaite uniquement enregistrer et utiliser les noms et prénoms qui sont communiqués par Fedict lors d'une identification et d'une authentification positives en vue de l'organisation de la gestion des accès et des utilisateurs.

16. Pour le traitement (collecte et enregistrement) de ces données, aucune autorisation n'est requise. Les données à caractère personnel, dont le nom et les prénoms, peuvent en effet être traitées dans les cas mentionnés à l'article 5 de la LVP et le demandeur peut en particulier invoquer l'article 5, premier alinéa, c) et/ou e) de la LVP.

C.2. Utilisation du numéro d'identification

17. Pour le bon fonctionnement du système, il est essentiel que les utilisateurs soient correctement identifiés. Cela signifie que les malentendus pouvant survenir à l'occasion d'une homonymie et d'une orthographe erronée doivent être exclus afin de ne pas hypothéquer les étapes ultérieures d'authentification et d'autorisation.

18. L'identification, l'authentification et l'autorisation électroniques doivent se faire de manière sûre et sécurisée. Le demandeur doit être certain de l'identité de la personne qui souhaite utiliser une application ou un service Web car ces canaux servent d'une part à octroyer un accès et d'autre part à poser des actes.

19. Pour pouvoir accorder une autorisation, le demandeur doit conserver certaines données d'utilisateur – que ce soit en utilisant un token ou la eID à cet effet – afin de pouvoir à tout moment procéder à l'authentification et déterminer le droit d'accès. Pour ce faire, outre le nom et les prénoms, il opte aussi pour la conservation du numéro d'identification du Registre national.

20. Le numéro d'identification unique du Registre national permet d'identifier une personne avec précision ainsi que de tracer toutes les consultations effectuées et tous les actes posés.

21. Le Comité conclut qu'à la lumière de la finalité indiquée, l'utilisation du numéro d'identification est conforme à l'article 4, § 1, 3° de la LVP.

C.3. Quant à la durée pour laquelle l'utilisation est demandée

22. L'utilisation est demandée pour une durée indéterminée, vu que le demandeur ne peut pas prévoir pour combien de temps le service mentionné au point B sera fourni à l'aide d'applications et de services Web.

23. Le Comité constate qu'à la lumière de cet élément, une autorisation d'une durée indéterminée est appropriée (article 4, § 1, 3° de la LVP).

C.4. Quant au délai de conservation

24. La demande fait mention d'un délai de conservation d'une durée indéterminée. En fait, le demandeur entend ainsi indiquer que le délai concret ne peut pas être fixé à l'avance.

25. Le Comité constate que la demande mentionne toutefois un certain nombre de critères permettant d'évaluer concrètement si les données d'une personne déterminée doivent encore être conservées, à savoir :

- lorsqu'une personne ne dispose pas de la qualité requise pour accéder aux applications et services Web ou qu'elle se désinscrit, il n'y a **en principe** plus aucune raison de conserver encore les données à caractère personnel de la personne concernée, dont son numéro d'identification, en vue de la gestion des utilisateurs et des accès. Ces données doivent donc être supprimées des banques de données y afférentes ;
- le demandeur a mis au point une politique d'archivage, dictée par les articles 1382 et 2262*bis* et suivants du Code civil. À la lumière de cette politique, il conserve certaines opérations et les données à caractère personnel s'y rapportant pendant 10 ans, les autres données pendant 20 ans².

² Le demandeur reçoit des informations électroniques fournies par des tiers. Ces informations sont transmises, sous certaines conditions, à des tiers (par exemple des entrepreneurs qui effectuent des travaux). Pour certaines informations, une indemnité est due. En cas de dommages, la validité des informations qui ont été fournies est souvent mise en doute. Dans ce cas, il faut pouvoir vérifier qui est responsable de l'enregistrement des données. *Idem dito* lorsque la fourniture d'informations pour laquelle une indemnité est due est contestée.

26. Dans la mesure où le demandeur tient compte des exigences formulées ci-dessus, le Comité estime qu'il agit conformément à l'article 4, § 1, 5° de la LVP.

C.5. Usage interne et/ou communication à des tiers

27. Il ressort des informations communiquées par le demandeur que le numéro d'identification sera exclusivement utilisé en interne.

28. Le Comité en prend acte et attire l'attention sur ce qui est mentionné ci-après au point C.6. concernant la communication de ce numéro à des tiers.

C.6. Connexions en réseau

29. La demande indique qu'il y aura une connexion en réseau avec Corve.

30. Le Comité fait remarquer que l'Access Control Management/Identity Management de l'Autorité flamande que le demandeur souhaite consulter est géré par le SGS-ICT – qui dispose à cet effet d'une autorisation. Ce sera donc avec ce service qu'une connexion sera établie, pas avec Corve.

31. Par souci d'exhaustivité, le Comité attire l'attention sur le fait que :

- si des connexions en réseau devaient être établies ultérieurement, le demandeur devra l'en informer au préalable ;
- le numéro d'identification du Registre national ne peut être utilisé dans des relations avec des tiers que dans la mesure où cela s'inscrit dans le cadre des finalités pour lesquelles ceux-ci ont également été autorisés à utiliser ce numéro.

D. SÉCURITÉ

D.1. Conseiller en sécurité de l'information

32. L'identité du conseiller en sécurité de l'information a été communiquée. Il a déjà été accepté précédemment³ en tant que conseiller en sécurité par le Comité.

³ Délibération RN n° 30/2007.

D.2. Politique de sécurité de l'information

33. Il ressort des documents fournis par le demandeur que ce dernier dispose d'une politique de sécurité ainsi que d'un plan en application de celle-ci.

34. Le Comité en a pris acte.

D.3. Personnes pouvant utiliser le numéro d'identification du Registre national et liste de ces personnes

35. La demande mentionne que le conseiller en sécurité et les membres du personnel du service chargé de la gestion pratique et de la maintenance de la gestion des accès et des utilisateurs utiliseront le numéro d'identification.

36. Comme le prescrit l'article 12 de la LRN, le demandeur doit dresser une liste des personnes qui utilisent le numéro du Registre national. Cette liste sera constamment actualisée et tenue à la disposition du Comité.

37. Les personnes figurant sur cette liste devront en outre signer une déclaration par laquelle elles s'engagent à préserver la sécurité et le caractère confidentiel des informations.

PAR CES MOTIFS,

le Comité

1° autorise, pour une durée indéterminée, l'agence autonomisée externe "Agentschap voor Geografische Informatie Vlaanderen", aux conditions fixées dans la présente délibération et en vue de la finalité mentionnée au point B à utiliser le numéro d'identification du Registre national.

2° stipule que lors de toute modification ultérieure de l'organisation de la sécurité de l'information pouvant avoir un impact sur les réponses données au questionnaire sécurité fourni au Comité (désignation du conseiller en sécurité et réponses aux questions relatives à l'organisation de la sécurité), l'agence autonomisée externe "Agentschap voor Geografische Informatie Vlaanderen" adressera au Comité un nouveau questionnaire relatif à l'état de la sécurité de l'information complété conformément à la vérité. Le Comité en accusera réception et se réserve le droit de réagir ultérieurement, s'il y a lieu ;

3° stipule que lorsqu'il enverra un questionnaire relatif à l'état de la sécurité de l'information à l'agence autonomisée externe "Agentschap voor Geografische Informatie Vlaanderen", cette dernière devra compléter ce questionnaire conformément à la vérité et le renvoyer au Comité. Celui-ci en accusera réception et se réserve le droit de réagir ultérieurement, s'il y a lieu.

4° refuse ce qui est demandé en sus.

Pour l'Administrateur e.c.,

La Présidente,

(sé) Patrick Van Wouwe

(sé) Mireille Salmon