Comité sectoriel du Registre national

Recommandation RN n° 01/2015 du 18 février 2015

Objet : Recommandation aux communes et administrations locales relative à la sécurité de l'information devant encadrer leurs accès au Registre national et traitements consécutifs des données du Registre national (RN-AR-2014-001)

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"), en particulier l'article 16, premier alinéa, 3° ;

Vu le rapport de la Présidente ;

Émet, le 18 février 2015, la recommandation suivante :

I. OBJET DE LA RECOMMANDATION

1. Suite à l'analyse de plaintes de citoyens concernant une utilisation abusive des données du Registre national au sein des communes et administrations locales ainsi qu'au constat, lors de contacts avec ces dernières à propos d'autorisations spécifiques, d'une organisation défaillante de la sécurité de l'information en leur sein et, même, d'une disponibilité inadéquate de ces données lors d'un contrôle in-situ, le Comité a considéré opportun de rassembler et de rappeler dans ces recommandations les principaux aspects de sécurité de l'information qui doivent être pris en compte par les communes et les administrations locales lors de leurs accès aux données du Registre national et lors du traitements de celles-ci.

2. Le Registre national est le système de traitement d'informations qui assure centralement l'enregistrement, la mémorisation et la communication d'informations relatives à l'identification des personnes physiques c'est-à-dire des citoyens. Un numéro d'identification est attribué à chaque personne lors de la première inscription de celle-ci au Registre national : le numéro national.

3. Le Registre national est alimenté notamment par chaque commune belge au départ de son registre de la population.

4. Afin de permettre l'exercice quotidien de leurs missions, les communes et administrations locales doivent disposer d'accès aux informations contenues centralement au Registre national et localement dans leur registre de la population et sont appelées à traiter ces données.

5. D'une manière générale, par la suite, ces données, dont le numéro national, seront nommées '*données du Registre national*'. De même, l'intitulé '*traitement de données du Registre national*' couvrira aussi bien l'accès proprement dit aux données du Registre national par les communes et les administrations locales que les traitements consécutifs des données obtenues par ces dernières et l'intitulé '*accès aux données du Registre National*', tout accès effectué soit centralement auprès du Registre national ou localement auprès du registre de la population ou sur toute copie locale des données du Registre national.

6. Les données du Registre national étant par nature des données à caractère personnel, l'accent mis par ces recommandations principalement sur les aspects de la sécurité de l'information spécifiques aux traitements des données du Registre national par les communes et les administrations locales ne préjuge pas de l'importance de la sécurité de l'information des données à caractère personnel dans son ensemble au sein de ces dernières pour laquelle nous

renvoyons aux '*Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel*[1]' ainsi qu'aux '*Lignes directrices pour la sécurité de l'information des données à caractère personnel dans les villes et les communes*[2]' éditées par la Commission de la protection de la vie privée et auxquelles les communes et les administrations locales doivent évidemment se conformer.

7. La sécurité de l'information étant un domaine en perpétuelle évolution, ces recommandations seront adaptées progressivement aux différentes évolutions légales, techniques ou autres.

II. LES GRANDS PRINCIPES

8. De la spécificité des traitements des données du Registre national effectués par les communes et les administrations locales et du cadre légal propre qui les régit peuvent être déduits les grands principes qui doivent constamment servir de 'fil rouge' tout au long du cycle de vie du système d'information permettant l'exécution de ces traitements, et ce, depuis les phases préparatoires et de conception jusqu'à la phase d'utilisation opérationnelle en passant par les phases de réalisation et de mise en production, afin de déterminer les objectifs de sécurité de l'information que ces dernières doivent s'efforcer d'atteindre pour respecter la loi.

9. Ces grands principes sont :

Conseiller en sécurité de l'information

10. Les communes et les administrations locales doivent disposer d'un conseiller en sécurité de l'information en tant que responsable de la surveillance et du contrôle de l'exécution de la politique de sécurité de l'information. Il veillera particulièrement à ce que les données du Registre national soient traitées correctement.

---

[1] http://www.privacycommission.be/nl/node/3941

[2] http://www.privacycommission.be/fr/node/7595

Politique de sécurité

11. Les communes et les administrations locales doivent disposer d'une politique de sécurité de qualité précisant clairement les stratégies et mesures retenues pour sécuriser les accès aux données du Registre national ainsi que les traitements de celles-ci.

Autorisation préalable

12. Tout traitement de données du Registre national effectué par les communes et les administrations locales doit être autorisé par la loi ou par une autorisation préalable du Comité.

Politique des d'accès

13. À tout moment, les données du Registre national ne peuvent être accessibles qu'aux utilisateurs et aux systèmes applicatifs qui en ont explicitement l'autorisation.

Minimisation des données

14. Tout traitement des données du Registre national doit être organisé de façon à ce que ne soient traitées (affichées, stockées, etc.) qu'uniquement les données strictement nécessaires et pertinentes au regard de la finalité poursuivie par cet accès.

Finalité incompatible

15. Les données du Registre national obtenues pour une certaine finalité ne peuvent être utilisées pour une finalité incompatible avec celle-ci.

Droit d'être informé

16. Toute personne dont les données du Registre national auront été traitées par une commune ou une administration locale doit pouvoir être informée par celle-ci de la raison de ce traitement.

III. RECOMMANDATIONS

17. De l'application de ces grands principes aux traitements des données du Registre national effectués par les communes et les administrations locales peuvent se déduire les recommandations suivantes :

Conseiller en sécurité de l'information

18. Les communes et les administrations locales doivent désigner un conseiller en sécurité de l'information et communiquer l'identité de ce dernier au Comité.

19. Elles doivent fournir au conseiller en sécurité de l'information la formation nécessaire à l'exécution correcte de sa fonction et au maintien de son niveau de compétence dans le temps.

20. Elles doivent prévoir les modalités pratiques nécessaires afin que le conseiller en sécurité dispose de toutes les informations nécessaires et utiles à l'exercice normal de sa mission.

21. Au sein de sa commune, le conseiller en sécurité de l'information sera responsable de la surveillance et du contrôle de l'exécution de la politique de sécurité de l'information. Il veillera notamment à ce que les données du Registre national soient traitées correctement et conformément à ces recommandations et effectuera tous les contrôles nécessaires afin de s'en assurer.

Politique de sécurité de l'information

22. Les communes et les administrations locales doivent disposer d'une politique de sécurité de l'information de qualité précisant notamment clairement les stratégies et mesures retenues pour sécuriser les accès aux données du Registre national ainsi que les traitements de celles-ci.

23. Cette politique de sécurité doit notamment comprendre les fondements de la sécurité de l'information propres au traitement des données du Registre national, les différents aspects de sensibilisation des utilisateurs à ces derniers ainsi que les sanctions prévues en cas d'enfreinte aux règles de sécurité relatives à la protection de ces données.

24. Les communes et les administrations locales doivent prévoir les moyens nécessaires pour la mise en œuvre et la maintenance de la politique de sécurité, tant en ressources humaines qu'en moyens matériels, logiciels, logistiques et financiers.

25. Afin de les soutenir dans cette démarche, la Commission de la protection de la vie privée a publié les '*Lignes directrices pour la sécurité de l'information des données à caractère personnel dans les villes et les communes*[3]' auxquelles le Comité renvoie.

---

[3] http://www.privacycommission.be/fr/node/7595

Autorisation préalable et appréciation des finalités

26. Les communes et les administrations locales doivent s'assurer que tous les traitements de données du Registre national effectués en leur sein soient bien autorisés soit par la loi, pour les finalités qui se situent dans le cadre des compétences qui leur sont règlementairement conférées, soit par une autorisation du Comité lorsqu'il s'agit d'une autre finalité spécifique, et qu'ils s'effectuent bien uniquement pour les finalités pour lesquelles ils ont été initialement autorisés.

27. Pour tous les traitement de données du Registre national pour lesquels ce ne serait pas le cas, une demande d'autorisation spécifique doit être introduite auprès du Comité.

28. Des procédures claires et bien définies doivent être mises en place afin de s'assurer que tout traitement de données du Registre national, et particulièrement toute consultation de ces données, ne puisse s'effectuer que sous le couvert d'une décision préalable du collège des bourgmestre et échevins et ce, après contrôle et appréciation de la finalité inhérente à ce traitement et qu'une publicité suffisante soit faite à ce propos au sein de la commune afin que chacun sache clairement ce qui est permis et ce qui ne l'est pas.

Identification de l'information et des supports

29. Les communes et les administrations locales doivent disposer de procédures de gestion visant à inventorier les localisations de toutes les données du Registre national sur quelque support que ce soit (papier, support électronique, etc.) ainsi que les différents processus et systèmes applicatifs utilisés pour les traiter afin d'évaluer le risque couru par ces données et d'organiser l'accès à ces supports, la gestion de ces derniers et les différents traitements des données concernées conformément aux présentes recommandations.

Politique des d'accès

30. À tout moment, les données du Registre national ne peuvent être accessibles qu'aux utilisateurs et aux systèmes applicatifs qui en ont explicitement l'autorisation et ce uniquement en cas de nécessité justifiée (need to know basis).

31. Pour ce faire, les communes et les administrations locales doivent disposer d'un système de gestion des utilisateurs et des accès permettant de sécuriser tout accès aux données du Registre national, que cet accès soit effectué directement auprès du Registre national ou sur une copie locale des données en provenance de celui-ci, et ce, par un système d'identification,

d'authentification et d'autorisation, que cet accès soit effectué par un utilisateur ou par un processus ou un système.

32. Le système d'identification doit obligatoirement permettre d'identifier individuellement chaque utilisateur ainsi que chaque processus ou système.

33. Le système d'authentification (mot de passe, eID, etc.) doit permettre à chaque demandeur d'accès (utilisateur ou système) de prouver qu'il est bien ce qu'il prétend être.

34. Si possible, l'authentification électronique de l'identité d'un utilisateur doit se faire de préférence à l'aide de la carte d'identité électronique (eID) car elle offre le maximum de garantie.

35. Si l'authentification des utilisateurs est effectuée au moyen de mots de passe, ceux-ci doivent être gérés sur base d'un processus formel (nombre de digits, complexité, renouvellement, etc.).

36. Le système d'autorisation doit s'assurer que chaque demandeur d'accès (utilisateur ou système) n'accède bien qu'aux seules données du registre national auxquelles il a le droit d'accéder c'est-à-dire uniquement celles qui sont strictement nécessaires à l'exécution des différentes finalités que sa fonction doit couvrir.

37. Ce système de gestion des utilisateurs et des accès doit limiter les accès des différents gestionnaires d'information (administrateur système, opérateur système, développeur, etc.) au strict minimum possible.

38. Afin d'éviter tout accès illicite, tous les systèmes applicatifs permettant d'accéder à des données du Registre national doivent prévoir un temps limite d'inactivité assez court (timeout) à l'échéance duquel la session est automatiquement terminée.

39. Les communes et les administrations locales doivent tenir à jour la liste nominative des personnes habilitées à accéder et à traiter les données à caractère personnel, avec leurs identifiants utilisés pour accéder aux différents systèmes ainsi que leurs droits d'accès respectifs.

40. L'attention des utilisateurs doit être particulièrement attirée sur leur propre responsabilité en ce qui concerne le maintien d'une protection efficace de l'accès, notamment sur le plan de l'utilisation de mots de passe, ou autre moyen d'authentification, et de la sécurité du matériel utilisé.

Minimisation des données

41. Les communes et les administrations locales doivent veiller à ce que tout traitement des données du Registre national soit organisé de façon à ce que ne soient traitées (affichées, stockées, etc.) qu'uniquement les données strictement nécessaires et pertinentes au regard de la finalité poursuivie par cet accès.

42. Elles doivent s'assurer que, pour tout traitement des données du Registre national, aucune trace de ces données ne subsiste inutilement après exécution du traitement dans aucune copie locale sur quelque support que ce soit ni dans aucun des systèmes techniques intermédiaires (logs, backups, données de connexion, etc.) nécessaires à l'exécution de ce traitement.

43. Elles veilleront particulièrement à ce que l'effacement des données du Registre national sur support magnétique ainsi que la destruction de tout support contenant ces données soient effectués de façon contrôlée et irréversible.

Traçage des accès

44. Les communes et les administrations locales doivent veiller à ce que tous les systèmes applicatifs permettant un accès aux données du Registre national, que cet accès se fasse directement au Registre national ou sur toute copie locale de ces données, effectuent un traçage des différents accès, que ces accès soient exécutés par un utilisateur ou par un système.

45. Ce traçage doit inclure les activités des différents gestionnaires d'information (administrateur système, opérateur système, développeur, etc.).

46. Ce traçage doit comprendre l'identification de l'utilisateur individuel ou du processus ou système qui a accédé à ces données, les données qui ont été accédées, la façon dont elles ont été accédées (en lecture, en modification, etc.), quand elles ont été accédées, ainsi que le motif de cet accès.

47. Si nécessaire, les systèmes applicatifs permettant un accès utilisateur aux données du Registre national doivent prévoir la possibilité d'une introduction obligatoire du motif de cet accès par l'utilisateur lui-même.

48. Ce traçage doit périodiquement et régulièrement être contrôlé afin de détecter toute infraction à la politique d'accès ou toute anomalie et de prendre toutes les mesures correctives qui s'imposent.

49. Généralement, les fichiers de journalisations permettant ce traçage doivent être conservés au moins 10 ans[4].

Formation et information des utilisateurs et collaborateurs

50. Les communes et les administrations locales doivent prendre toutes les mesures nécessaires afin que toute personne (interne ou externe) intervenant dans le traitement des données du Registre national soit correctement formée à l'exercice de sa fonction et de ses responsabilités de sécurité et constamment suffisamment informée de ses devoirs et responsabilités lors de ces traitements comme notamment l'obligation de secret professionnel, l'obligation de mettre tout en œuvre pour maintenir la confidentialité, l'intégrité et la disponibilité des données du Registre national traitées ainsi que l'obligation de signaler les risques et les incidents de sécurité relatifs à ces données.

Elles veilleront notamment à :

51. faire signer un engagement de confidentialité visant à ne donner accès aux données du Registre national ou à ne communiquer celles-ci qu'aux personnes autorisées ;

52. prendre toutes les mesures jugées nécessaires pour réduire le risque que ces données soient rendues accessibles à une personne non autorisée par erreur ou par toute malveillance prévisible ;

53. organiser une procédure de sanction en cas d'enfreinte aux règles de sécurité relatives à la protection de ces données.

Sous-traitance

54. Lorsque le traitement des données du Registre national est confié à un sous-traitant, en tout ou en partie, les communes et les administrations locales doivent veiller à répercuter dans le contrat de sous-traitance, les mêmes obligations de sécurité de l'information que celles devant être en vigueur au sein de l'organisme lui-même.

---

[4] RN 40/2010
http://www.privacycommission.be/sites/privacycommission/files/documents/d%C3%A9lib%C3%A9ration_RN_40_2010_0.pdf
ou
RN 45/2010
http://www.privacycommission.be/sites/privacycommission/files/documents/d%C3%A9lib%C3%A9ration_RN_45_2010.pdf

Développement de systèmes applicatifs

55. Les communes et les administrations locales doivent veiller à ce que les systèmes applicatifs destinés à traiter les données du Registre national soient développés selon le principe du 'Privacy by Design' qui consiste à concevoir des produits et des services en prenant en compte, dès leur conception et tout au long du cycle de vie de la technologie concernée, les aspects liés à la protection des données à caractère personnel et dans notre cas particulier, les aspects liés à la protection des données du Registre national ainsi que le respect des valeurs qui en découlent.

56. Le développement de nouveaux systèmes applicatifs destinés à traiter les données du Registre national doit donc être basé sur une approche structurée qui impose les recommandations reprises ci-dessus dès le stade de la conception, les intègre dès le départ d'une façon optimale dans les spécifications initiales et veille à ce qu'elles soient prises en compte tout au long du cycle de vie du système applicatif concerné.

57. Un soin particulier sera apporté lors de la conception et du développement de tels systèmes applicatifs afin que, une fois le traitement concerné exécuté, aucune trace des données du Registre national ne subsiste inutilement dans aucun des systèmes techniques intermédiaires (logs, backups, etc.) nécessaires à l'exécution de ce traitement.

Surveillance, revue et maintenance

58. Au vu de la situation actuelle, il est fortement recommandé aux communes et administrations locales d'effectuer dans les plus brefs délais une autoévaluation de l'efficacité de leur politique actuelle de sécurité afin de s'assurer que les traitements de données du Registre national réalisés en leur sein s'effectuent bien conformément aux présentes recommandations. Pour ce faire, les systèmes applicatifs utilisés ainsi que de l'organisation pratique mise en place pour réaliser ces traitements doivent être analysés en profondeur afin de détecter à la lumière de ces recommandations les éventuels manquements et d'organiser et de planifier les mesures correctrices qui s'imposent.

59. Une fois une politique de sécurité de l'information cohérente installée, elles doivent alors veiller à ce que les mesures de sécurité techniques ou organisationnelles mises en place pour sécuriser les données du Registre national restent valides dans le temps et fassent l'objet de révisions régulières.

60. Pour ce faire, elles doivent notamment s'assurer de ce que une surveillance permanente s'effectue sur les traitements, l'évolution des ressources et l'analyse des journaux de traçage de façon à détecter à temps les différents besoins de maintenance de la sécurité et à prendre les mesures correctrices qui s'imposent.

61. Le conseiller en sécurité devra jouer un rôle primordial dans ces actions de surveillance et de contrôle.

Pour l'Administrateur f.f., abs. La Présidente,

(sé) An Machtens (sé) Mireille Salmon

Chef de section OMR f.f.