Comité sectoriel du Registre national

Délibération RN n° 21/2015 du 25 mars 2015

Objet: Autorisation générale d'utilisation du numéro d'identification du Registre national dans le cadre du recours au système "Federal Authentication Service" de Fedict pour la gestion des accès et des utilisateurs aux applications informatiques développées dans le cadre de missions de service public (RN-MA-2015-102)

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 d'avis technique et juridique adressée au Service public fédéral Intérieur en date du 26 novembre 2014 ;

Vu les questions posées par Fedict suite à la délibération n° 108/2014 adoptée le 10 décembre 2014, le Comité a décidé en sa séance du 18 février 2015 de remplacer sa délibération n° 108/2014 par la présente;

Vu les informations obtenues de Fedict en date du 2 mars 2015 ;

Vu le rapport de la Présidente ;

Émet, après délibération, la décision suivante, le 25 mars 2015:

I. OBJET ET CONTEXTE DE L'AUTORISATION GENERALE

1. Au vu du nombre croissant de requêtes adressées au Comité concernant l'utilisation du numéro de registre national dans le cadre de l'utilisation du système « FAS » (Federal Authentication Service) de Fedict, le Comité a décidé d'adopter la présente autorisation générale. Cette décision avait déjà été prise par le Comité dans le cadre de sa délibération n° 108/2014 du 10 décembre 2014 mais au regard de différentes questions et demandes de précisions soulevées par FEDICT postérieurement à sa publication, le Comité a décidé, lors de sa séance du 18 février 2015, de rouvrir le dossier et de substituer sa précédente délibération n°108/2014 par la présente.

2. Le système « FAS » peut en effet avoir pour utilisateurs finaux l'ensemble des services publics et institutions publiques, en ce compris les entreprises ou les personnes chargées d'une mission de service public, qui souhaitent disposer d'un processus sécurisé d'authentification pour les accès à leurs applications, moyennant la conclusion d'une convention d'utilisation avec le SPF Technologies. Certains utilisateurs souhaitent également recevoir de Fedict, en réponse à chaque processus d'authentification réussi, le numéro d'identification du Registre national des personnes concernées pour assurer la gestion de utilisateurs et des accès à leurs applications informatiques.

3. Tout responsable de traitement visé au considérant 10 qui adressera au Comité une déclaration écrite et signée aux termes de laquelle il s'engage à adhérer aux conditions de la présente autorisation unique pourra à cette fin et utiliser le numéro du Registre national moyennant le respect des conditions ci-dessous stipulées.

4. Les nom et adresse des responsables de traitement qui auront envoyé au Comité en tant qu'utilisateur FAS un engagement de conformité pour leurs traitements de données aux conditions fixées dans la présente décision seront publiés sur le site de la Commission de la protection de la vie privée en annexe de la présente délibération, une fois que le Comité les aura informé que l'autorisation peut entrer en vigueur dans leur chef.

5. Le Comité attire l'attention sur le fait que la présente autorisation vise à couvrir la communication par Fedict du numéro d'identification du Registre national à l'utilisateur[1] du système FAS. A ce jour, le système FAS peut être utilisé au moyen des méthodes d'authentification suivantes :
    - les identifiants avec mot de passe ;
    - les identifiants avec mot de passe et token ou un autre certificat (comme un sms ou un certificat délivré par une autorité de certification reconnue);
    - la carte d'identité électronique utilisée au moyen d'un lecteur de carte connecté avec code PIN ;
    - la carte d'identité électronique utilisée au moyen d'un lecteur de carte sans fil avec code PIN.

6. Il ressort des informations obtenues de Fedict que les méthodes d'authentification avec mots de passe et identifiants ne sont utilisées qu'après enregistrement de la personne concernée au moyen de sa carte d'identité électronique[2] (processus d'enregistrement pour obtenir les mot de passe et identifiant nécessitant l'authentification à l'aide de la carte d'identité électronique).

7. Lorsque l'authentification d'une personne concernée est réussie, « FAS » transmet cette information d'authentification positive en communiquant les nom, prénom et numéro de Registre national de cette personne au responsable du traitement (également visé dans la présente autorisation comme « utilisateur FAS » ou « adhérent ») pour lui permettre de gérer les accès et/ou les utilisateurs (visés également dans la présente délibération comme « personnes concernées ») à son application informatique concernée par cette authentification.

8. Le Comité a déjà pu rencontrer des demandes visant à recourir au système FAS de Fedict[3] et s'y est toujours montré favorable.

---

[1] Par utilisateur FAS, l'on entend les organisme visés à l'article 5, alinéa 1er, 1° et 2°, qui font le choix d'utiliser le système FAS de Fedict pour assurer l'authentification sécurisée des accès à leurs applications informatiques.

[2] On parle de eID « bootstrap ».

[3] Voir en ce sens les délibérations RN suivantes : n°29/2013 du 17 avril 2013, *relative à la demande formulée par l'Autorité flamande – Département Environnement, Nature et Énergie afin d'utiliser le numéro d'identification du Registre national en vue de la gestion des utilisateurs et des accès pour des applications d'e-government et afin que soit adaptée la délibération RN n° 34/2011*; n° 31/2014 du 9 avril 2014 *relative à la demande formulée par le Service public fédéral Personnel et Organisation afin d'être autorisé à utiliser le numéro de Registre national dans le cadre de l'enregistrement et de l'authentification des utilisateurs des applications fédérales e-Procurement*; n°48/2014 du 9 juillet 2014 *relative à la demande formulée par le Vlaams Infrastructuurfonds voor Persoonsgebonden Aangelegenheden (Fonds d'infrastructure flamand affecté aux matières personnalisables) du Département Bien-être, Santé publique et Famille afin d'être autorisé à utiliser le numéro d'identification du Registre national pour la gestion des utilisateurs et des accès de l'application Inter-VWA* ; n°61/2014 du 30 juillet 2014 *relative à la demande formulée par l'agence "Toerisme Vlaanderen" (Office du Tourisme de la Flandre) afin d'accéder aux informations du Registre national et d'utiliser le numéro d'identification de ce Registre en vue du suivi des demandes de subvention et de l'élaboration du système de gestion des utilisateurs et des accès* ; n° 62/2014 du 30 juillet 2014 *relative à la demande formulée par Infrabel SA afin d'utiliser le numéro d'identification du Registre national en vue d'organiser la gestion des utilisateurs et des accès de l'application Crisscomm* et la n° 89/2014 du 29 octobre 2014, *relative à la demande formulée par le SPF Justice afin d'utiliser le numéro de Registre national en vue du projet pilote e-Deposit*.

II. CONDITIONS

A. Responsables de traitement bénéficiaires de la présente autorisation unique.

9. L'autorisation d'utiliser le numéro d'identification du Registre national peut être accordée par le Comité aux « *autorités publiques belges pour les informations qu'elles sont habilitées à connaître en vertu d'une loi, d'un décret ou d'une ordonnance* » et 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*" (Article 5, al. 1er, 1° et 2° et article 8 de la LRN).

10. Seules les autorités publiques belges visées à l'article 5, alinéa 1er, 1° de la LRN ainsi que les organismes publics ou privés visés à l'article 5, alinéa 1er 2° mais uniquement pour les informations nécessaires à l'accomplissement des tâches d'intérêt général qui leur sont confiées par ou en vertu d'une loi d'un décret ou d'une ordonnance , qui adresseront au Comité une déclaration écrite et signée au terme de laquelle ils s'engagent à adhérer aux conditions de la présente autorisation unique seront autorisés à traiter le numéro d'identification dudit Registre pour les finalités ci-après décrites.

11. A son engagement de respecter les conditions de la présente délibération, l'organisme concerné devra joindre les formulaires complétés et signés relatif au candidat conseiller en sécurité et à la déclaration de conformité de son système de sécurité, pour évaluation par le Comité.

B. Finalités du traitement

12. Seuls peuvent faire l'objet d'un engagement de conformité par référence à la présente autorisation unique l'utilisation du numéro d'identification du Registre national par le responsable de traitement utilisateur FAS, visé au considérant 10, pour la gestion des accès et/ou des utilisateurs aux applications informatiques développées pour réaliser ses missions de service public.

13. Le recours au système FAS, avec communication par Fedict du numéro de Registre national de la personne concernée qui s'est authentifiée avec succès, doit permettre à l'utilisateur FAS de gérer les accès/ou les utilisateurs à son application informatique. La gestion des accès (en ce compris l'authentification) est un processus de vérification qui permet au responsable de

traitement d'une application informatique d'avoir la garantie de ce que la personne concernée qui se connecte à son application est bien en droit d'y accéder et est effectivement la personne qu'elle prétend être. Ainsi, un espace personnel au sein d'une application informatique est uniquement accessible à la personne qui dispose des droits d'accès. La gestion des utilisateurs consiste en la gestion au sein d'une application informatique, des droits spécifiques (tels que la lecture, l'écriture,…) dont disposent les personnes concernées, parfois en fonction certains rôles ou mandats dont elles sont titulaires. Les applications informatiques visées ont en effet généralement pour but de permettre aux personnes concernées d'accéder plus facilement à leur dossier pour le consulter, le suivre ou y apporter les modifications nécessaires, à l'introduction de demandes ou encore à l'envoi de documents.

C. Numéro d'identification du Registre national des personnes physiques

14. Afin d'éviter que des personnes non habilitées n'accèdent à des informations via l'application du responsable de traitement, elles doivent pouvoir être identifiées d'une manière précise, de sorte que les droits d'accès adéquats soient assurés[4].

15. Cela signifie qu'il faut exclure les malentendus pouvant survenir à la suite d'une homonymie ou d'une orthographe erronée afin de ne pas compromettre les étapes ultérieures d'authentification et d'autorisation. L'identification, l'authentification et l'autorisation électroniques doivent s'effectuer de manière sûre et sécurisée. L'organisme mettant son application informatique ou un service web à disposition doit être certain de l'identité de la personne qui souhaite l'utiliser car ces canaux permettent d'une part d'accéder à un certain nombre de données à caractère personnel et d'autre part d'effectuer certaines opérations.

16. Le numéro d'identification du Registre national constitue un instrument adéquat pour assurer la gestion des utilisateurs et des accès à une application informatique. Il s'agit d'un numéro unique qui permet d'identifier une personne avec une grande précision. Les erreurs pouvant survenir notamment en raison d'une homonymie et/ou de fautes d'orthographe sont exclues.

17. Le principe de finalité implique que tout bénéficiaire d'une autorisation, qui réalise un traitement de données autorisé pour une finalité incompatible à celle pour laquelle il a été autorisé, commet un détournement de finalité pénalement punissable (art. 11 LRN et 39 LVP).

---

[4] Voir en ce sens la délibération n° 62/2014 du 30 juillet 2014, *relative à la demande formulée par Infrabel SA afin d'utiliser le numéro d'identification du Registre national en vue de la gestion des utilisateurs et des accès de l'application Crisscrom,* page 4, point 11.

D. Durée de la présente autorisation

18. Le responsable de traitement adhérent ne pourra se prévaloir de l'autorisation générale, que pendant la durée de vie de son application informatique développée pour assurer sa mission de service publique et concernée par le système FAS. Dès suppression de l'application informatique concernée, l'adhérent s'engage à communiquer cet état de fait sans délai au Comité.

19. À la lumière de ces éléments et moyennant le respect de cette condition, une autorisation d'une durée indéterminée est appropriée (article 4, § 1, 3°, de la LVP).

E. Durée de conservation

20. Le Comité constate qu'il est difficile de prévoir un délai de conservation concret. Le numéro d'identification au Registre national doit pouvoir être conservé aussi longtemps que nécessaire pour permettre la gestion des accès et des utilisateurs de l'application informatique ou du service web mis à disposition.

21. Par ailleurs, si le numéro d'identification des personnes concernées est conservé dans les loggings en vue de garantir la traçabilité des consultations ou opérations effectuées, la durée de conservation du numéro d'identification du Registre national est en principe au minimum de 10 ans[5]. Dans le cadre de la gestion des accès et des utilisateurs, les loggings doivent en effet permettre de constater des irrégularités ou des abus. Compte tenu du fait que les abus concernant le traitement de données à caractère personnel sont des faits punissables, il est recommandé de conserver de tels loggings pendant au moins 10 ans.

22. À condition que l'adhérent conserve le numéro d'identification du Registre national pendant le temps nécessaire pour assurer la gestion des utilisateurs et accès à son application informatique, en ce compris la conservation des loggings liés pendant une période lui permettant d'assurer la gestion d'un contentieux éventuel, il agit conformément à l'article 4, § 1, 5°, de la LVP.

[5] Voir en ce sens la délibération RN n° 70/2012 du 5 septembre 2012, *relative à la demande de révision de la délibération RN n° 34/2012,* page 5, point 18.

F. Usage interne et/ou communication à des tiers – destinataires éventuels

23. Le numéro de RN sera uniquement utilisé en interne par les membres du personnel du responsable de traitement en charge de la réalisation de finalité précitée. Le Comité souligne par ailleurs qu'il ne peut être fait usage du numéro de Registre national que dans le cadre des applications et/ou services web des responsables de traitement concernés, développés dans le cadre et pour leur(s) mission(s) de service public. Si le numéro de Registre national devait être lié à un numéro en interne par l'organisme concerné, le Comité souligne qu'il ne peut en être ainsi que pour réaliser la finalité précitée. De la même façon, le numéro d'identification au Registre national ne peut être conservé par lesdits responsables de traitement que dans ce cadre.

G. Connexion en réseaux

24. Il ressort des informations obtenues auprès de Fedict que l'utilisation du numéro d'identification du Registre national pour la gestion des utilisateur et des accès n'implique pas de réalisation de connexion réseau.

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

- si des connexions en réseau devaient être réalisées par l'adhérent, il devra en informer le Comité au préalable ;
- le numéro d'identification du Registre national ne peut en tout cas être utilisé dans des relations avec des tiers que pour autant que cela s'inscrive dans le cadre des finalités en vue desquelles ces derniers ont également été autorisés à utiliser ce numéro.

H. Sécurité

H.1. Conseiller en sécurité de l'information

26. Un conseiller en sécurité de l'information est désigné par le responsable de traitement. Celui-ci doit être en mesure d'apprécier en toute indépendance la sécurité de l'information.

27. L'identité de ce conseiller est communiquée au Comité sectoriel du Registre national en même temps que la demande d'adhésion à l'autorisation générale au moyen du questionnaire d'évaluation du candidat conseiller en sécurité.

H.2. Politique de sécurité de l'information

28. Une politique de sécurité est également adoptée en tenant compte notamment des mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel adoptées par la Commission de la protection de la vie privée et disponibles sur son site web. Elle devra être mise en pratique sur le terrain afin que les traitements de données réalisés pour les finalités précitées soient adéquatement sécurisés tant d'un point de vue organisationnel que technique.

29. Toute information utile à ce sujet est communiquée au Comité sectoriel pour le Registre national en même temps que la demande d'adhésion au moyen de la déclaration ad hoc, afin qu'il soit en mesure d'apprécier en toute indépendance la sécurité de l'information.

H.3. Personnes utilisant le numéro d'identification et liste de ces personnes

30. Seuls les membres du personnel de l'adhérent en charge de la réalisation de la finalité visée au point B de la présente délibération pourront utiliser le numéro de Registre national.

H.4. Sous-traitance

31. En cas d'appel aux services d'un sous-traitant pour la réalisation des traitements de données prédécrits, tout bénéficiaire de la présente autorisation unique devra choisir un sous-traitant de qualité et encadrer sa relation avec ce dernier au moyen d'un contrat répondant au prescrit de l'article 16, §1er de la loi vie privée.

I. Gestion des accès et des utilisateurs liée à des rôles/mandats/qualités dont sont titulaires les personnes concernées

32. Les adhérents qui recourent au système FAS de Fedict pour leurs applications informatiques, dont la gestion des accès et des utilisateurs se fait en fonction de rôles/qualités/mandats particuliers dont disposent les personnes concernées, devront utiliser le système GGA géré par Fedict qui fait également partie intégrante de CSAM.. Ceci permettra en effet de vérifier que leur gestion des utilisateurs et des accès se fait en fonction de mandats, qualités ou rôles particuliers dont disposent les personnes concernées quant à l'accès à l'application web dont question.

33. La Commission a par ailleurs jugé qu'un comité sectoriel ne se prononçait pas sur les modalités techniques liées à l'organisation de la gestion des utilisateurs et des accès, pour autant que les principes relatifs à l'organisation de cette gestion et le recours à des sources authentiques soient traités conformément aux bonnes pratiques mises en avant par la Commission dans :

- la recommandation n° 01/2008 du 24 septembre 2008 relative à la gestion des accès et des utilisateurs dans le secteur public ;
- la recommandation d'initiative n° 09/2012 du 23 mai 2012 relative aux sources authentiques de données dans le secteur public ;
- la recommandation d'initiative n° 03/2009 du 1er juillet 2009 concernant les intégrateurs dans le secteur public.

34. Le Comité est d'accord sur le fait que le recours au système GGA doit devenir la norme dans la gestion des utilisateurs et des accès pour les adhérents à la présente délibération, pour des applications d'e-government ou autres applications informatiques développées dans le cadre de missions de service publique, afin de limiter le risque d'accès illégitime aux données. Par conséquent, l'adhérent qui se trouve dans les conditions visées au point 33 de la présente autorisation, doit utiliser le système GGA pour sa gestion des accès.

PAR CES MOTIFS,

le Comité

1° autorise, pour une durée indéterminée, toute autorité publique et organisme visés au considérant 10 ci-dessus qui adressera au Comité l'engagement écrit et signé d'adhérer aux conditions exposées dans la présente délibération, à utiliser le numéro d'identification du Registre national pour réaliser la finalité prédécrite au point B ;

Toute demande en vue de bénéficier de la présente autorisation générale doit, à peine d'irrecevabilité, être adressée au comité du Registre national, dûment signée par le responsable de traitement qui s'engage à remplir les conditions de la présente autorisation générale au moyen du formulaire d'adhésion disponible sur le site web de la Commission accompagné de la déclaration relative à la sécurité et du questionnaire d'évaluation pour le candidat conseiller en sécurité, dûment complétés. Le Comité sectoriel du Registre national, après évaluation, informera l'adhérent de la date à laquelle l'autorisation générale entrera en vigueur dans son chef.

2° stipule que Fedict ne pourra donc rendre le système FAS accessible qu'aux responsables de traitement qui auront satisfait aux exigences développées dans la présente délibération ;

3° stipule que lors de toute modification ultérieure de l'organisation de la sécurité de l'information pouvant avoir un impact sur les réponses données aux questionnaires relatifs à la sécurité fourni au Comité (désignation du conseiller en sécurité et réponses aux questions relatives à l'organisation de la sécurité), les bénéficiaires de la présente autorisation adresseront 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 ;

4° stipule que, lorsqu'il enverra aux bénéficiaires de la présente autorisation un questionnaire relatif à l'état de la sécurité de l'information, ceux-ci devront compléter ce questionnaire conformément à la vérité et le renvoyer au Comité. Ce dernier en accusera réception et se réserve le droit de réagir ultérieurement, s'il y a lieu.

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

(sé) An Machtens (sé) Mireille Salmon
Chef de section OMR f.f.