



Avis n° 16/2019 du 6 février 2019

Objet : projet d'arrêté royal fixant les conditions, la procédure et les conséquences de l'agrément de prestataires de services pour l'échange électronique de messages par le biais de l'eBox (CO-A-2019-002)

L'Autorité de protection des données (ci-après "l'Autorité") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après "la LCA") ;

Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE* (Règlement général sur la protection des données, ci-après "le RGPD") ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

Vu la demande d'avis du SPF Stratégie et Appui (ci-après le "SPF BOSA"), reçue le 20 décembre 2018 ;

Vu le courrier complémentaire du Ministre de l'Agenda numérique, des Télécommunications et de la Poste, chargé de la Simplification administrative, de la Lutte contre la fraude sociale, de la Protection de la vie privée et de la Mer du Nord, reçu le 15 janvier 2019 et vu les informations complémentaires transmises par le SPF BOSA les 17, 18 et 22 janvier 2019 ;

Vu le rapport de Monsieur Frank De Smet ;

Émet, le 6 février 2019, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. En date du 20 décembre 2018, le SPF BOSA a demandé à l'Autorité d'émettre un avis sur un projet d'arrêté royal *fixant les conditions, la procédure et les conséquences de l'agrément de prestataires de services pour l'échange électronique de messages par le biais de l'eBox* (ci-après "le projet d'arrêté royal"). Les 17, 18 et 22 janvier 2019, des informations complémentaires étayant la demande d'avis ont été fournies, à la demande du Secrétariat de l'Autorité.

2. Le projet d'arrêté royal vise à exécuter certaines dispositions du projet de loi *relatif à l'échange électronique de messages par le biais de l'eBox* (ci-après "le projet de loi"), qui est actuellement examiné à la Chambre¹ et à propos duquel le prédécesseur en droit de l'Autorité – à savoir la Commission de la protection de la vie privée (ci-après "la Commission") – a émis son avis n° 47/2018. Le projet de loi crée un cadre légal pour l'échange électronique de messages entre instances publiques et entreprises, citoyens ou autres instances publiques. Il crée également un fondement légal pour la création de deux plateformes pour l'échange électronique de messages² : l'eBox pour les personnes physiques (qui sera proposée par le Service public fédéral compétent pour l'Agenda numérique) et l'eBox pour les titulaires d'un numéro d'entreprise (qui sera proposée par l'Office national de sécurité sociale). En outre, le projet de loi tend à régir la collaboration avec des partenaires privés qui souhaitent rendre ces plateformes accessibles à des utilisateurs et proposer des services complémentaires. L'article 11 du projet de loi dispose notamment que le SPF BOSA peut agréer des "prestataires de services" qui pourront mettre les messages électroniques des utilisateurs à la disposition de personnes physiques. Le deuxième paragraphe de cet article prévoit que le Roi fixera les conditions, la procédure et les conséquences de cet agrément et le projet d'arrêté royal traite spécifiquement de ce volet³.

¹ Voir les documents parlementaires Chambre DOC 54 3442/001.

² Ceci est résumé à la page 1 du Rapport au Roi en ces termes : "*La finalité de l'eBox est d'une part de proposer aux citoyens/entreprises un lieu central, fiable et moderne pour l'échange de messages avec les services publics. D'autre part, l'intention est également de mettre à la disposition des services publics un outil permettant de dématérialiser l'envoi de messages officiels et donc de réduire considérablement les frais postaux (lettres et lettres recommandées)*". [Traduction libre effectuée par le Secrétariat de l'Autorité en l'absence de traduction officielle]

³ La Commission avait d'ailleurs également recommandé au point 38 de son avis n° 47/2018 de régler ces aspects par le biais d'un arrêté d'exécution.

3. Le projet d'arrêté royal comporte six chapitres :
- Le Chapitre I définit les termes utilisés dans le projet d'arrêté royal et explique l'objet du projet d'arrêté royal ;
 - Le Chapitre II contient les conditions auxquelles un prestataire de services doit satisfaire afin d'obtenir un agrément ;
 - Le Chapitre III régit la procédure d'agrément ;
 - Le Chapitre IV porte sur les conséquences de l'agrément du prestataire de services ;
 - Le Chapitre V comprend les dispositions relatives au contrôle, à la suspension et au retrait de l'agrément ;
 - Le Chapitre VI contient plusieurs dispositions finales.
4. Dans le présent avis, l'Autorité se concentre uniquement sur les dispositions du projet d'arrêté royal qui peuvent être améliorées⁴. Le présent avis est aussi émis sous la réserve que les dispositions du projet de loi sur lesquelles le projet d'arrêté royal repose ne subissent plus de modifications significatives.

II. EXAMEN DE LA DEMANDE D'AVIS

A. Remarques transversales

a) Prise de connaissance du contenu des messages par le prestataire de services

5. L'article 11, § 5 du projet de loi⁵ établit le principe selon lequel le prestataire de services d'un service agréé ne prend pas connaissance, dans le cadre du service agréé, du contenu des messages. Il ne peut utiliser le contenu des messages que si cela est strictement nécessaire pour offrir un autre service (un "service à valeur ajoutée") et si l'utilisateur a donné à cette fin son "*accord explicite et préalable*".
6. Au point 36 de son avis n° 47/2018, la Commission avait déjà observé qu'il existait un conflit entre d'une part le principe selon lequel un service agréé ne peut pas avoir connaissance du

⁴ Concernant certains articles du projet d'arrêté royal, il est parfois nécessaire, pour une bonne compréhension et/ou pour une compréhension complète, d'analyser également des dispositions du projet de loi, ce que l'Autorité fait également dans ces cas. Ces références ponctuelles au projet de loi n'impliquent toutefois pas que le présent avis contienne une analyse exhaustive du texte actuel du projet de loi et de sa conformité avec l'avis n° 47/2018.

⁵ "*Le prestataire d'un service agréé ne prend pas connaissance, dans le cadre du service agréé, du contenu des messages échangés par son biais, et n'utilise les messages d'aucune manière, sauf si cela est strictement nécessaire pour offrir le service agréé, comme demandé par l'utilisateur et moyennant son accord explicite et préalable.*"

L'Autorité remarque par ailleurs qu'une erreur s'est glissée dans cette disposition du projet de loi : à la troisième occurrence de la notion de "service agréé", celle-ci doit être remplacée par "service à valeur ajoutée".

contenu d'un message et d'autre part le fait qu'un service agréé pourrait également offrir d'autres services tels que la création automatique d'ordres de paiement. La Commission avait dès lors suggéré que la prise de connaissance dans le chef des prestataires de services agréés offrant un service à valeur ajoutée soit limitée à des métadonnées. Les prestataires de services agréés n'auraient donc jamais accès au contenu des messages. L'Autorité est toutefois déçue de constater qu'à l'article 11, § 5 du projet de loi, l'on a finalement opté pour un autre système. Il a en effet seulement été ajouté à l'article en question que le destinataire doit donner son "*accord explicite et préalable*" avant qu'un prestataire de services puisse utiliser l'intégralité du contenu des messages pour offrir un service à valeur ajoutée.

7. **L'Autorité s'oppose fermement à cette approche. Le fait que l'intégralité du contenu des messages de l'eBox pourra être consultée en vue d'offrir des services à valeur ajoutée est inacceptable.** Elle estime en effet que la comparaison pourrait être faite avec la Poste classique, où les lettres pourraient être ouvertes et lues - moyennant certes une sorte d' "accord" général des personnes concernées - afin de pouvoir proposer des services supplémentaires. Vu le secret de la correspondance ancré dans la Constitution⁶ et la contradiction manifeste avec le principe de minimisation des données, l'Autorité ne peut en aucun cas souscrire à cette approche. Elle redoute d'ailleurs que l' "accord" en question ne sera rien de plus qu'une formalité, le citoyen réalisant à peine ce pour quoi il donne son "accord".
8. À l'instar de la Commission⁷, l'Autorité plaide dès lors pour que les prestataires de services n'aient accès qu'à des métadonnées, et ce uniquement en vue d'être utilisées pour des services à valeur ajoutée, à condition que cela soit également nécessaire pour proposer un tel service et si l' "*accord explicite et préalable*" du destinataire a été obtenu. Les prestataires de services agréés ne pourraient donc jamais accéder au contenu du message proprement dit (aucune fonctionnalité permettant aux prestataires de services de lire ou d'utiliser les messages proprement dits ne peut être prévue, ni pour le service agréé, ni pour les services à valeur ajoutée).
9. L'Autorité attire également l'attention sur le fait que définir précisément les données pouvant être reprises dans les métadonnées, et ce par type de message et par service public, favorisera la prévisibilité de l'accord préalable. Dans le cas contraire, le citoyen comprendra à peine à quelles données le prestataire de services aura accès dans le cadre des services à valeur ajoutée (voir le point 7, *in fine*).

⁶ Voir l'article 29 de la Constitution.

⁷ Voir le point 36 de son avis n° 47/2018.

10. Enfin et à titre subsidiaire, l'Autorité constate que certains passages du (Rapport au Roi du) projet d'arrêté royal peuvent prêter à confusion et demande dès lors de les adapter :
- L'article 3, § 1^{er} du projet d'arrêté royal énonce que les prestataires de services doivent offrir leur service agréé à chaque destinataire *"sans aucune discrimination (...) sur la base du contenu"*. Mais comment un prestataire d'un service agréé pourrait-il discriminer sur la base du contenu s'il ne le connaît pas ?
 - L'article 13 du projet d'arrêté royal dispose que le prestataire de services ne peut pas prendre connaissance du contenu des messages et qu'il ne peut pas les utiliser *"d'une autre manière"*. Cette formulation semble contraire à l'article 11, § 5 du projet de loi qui permet bel et bien de prendre connaissance de l'intégralité du contenu des messages pour des services à valeur ajoutée (ce à quoi l'Autorité s'oppose donc - voir ci-avant le point 7).
 - À la p. 4 du Rapport au Roi du projet d'arrêté royal, on peut lire : *"Le prestataire d'un service agréé ne prend pas connaissance, dans le cadre du service agréé, du contenu des messages échangés par son biais, et n'utilise les messages d'aucune manière, sauf moyennant l'accord explicite préalable de la personne concernée"*. [Traduction libre effectuée par le Secrétariat de l'Autorité en l'absence de traduction officielle]. Cette phrase n'indique pas assez clairement que la première partie se rapporte à la prestation d'un service agréé et la dernière partie à l'offre d'un service à valeur ajoutée (où la connaissance du contenu ne pourrait d'ailleurs porter que sur les métadonnées - voir plus haut le point 8).

b) Délai de conservation

11. L'Autorité constate que le projet d'arrêté royal manque de précision concernant les délais de conservation. Dans ses explications du 18 janvier 2019, le SPF BOSA indiquait que toutes les données seraient détruites en principe au plus tôt 1 mois et au plus tard 2 mois après l'arrêt du service. Le SPF BOSA expliquait que ce délai était dicté par le fait qu'une personne pouvait encore avoir reçu quelque chose juste avant de désactiver le service. Il est en outre possible qu'en cas de décès, le mandataire doive encore pouvoir accéder à certains documents. Le SPF BOSA donnait encore l'explication suivante : *"L'eBox ne contient pas de documents mais des liens vers les documents au niveau des expéditeurs/fournisseurs. Les expéditeurs déterminent le délai pendant lequel le document est disponible. Ensuite, il disparaît. Les documents ne peuvent donc pas être effacés."* [Traduction libre effectuée par le Secrétariat de l'Autorité en l'absence de traduction officielle]. L'Autorité estime que cette explication précitée du SPF BOSA n'est pas cohérente avec les explications du SPF BOSA reprises plus haut concernant le délai de conservation de 1 à 2 mois. Elle demande que des

règles claires en matière de conservation des messages soient définies dans le projet d'arrêté royal.

c) Utilisation du numéro de Registre national

12. L'Autorité observe que tout au long du texte du projet d'arrêté royal, il est question de l'utilisation du "*numéro d'identification unique*" tandis que le Rapport au Roi du projet d'arrêté royal utilise les termes "numéro de Registre national". L'Autorité demande d'utiliser la notion correcte de "numéro de Registre national".

B. Commentaire des articles

a. Article 4

13. L'article 4 du projet d'arrêté royal dispose qu'une organisation qui souhaite être agréée pour offrir un service d'extraction de données doit notamment pouvoir démontrer qu'elle "*offre le service depuis déjà au moins deux ans avant l'introduction de la demande d'agrément, ou dispose déjà de minimum 50.000 destinataires belges*". L'Autorité se demande comment cette condition s'articule avec la condition qu'une organisation doit d'abord être agréée pour pouvoir offrir un service d'extraction de données. Cela ressemble à l'histoire de l'œuf et de la poule. C'est pourquoi l'Autorité demande de clarifier cet aspect dans le Rapport au Roi du projet d'arrêté royal.

b. Article 7

14. L'article 7, § 2 du projet d'arrêté royal énonce que "*(...) l'autorité d'agrément (...) peut offrir au prestataire de services les éventuels messages disponibles dans l'eBox pour une transaction*". Le texte ne permet pas de savoir clairement de quelle manière ces messages seront offerts. En prendra-t-on par ex. une copie ou un accès y sera-t-il accordé ? Il est par contre indiqué à la p. 3 du Rapport au Roi du projet d'arrêté royal que les messages ne seront pas conservés auprès du prestataire de services. Et dans les explications complémentaires fournies par le SPF BOSA le 22 janvier 2019, il est également précisé qu'aucun document ne serait conservé dans l'eBox mais uniquement des liens vers les documents. Compte tenu de ces constatations, l'Autorité demande de mentionner explicitement dans le texte du projet d'arrêté royal que les messages ne seront pas conservés auprès du prestataire de services et de clarifier de quelle façon a exactement lieu le traitement visé à l'article 7, § 2.

c. Article 9

15. L'article 9 du projet d'arrêté royal décrit quels "*contrôles*" le service agréé doit effectuer afin d'éviter des abus. L'Autorité a quelques remarques ponctuelles à ce sujet :

- L'Autorité estime que dans certains cas, les *"contrôles"* énumérés constituent plutôt des *"mesures"*, c'est pourquoi elle recommande d'ajouter ce dernier terme à cette disposition ;
- L'un des *"contrôles"* à effectuer vise à éviter l'abus suivant : *"une tierce partie qui se fait passer pour l'eBox ou pour un prestataire de services"*. L'Autorité considère toutefois qu'il n'appartient pas au prestataire de services agréé mais bien à l'eBox même d'effectuer ces contrôles et elle demande d'adapter le projet d'arrêté royal en ce sens ;
- L'article 9 du projet d'arrêté royal ne traite pas seulement de *"contrôles"* relatifs à l'échange d'informations entre le prestataire de services et l'eBox, mais aussi de transactions entre le prestataire de services et le destinataire (voir la première phrase de l'article 9, § 1^{er}). Néanmoins, cet article se trouve dans la Section 4, dont le titre est le suivant : *"Échange d'informations entre l'eBox et le prestataire de services"*. L'Autorité demande dès lors de lever cette incohérence entre le titre et le texte.

d. Article 12

16. L'article 12 du projet d'arrêté royal dispose que le prestataire de services doit établir une piste d'audit sécurisée *"afin que les données puissent être reconstituées pour chaque transaction spécifique (...)"*. L'Autorité observe que la notion large *"les données"* donne l'impression que dans le cadre de la journalisation, les messages complets seront conservés, ce qui ne peut évidemment pas être le but. L'utilisation d'un terme plus précis s'impose dès lors.
17. Par ailleurs, l'Autorité constate que l'article 12, point 4 du projet d'arrêté royal prévoit que le prestataire de services doit conserver entre autres les éléments suivants : *"(...), les métadonnées du message électronique (...), à savoir le nom du fichier, le type de fichier et la taille du fichier"*. Les informations complémentaires communiquées par le SPF BOSA précisait ceci : *"il s'agit ici de la piste d'audit qui doit être conservée par le prestataire de services. Chaque partenaire de la chaîne prend en charge une partie de la piste d'audit. La partie de l'expéditeur vers le fournisseur de document (intégrateur de services) n'est pas journalisée par le prestataire de services"*. [Traduction libre effectuée par le Secrétariat de l'Autorité en l'absence de traduction officielle]. Cependant, l'Autorité se pose malgré tout encore la question de savoir si les éléments qui seront conservés par le prestataire de services, combinés aux pistes d'audit des autres partenaires de la chaîne, suffisent pour pouvoir "reconstituer" les "transactions spécifiques".

e. Articles 18 & 21

18. Dans le projet d'arrêté royal, on impose aux prestataires de services deux obligations qui, sur le plan terminologique, présentent de fortes ressemblances avec des notions du RGPD, et ce alors que ces obligations sont indépendantes du RGPD. L'article 18 du projet d'arrêté royal impose aux prestataires de services l'obligation notamment de soumettre à l'autorité d'agrément une *"analyse d'impact"* à chaque fois qu'ils souhaitent introduire une nouvelle version logicielle et l'article 21 du projet d'arrêté royal oblige les prestataires de services à avertir l'autorité d'agrément des violations de la sécurité. L'article 18 du projet d'arrêté royal fait penser à l'analyse d'impact relative à la protection des données prévue aux articles 35 & 36 du RGPD, tandis que l'article 21 du projet d'arrêté royal présente des similitudes terminologiques avec la notification d'une violation de données à caractère personnel telle que prévue aux articles 33 & 34 du RGPD. Afin d'éviter toute confusion entre ces notions du RGPD et le texte du projet d'arrêté royal, l'Autorité demande de bien expliquer la différence entre les deux dans le Rapport au Roi du projet d'arrêté royal.

f. Article 36

19. L'article 36 du projet d'arrêté royal décrit six situations dans lesquelles le prestataire de services doit confirmer à l'autorité d'agrément qu'il satisfait toujours aux conditions d'agrément. Le point 3 de l'article 36 indique que le prestataire de services doit effectuer la confirmation susmentionnée *"avant une modification du contrôle du prestataire de services qui peut avoir un impact sur le service"*. On ne sait pas clairement ce qu'il convient d'entendre par *"modification du contrôle"*. Dans ses explications du 17 janvier 2019, le SPF BOSA avait donné à ce propos l'exemple suivant : *"Le prestataire de services est repris par une autre entreprise qui ne considère plus ce type de prestation de services comme stratégique"*. [Traduction libre effectuée par le Secrétariat de l'Autorité en l'absence de traduction officielle]. Compte tenu de cet exemple, l'Autorité estime que la partie de phrase *"modification du contrôle"* n'exprime pas bien ce qui est exactement visé.

PAR CES MOTIFS

l'Autorité invite le SPF BOSA à tenir compte des remarques et des recommandations formulées ci-avant, lesquelles peuvent se résumer comme suit :

- ne pas laisser les prestataires de services prendre connaissance du contenu intégral des messages mais uniquement des métadonnées (points 5 à 9 inclus) ;
- prévoir des règles claires en matière de délais de conservation (point 11) ;

- tout au long du texte du projet d'arrêté royal, utiliser la notion de "numéro de Registre national" (point 12) ;
- retravailler les articles 4, 7, 9, 12, 18, 21 & 36 du projet d'arrêté royal, comme exposé aux points 13 à 19 inclus.

(sé) An Machtens
Administrateur f.f.

(sé) Willem Debeuckelaere
Président,
Directeur du Centre de connaissances