Avis n° 18/2017 du 12 avril 2017

Objet : projet d'arrêté royal fixant les conditions, la procédure et les conséquences de l'agrément de services d'identification électronique pour applications publiques numériques (CO-A-2017-008)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

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 29 ;

Vu la demande d'avis de Monsieur Jan DEPREST, Président du Service public fédéral ICT, reçue le 10 février 2017 ;

Vu le rapport de Monsieur Ivan VANDERMEERSCH ;

Émet, le 12 avril 2017, l'avis suivant :

La Commission attire l'attention sur le fait qu'une nouvelle réglementation européenne relative à la protection des données à caractère personnel a été promulguée récemment : le Règlement général 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 la Directive Police et Justice. Ces textes ont été publiés au journal officiel de l'Union européenne le 4 mai 2016[1].

Le Règlement, couramment appelé GDPR (General Data Protection Regulation ou RGPD pour Règlement général sur la protection des données), est entré en vigueur vingt jours après sa publication, soit le 24 mai 2016, et est automatiquement applicable deux ans plus tard, soit le 25 mai 2018. La Directive Police et Justice doit être transposée dans la législation nationale au plus tard le 6 mai 2018.

Pour le Règlement, cela signifie que depuis le 24 mai 2016, pendant le délai d'exécution de deux ans, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part aussi une obligation négative, appelée "devoir d'abstention". Cette dernière obligation implique l'interdiction de promulguer une législation nationale qui compromettrait gravement le résultat visé par le Règlement. Des principes similaires s'appliquent également pour la Directive.

Il est dès lors recommandé d'anticiper éventuellement dès à présent ces textes. Et c'est en premier lieu au(x) demandeur(s) de l'avis qu'il incombe d'en tenir compte dans ses (leurs) propositions ou projets. Dans le présent avis, la Commission a d'ores et déjà veillé, dans la mesure du possible et sous réserve d'éventuels points de vue complémentaires ultérieurs, au respect de l'obligation négative précitée.

---

[1] 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)*

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil*

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC.)

I. CONTEXTE

1. Le projet d'arrêté royal fixant les conditions, la procédure et les conséquences de l'agrément de services d'identification électronique pour applications publiques numériques, ci-après le projet, vise à exécuter l'article 12 de la loi en matière d'identification électronique - qui doit encore être promulguée. L'avant-projet de loi relative à l'identification électronique, ci-après l'avant-projet de loi, fait l'objet de l'avis n° 48/2016 de la Commission du 21 septembre 2016. Le 16 février 2017, une nouvelle version de l'avant-projet de loi datant du 20 décembre 2016 a été communiquée, soit après l'avis de la Commission.

2. Le projet s'inscrit dans le cadre du volet de l'avant-projet de loi qui, en ce qui concerne la Belgique, étaie juridiquement l'identification électronique pour applications publiques, dont l'agrément de services d'identification électronique. L'article 12 de l'avant-projet de loi offre la possibilité d'accéder à des applications publiques numériques sur la base d'un service d'identification électronique, fourni par des acteurs qui ne sont pas des instances publiques.

3. L'identification électronique se fait via des systèmes numériques et va de pair avec le traitement automatisé de données à caractère personnel. Les dispositions de la LVP sont donc applicables. L'analyse se limite aux articles qui concernent le traitement de données à caractère personnel.

II. EXAMEN QUANT AU FOND

Remarque préalable

4. Ce sont les gestionnaires d'applications publiques numériques qui sont les responsables du traitement au sens de l'article 1, § 4 de la LVP. Conjointement avec les sous-traitants auxquels ils ont recours, ils doivent garantir la sécurité des données à caractère personnel à l'aide de mesures techniques et organisationnelles requises (article 16, § 4 de la LVP).

5. Le rôle de Fedict (le service public fédéral Technologie de l'Information et de la Communication, repris depuis le 1er mars 2017 dans le Service public fédéral Stratégie et Appui[1]) est notamment d'exploiter un service commun d'authentification ("Federal Authentication Service" ou "FAS"). Ce service constitue une base essentielle pour permettre aux administrations, aux citoyens et aux entreprises d'utiliser dans la pratique les technologies de l'information et de la communication pour des applications publiques numériques.

[1] Arrêté royal du 22 février 2017 *portant création du Service public fédéral Stratégie et Appui*.

6. La Commission déduit du projet que lorsque Fedict fournit un agrément à un prestataire de services, selon le cas pour une option d'identification avec le niveau élevé ou le niveau substantiel, le service d'authentification agréé est automatiquement repris dans ce niveau dans le FAS. Concrètement, cela impliquerait que toutes les applications publiques numériques qui utilisent le FAS doivent alors accepter automatiquement cette option d'identification agréée pour leurs applications classées dans le niveau correspondant (substantiel ou élevé).

7. La Commission reconnaît qu'une analyse approfondie par Fedict offre des garanties en matière de sécurité à un certain niveau des options d'identification agréées. Dans le même temps, la Commission constate que les gestionnaires d'applications publiques numériques n'ont officiellement qu'une seule occasion d'adopter un point de vue dans la procédure, plus précisément dans le cadre de la consultation du Collège des présidents des services publics fédéraux et des services publics de programmation, du Collège des administrateurs délégués des institutions de sécurité sociale et du Collège des administrateurs délégués des organismes d'intérêt public fédéraux, avant l'agrément (art. 12 de l'avant-projet de loi). Inévitablement, la question se pose alors de savoir si les gestionnaires d'applications publiques numériques, sur la base d'une analyse des risques et, dans certains secteurs, en concertation avec les utilisateurs des services, conservent encore la possibilité de décider quelles options d'identification agréées ils acceptent dans un contexte déterminé. La nature des données à sécuriser et des risques potentiels est en effet explicitement mentionnée à l'article 16, § 4 de la LVP lors de la définition des mesures de sécurité à prendre. La question se pose par ailleurs de savoir si le projet tient suffisamment compte de l'article 28(2) du RGPD qui est libellé comme suit :

> "*Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.*"

8. L'obligation de sécurité qui repose sur le responsable du traitement tient également compte de l'état de la technique en la matière et des frais qu'entraîne l'application des mesures (art. 16, § 4 de la LVP). La Commission constate toutefois que le gestionnaire de l'application publique numérique ne reçoit dans le projet aucune certitude quant aux conséquences financières de l'agrément d'une option d'identification. Le projet prévoit que l'utilisation de l'option d'identification est gratuite pour l'utilisateur (art. 42 du projet). Pour le reste, il délègue au ministre compétent pour l'Agenda numérique la compétence de fixer un modèle d'indemnité pour couvrir les frais engendrés afin d'établir la connexion au service fédéral d'authentification. Le projet devrait au moins apporter des éclaircissements quant à savoir si l'indemnité susmentionnée signifie l'indemnité unique pour

l'utilisation de cette option d'identification agréée, avec la certitude que l'on n'attend pas de contribution supplémentaire des gestionnaires d'applications publiques, et ce quel que soit le nombre de transactions effectuées avec leur application. À défaut de certitude à ce sujet, le risque est réel que des gestionnaires préfèrent des options d'identification non-agréées – dont les frais sont calculables à l'avance – à des options d'identification agréées qui garantissent un niveau minimum de sécurité, mais dont les frais ne peuvent pas être estimés. Cela saperait la finalité du projet.

9. En sus de tout ce qui précède, il faut par ailleurs noter que le FAS n'est pas uniquement utilisé par des services publics au sens strict mais aussi par d'autres acteurs dans certains secteurs qui sont fréquemment en contact avec des applications publiques numériques (par ex. dans le secteur social, le secteur de la santé, les avocats, ...).

Article 8 du projet

10. L'article 8 du projet renvoie, pour la procédure d'enregistrement, aux exigences pour la preuve et la vérification d'identité décrites au point 2.1.2. de l'annexe au règlement d'exécution (UE) n° 2015/1502.

11. Il importe que les services d'authentification agréés se basent sur des procédures d'enregistrement solides. Les procédures d'enregistrement qui sont basées sur la vérification de l'identité à l'aide de l'eID répondent parfaitement aux exigences susmentionnées. Une très large majorité des personnes qui ont besoin d'un accès à des services publics disposent d'une eID.

12. Le règlement d'exécution (UE) n° 2015/1502 n'impose ni pour le niveau élevé, ni pour le niveau substantiel que l'on ait recours à l'eID. Afin de susciter un niveau similaire de confiance parmi les utilisateurs, le projet doit imposer pour les procédures d'enregistrement sans utilisation de l'eID (c'est-à-dire soit par la personne concernée elle-même, soit via un intermédiaire) des exigences plus spécifiques que celles décrites au point 2.1. de l'annexe au règlement d'exécution (UE) n° 2015/1502 par niveau – élevé ou substantiel. La Commission estime en particulier que dans de tels cas, la responsabilité de l'autorité d'enregistrement doit être clairement définie dans les conditions d'agrément.

Articles 9 et 10 du projet

13. L'article 9 du projet garantit la liberté pour l'utilisateur de choisir de modifier son choix relatif au service d'identification électronique ou d'y mettre fin. L'article 10 ajoute à cela que le choix d'un service d'identification électronique agréé déterminé n'empêche pas l'utilisateur d'utiliser également d'autres services.

14. La Commission attire l'attention sur le fait que cette liberté de choix ne peut être exercée effectivement que dans la mesure où l'autorité propose des options d'identification pratiques pour accéder aux applications publiques numériques. La Commission estime qu'il n'est en effet pas approprié de lier les utilisateurs à un service déterminé.

Article 11 du projet

15. L'article 11 du projet dispose que :

> *"Lors de chaque identification, le service d'identification électronique envoie à l'autorité d'agrément le numéro d'identification unique de l'utilisateur, sur la base duquel l'autorité d'agrément détermine l'identité de l'utilisateur.*"

16. Le numéro d'identification unique est soit le numéro de Registre national, soit le numéro de la Banque-carrefour, selon l'Exposé des motifs. L'article 4, § 1er de la loi du 5 mai 2014 relative à la collecte unique des données[2] oblige les instances fédérales à utiliser, dans le cadre de l'exécution de leurs missions, le numéro de Registre national pour l'identification des personnes physiques. Les personnes qui ne disposent pas d'un numéro de Registre national peuvent se voir attribuer un numéro de la Banque-carrefour.

17. Bien que l'article 12, § 2 de l'avant-projet de loi charge le Roi de déterminer la procédure, les conditions et les conséquences relatives à l'agrément, certains aspects sont régis de manière univoque au § 5 de l'article 12 de l'avant-projet de loi. Tout d'abord, il est explicitement précisé que le fournisseur d'un service d'identification électronique agréé, en raison de son agrément, est autorisé, en sa qualité de sous-traitant de Fedict, à utiliser le numéro de Registre national. L'avant-projet de loi instaure dès lors une exception légale à l'article 8 de la loi du 8 août 1983 *organisant un registre national des personnes physiques* qui dispose que l'autorisation d'utiliser le numéro de Registre national est accordée par le Comité sectoriel du Registre national.

18. La définition de la finalité pour laquelle le service d'identification électronique agréé peut utiliser le numéro d'identification unique est mentionnée à l'article 17 du projet.

Article 12 du projet

19. L'article 12 du projet dispose ce qui suit :

---

[2] Loi du 5 mai 2014 *garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier*.

"Dans le cadre du service d'identification électronique, l'échange d'informations entre le prestataire de services et l'autorité d'agrément se déroule conformément aux protocoles techniques exposés dans les spécifications techniques."

20. La Commission estime que les spécifications techniques doivent définir des exigences appropriées pour la sécurisation de l'échange d'informations (conformément à l'article 16, § 4 de la LVP[3]).

Article 13 du projet

21. Le projet impose au prestataire de services de prendre des mesures en matière de sécurisation de l'option d'identification. Trois risques spécifiques en matière de sécurité sont cités.

"*§ 1er. Lors de chaque échange d'informations entre l'autorité d'agrément et le prestataire de services, ainsi qu'entre le prestataire de services et l'utilisateur, le service d'identification électronique effectue des contrôles afin d'éviter, au moins, les abus suivants :*

1. le nouvel envoi d'un même message ou d'une même tentative d'identification ;

2. la modification du contenu des informations échangées ;

3. une tierce partie qui se fait passer pour le service opérationnel ou le prestataire de services.

§ 2. Les abus mentionnés au paragraphe 1er sont détectés et mènent à l'échec de l'identification.

§ 3. Le service d'identification électronique comprend suffisamment de mécanismes de contrôle afin de détecter pro-activement des risques éventuels en matière de sécurité. Le prestataire de services établit des rapports à ce sujet conformément à la procédure décrite à la sous-section 5 de la section 2."

22. Les termes "risques en matière de sécurité" comprennent les "*attaques ; effractions, tant physiques qu'électroniques ; dommages à la réputation et à l'image et tout préjudice éventuel qui peut avoir des conséquences négatives sur la prestation de services*" (article 1er, 13° du projet).

23. Là où l'article 33 du RGPD en matière de "notification d'une violation de données à caractère personnel" s'applique, le prestataire de services devra également effectuer certaines notifications à

[3] L'article 16, § 4 de la LVP dispose que "*Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.*"

l'autorité de contrôle, outre l'obligation de notification à l'autorité d'agrément (article 25 du projet). La Commission constate que la notion de "risques en matière de sécurité" chevauche au moins partiellement celle de "violation de données à caractère personnel", c'est-à-dire "*une violation de la sécurité* (dans le sens d'incident) *entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données*" (article 4, point 12 du RGPD).

24. Le renvoi aux dommages à la réputation et à l'image dans la définition des risques en matière de sécurité indique clairement que le but du projet est notamment de préserver la confiance des utilisateurs et des services publics qui utilisent le service.

25. La conservation des fichiers de journalisation constitue une mesure visant à permettre d'établir des rapports sur la mesure dans laquelle les risques en matière de sécurité se sont réalisés - concrètement lorsque la détection d'un abus a conduit à l'échec de l'identification (article 13, § 2 du projet). La Commission constate toutefois que l'obligation de conserver des pistes d'audit vaut exclusivement pour les transactions, c'est-à-dire toute identification réussie au moyen d'un service agréé d'identification électronique. Ces pistes d'audit doivent être conservées pendant 10 ans (article 16, § 2 du projet), un délai qui, selon l'Exposé des motifs, se base sur les délais de prescription de droit commun.

26. La Commission estime que l'autorité d'agrément doit conclure des accords dans un accord de coopération avec les prestataires de services sur la conservation des pistes d'audit d'identifications ayant échoué en vue de gérer les risques en matière de sécurité.

Article 14 du projet

27. L'article 14 du projet est libellé comme suit :

> *"Le prestataire de services n'utilise les données à caractère personnel que pour la prestation de services. Le prestataire de services traitera les données à caractère personnel conformément à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, aux arrêtés d'exécution et aux directives et recommandations de la Commission de la protection de la vie privée ainsi qu'au Règlement européen (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*."

28. La première phrase impose une limitation au traitement de données à caractère personnel par les prestataires de services qui, à première vue, est plus stricte que l'article 4, § 1, 2° de la LVP. Le projet vise à permettre aux prestataires de services d'également utiliser les options d'identification qu'ils ont mises au point pour l'accès à leurs propres services pour leurs utilisateurs en tant qu'option d'identification, pour l'accès à des applications publiques numériques. Les prestataires de services disposent de données à caractère personnel de leurs utilisateurs qu'ils utilisent pour des finalités déterminées, explicites et légitimes (voir l'article 4, § 1, 2° de la LVP), le cas échéant, il s'agit d'une ou de plusieurs finalités commerciales. Par définition, dans ce cas, les prestataires de services n'utiliseront pas exclusivement les données à caractère personnel qu'ils traitent lors de chaque utilisation de l'option d'identification pour *"le service garantissant l'identité de l'utilisateur qui tente d'accéder à des applications publiques numériques sur la base d'une option d'identification*", mais également pour leurs propres finalités.

29. Afin d'être cohérent avec la finalité du projet, la Commission demande que cette disposition soit réécrite, de manière à ce qu'il soit clair que seules les données à caractère personnel exclusivement collectées dans le cadre de la fourniture du service d'identification électronique peuvent également exclusivement être utilisées par la suite pour la prestation de services.

30. Le renvoi explicite, à la deuxième phrase de l'article, à la LVP et au RGPD sert uniquement à conscientiser les prestataires de services. Il va de soi que les prestataires de services doivent respecter la réglementation applicable à leur activité - à savoir la loi du 8 août 1983 *organisant un registre national des personnes physiques* qui régit l'utilisation du numéro de Registre national -, qu'il y soit fait référence explicitement ou non.

Article 15 du projet

31. L'article 15 du projet renvoie aux mécanismes visant à protéger les données à caractère personnel comme décrit au point 2.3.1 de l'annexe au règlement d'exécution (UE) n° 2015/1502, mais omet de spécifier que le prestataire de services a le choix entre le niveau substantiel ou élevé (en comparaison avec les articles 5, 6 et 8 du projet).

Article 16 du projet

32. L'article 16, § 1er du projet dispose ce qui suit :

> *"Le prestataire de services ne prend pas connaissance des applications publiques numériques auxquelles l'utilisateur demande l'accès à l'aide du service d'identification électronique*."

33. Cette disposition doit être lue conjointement avec les articles 33 et 35 du projet.

"*Art. 33. Lors de l'identification de l'utilisateur sur une application publique numérique, le service fédéral d'authentification connecte l'utilisateur au service d'identification électronique agréé choisi par l'utilisateur.*

Art. 35. Le fournisseur d'un service d'identification électronique agréé utilise le numéro d'identification unique pour offrir, par le biais du portail d'accès de l'autorité d'agrément, le service d'identification électronique agréé."

34. Il en découle que le service d'authentification fédéral (régi à l'article 11 de l'avant-projet de loi), veille, en tant qu'intermédiaire, à ce que le prestataire de services ne soit pas informé de l'application publique numérique à laquelle l'utilisateur souhaite accéder. Il résulte de l'article 35 du projet qu'après une identification réussie, le prestataire de services communique ce fait, couplé au numéro d'identification unique, au service d'authentification fédéral qui, à son tour, répercute ce fait à l'application publique numérique.

35. L'article 16, § 2 du projet dispose que :

"Le prestataire de services établit une piste d'audit sécurisée afin que les données puissent être reconstituées pour chaque transaction spécifique, et ce, en vue de la sécurisation des données et de la protection de la vie privée. À cet effet, le prestataire de services conserve, pour chaque identification, les données suivantes, et ce, pour une durée de dix ans à compter du moment de ladite identification :

1. les nom et prénom de l'utilisateur qui s'identifie ;

2. le numéro d'identification unique de l'utilisateur ;

3. le service d'identification électronique du prestataire de services avec lequel l'utilisateur s'identifie ; et

4. le moment de l'identification."

36. L'intérêt des fichiers de journalisation a déjà été précisé précédemment au point 16. En ce qui concerne le contenu des pistes d'audit d'identifications réussies, la Commission part du principe que la notification obligatoire des "*nom et prénom de l'utilisateur qui s'identifie*" suppose que chaque option d'identification traite les nom et prénom de l'utilisateur lors de chaque tentative d'identification. Les prestataires de services qui utilisent d'autres données (adresse e-mail, numéro de gsm, numéro de compte bancaire, ...) pour identifier leurs utilisateurs dans le processus d'identification sont obligés de reprendre en plus systématiquement les nom et prénom dans la piste d'audit. La Commission estime que sur ce point, la formulation du projet est disproportionnée. Ici, le projet va plus loin que la conservation de l'identifiant que l'utilisateur a effectivement utilisé pour s'identifier. En outre, le service d'authentification fédéral peut retrouver les nom et prénom de la personne concernée à l'aide du numéro d'identification unique. Le numéro d'identification unique suffit pour cette finalité.

Article 17 du projet

37. L'article 17 du projet dispose ce qui suit :

"*Le prestataire de services prend des mesures afin de garantir que le numéro d'identification unique de l'utilisateur n'est utilisé que pour la finalité de l'identification électronique par le biais du portail d'accès de l'autorité d'agrément.*"

38. Les prestataires de services qui souhaitent être agréés doivent dès lors offrir des garanties qu'ils n'utiliseront pas pour d'autres finalités commerciales les données à caractère personnel qu'ils ont collectées en vue de la finalité pour laquelle ils sont agréés.

39. Vu que l'avant-projet de loi régit l'utilisation du numéro de Registre national, il faut supprimer du préambule le renvoi superflu à "*la loi du 8 août 1983 organisant un registre national des personnes physiques, article 8, § 1er, alinéa 2*". Ce renvoi doit également être supprimé dans le rapport au Roi.

Articles 21 et 22 du projet

40. Les articles 21 et 22 du projet contiennent un règlement concernant le déploiement de nouvelles versions du logiciel par le prestataire de services agréé. En la matière, le prestataire de services agréé doit conclure des accords avec l'autorité d'agrément.

41. L'article 22 du projet dispose :

"*Le prestataire de services soumet à l'approbation de l'autorité d'agrément chaque nouvelle version logicielle qui a un impact significatif sur l'utilisateur, au plus tard un mois avant la date d'introduction du déploiement, et l'accompagne d'une analyse d'impact.*"

42. Des modifications dans les spécifications techniques des options d'identification agréées peuvent avoir un impact sur les applications publiques numériques qui les utilisent via le FAS. Étant donné que les prestataires de services agréés ne peuvent pas savoir pour quelles applications publiques numériques l'option d'identification qu'ils fournissent est utilisée, l'autorité d'agrément doit veiller à ce qu'il n'y ait aucun impact découlant de modifications techniques. La Commission estime que le projet doit élaborer les garanties nécessaires à cet effet.

Article 23 du projet

43. L'article 23 du projet dispose :

> "*Le prestataire de services développe des mécanismes qui garantissent un service ininterrompu pendant la durée de l'agrément.*"

44. Le projet reconnaît l'importance de la continuité du service pendant la période d'agrément, par contre, il ne contient aucun règlement pour la période qui suit la fin de l'agrément. Les situations qui sont ici visées concernent à la fois celles dans lesquelles le prestataire de services décide lui-même de mettre fin au service et celles dans lesquelles l'agrément est suspendu ou retiré. Dans certaines circonstances, l'arrêt soudain d'un service peut être inévitable. Toutefois, la Commission estime que l'autorité d'agrément doit établir dans les conditions d'agrément que les scénarios d'arrêt progressif sont la règle. Ainsi, les utilisateurs d'options d'identification ne sont pas subitement mis devant le fait accompli et peuvent graduellement passer à d'autres services. Le gestionnaire de l'application publique numérique a aussi ainsi la possibilité de prendre des mesures transitoires si nécessaire. Le scénario d'arrêt progressif recommandé dépend du contexte.

Article 27 du projet

45. L'article 27 du projet énumère les cas où le demandeur d'une procédure d'agrément peut être exclu ou le prestataire de services perdre l'agrément, notamment s'il *"a fait l'objet d'une condamnation prononcée par une décision judiciaire ayant force de chose jugée pour toute infraction à la législation relative à la protection de la vie privée*."

46. Dans ce cadre, on perd de vue qu'en vertu du RGPD (articles 58.2 et 83), la Commission aura le pouvoir d'imposer des sanctions administratives. Dans de tels cas, une suspension ou un retrait de l'agrément est également envisageable. La Commission estime qu'un renvoi à ce pouvoir doit être ajouté.

Remarque terminologique

47. Le projet utilise à plusieurs endroits les termes 'vie privée' alors que l'arrêté royal vise à encadrer le traitement de données à caractère personnel, d'après le renvoi, à l'article 14, à la LVP et au RGPD. Étant donné que le projet concerne un règlement en matière de traitement de données à caractère personnel, la Commission demande que la terminologie soit adaptée en conséquence.

PAR CES MOTIFS

la Commission

émet un avis **favorable** à condition qu'il soit tenu compte des remarques qu'elle a formulées aux points 7, 8, 9, 12, 20, 26, 31, 36, 39, 42, 44, 46 et 47.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere