Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 35/2025 du 19 mai 2025

Objet : un avant-projet de loi *rétablissant l'article 31bis des lois sur le Conseil d'État, coordonnées le 12 janvier 1973, pour ce qui concerne la procédure électronique devant la section du contentieux administratif du Conseil d'État* (CO-A-2025-024)

Mots-clés : délai de conservation différencié - fichiers de journalisation - journalisation - connexion - données de journalisation - Breyer - Digital Platform for Attorneys (DPA) - terme 'connexion' - spécification des personnes concernées et corrélation avec la mission fonctionnelle

Traduction

Introduction :

L'avis concerne les articles 1er à 4 inclus d'un avant-projet de loi *rétablissant l'article 31bis des lois sur le Conseil d'État, coordonnées le 12 janvier 1973, pour ce qui concerne la procédure électronique devant la section du contentieux administratif du Conseil d'État*.

L'avant-projet de loi vise à rétablir l'article 31*bis* des lois coordonnées sur le Conseil d'État en vue d'introduire une base légale pour la création d'une plate-forme électronique et des traitements de données connexes qui en découlent.

L'Autorité formule en particulier des remarques concernant le délai maximal de conservation des différents types de données énumérés dans l'avant-projet de loi. Une attention particulière doit également être accordée à plusieurs aspects relevant de la minimisation des données, qui d'une part requièrent de petites adaptations et d'autre part sont fondamentalement remis en cause.

Pour la liste complète des remarques, il est renvoyé au dispositif.

Le Service d'Autorisation et d'Avis de 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 de Monsieur Bernard Quintin, Ministre de la Sécurité et de l'Intérieur, chargé de Beliris (ci-après : le "demandeur"), reçue le 24 mars 2025 ;

Vu les explications complémentaires quant au contenu, reçues le 16 avril 2025 ;

Émet, le 19 mai 2025, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. Le 24 mars 2025, le demandeur a sollicité l'avis de l'Autorité concernant un avant-projet de loi *rétablissant l'article 31bis des lois sur le Conseil d'État, coordonnées le 12 janvier 1973, pour ce qui concerne la procédure électronique devant la section du contentieux administratif du Conseil d'État* (ci-après : le "Projet").

2. Le Projet vise le rétablissement de l'article 31*bis* des lois coordonnées sur le Conseil d'État et donne une base légale explicite à la création et à l'utilisation d'une plate-forme électronique permettant au Conseil d'État de recourir à une procédure électronique pour gérer les recours qui lui sont soumis et ainsi exécuter la mission d'intérêt public dont il est investi par l'article 160 de la *Constitution*.

3. L'Autorité note - sur la base des explications complémentaires du demandeur - que l'intention est de remplacer l'article 85*bis* de l'arrêté du Régent du 23 août 1948 *déterminant la procédure devant la section du contentieux administratif du Conseil d'État* (ci-après : le règlement de procédure du Conseil d'État), qui régit le fonctionnement de la procédure électronique. L'Autorité rappelle qu'en

vertu de l'article 46, § 1er du règlement d'ordre intérieur de l'Autorité de protection des données, elle examine uniquement les projets normatifs dans leur stade final de rédaction, à savoir après qu'ils ont été approuvés par le gouvernement de l'entité fédérée concernée ou le Conseil des ministres, si une telle approbation est requise. À la lumière de cet élément, - bien que de possibles adaptations futures auront été prises en considération, c'est-à-dire des définitions, voir ci-dessous - l'Autorité ne peut pas, dans le cadre du présent avis, se prononcer quant au contenu du nouveau projet d'arrêté royal *modifiant la procédure électronique devant la section du contentieux administratif du Conseil d'État*, celui-ci n'ayant actuellement encore fait l'objet d'aucune demande d'avis.

II. EXAMEN QUANT AU FOND

a. Base juridique

4. *Rappel des principes* : Chaque traitement de données à caractère personnel doit avoir une base juridique ou de licéité, comme le prévoit l'article 6, paragraphe 1 du RGPD. Les traitements de données qui sont instaurés par une mesure normative sont presque toujours basés sur l'article 6, paragraphe 1, point c) ou e) du RGPD[1]. Le lecteur est renvoyé à l'application de ces principes telle que définie ci-après.

5. **En plus de devoir être nécessaire et proportionnée**, toute norme régissant le traitement de données à caractère personnel (et constituant par nature une ingérence dans le droit à la protection des données à caractère personnel) **doit répondre aux exigences de prévisibilité et de précision afin que les personnes concernées au sujet desquelles des données sont traitées aient une idée claire du traitement de leurs données**. En vertu de l'article 6.3 du RGPD, lu en combinaison avec les articles 22 de la *Constitution* et 8 de la CEDH, une telle norme légale doit décrire les éléments essentiels des traitements allant de pair avec l'ingérence de l'autorité publique :
   - la (les) finalité(s) précise(s) et concrète(s) des traitements de données ;
   - la désignation du (des) responsable(s) du traitement (à moins que cela ne soit clair).

   Si les traitements de données à caractère personnel allant de pair avec l'ingérence de l'autorité publique représentent une ingérence importante dans les droits et libertés des personnes

[1] Article 6, paragraphe 1 du RGPD : "*Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : (...)*

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; (…)

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; (...)."

concernées, conformément aux principes de légalité et de prévisibilité, la disposition légale en la matière doit également comprendre les éléments essentiels (complémentaires) suivants :[2]

- les (catégories de) données à caractère personnel traitées qui sont pertinentes et non excessives ;
- les catégories de personnes concernées dont les données à caractère personnel seront traitées ;
- les (catégories de) destinataires des données à caractère personnel ainsi que les circonstances dans lesquelles ils reçoivent les données et les motifs y afférents ;
- le délai maximal de conservation des données à caractère personnel enregistrées ;
- l'éventuelle limitation des obligations et/ou des droits visé(e)s aux articles 5, 12 à 22 et 34 du RGPD.

6. *Application concrète :* le traitement de données à caractère personnel auquel le présent Projet soumis pour avis donne lieu repose sur l'article 6.1.e) du RGPD[3]. Considérant que le Projet implique un traitement de données à caractère personnel : *i) qui porte sur des catégories particulières de données à caractère personnel (données sensibles) au sens des articles 9 et/ou 10 du RGPD et/ou sur des données hautement personnelles ; ii) qui a lieu à des fins de surveillance ou de contrôle*[4] *; iii) au cours duquel les données sont communiquées ou accessibles à des tiers*[5] *; iv) qui prévoit l'utilisation du numéro de Registre national,* , l'Autorité estime qu'il s'agit **en l'occurrence d'une ingérence importante**.

7. L'Autorité vérifie ci-après dans quelle mesure le Projet répond à ces conditions.

b. Finalités

8. Conformément à l'article 5.1.b) du RGPD, le traitement de données à caractère personnel ne peut être effectué que pour des finalités déterminées, explicites et légitimes.

9. À cet égard, le projet d'article 31*bis*, § 1er, alinéa 1er précise : "*Le Conseil d'État crée et gère une plate-forme électronique qu'il met à la disposition des parties pour l'introduction et la gestion des procédures contentieuses portées devant lui.*" Lu conjointement avec l'article 85*bis* du règlement

---

[2] Voir DEGRAVE, E., "*L'e-gouvernement et la protection de la vie privée – Légalité, transparence et contrôle*", Collection du CRIDS, Larcier, Bruxelles, 2014, p. 161 e.s. (voir e.a. : Cour européenne des droits de l'homme, Arrêt *Rotaru c. Roumanie*, 4 mai 2000) ; Voir également quelques arrêts de la Cour constitutionnelle : l'Arrêt n° 44/2015 du 23 avril 2015 (p. 63), l'Arrêt n° 108/2017 du 5 octobre 2017 (p. 17) et l'Arrêt n° 29/2018 du 15 mars 2018 (p. 26).

[3] Article 6.1.e) du RGPD : "*le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.*"

[4] Données de journalisation.

[5] Compte tenu des dispositions du projet d'arrêté royal *modifiant la procédure électronique devant la section du contentieux administratif du Conseil d'État* qui doit encore être soumis à l'avis de l'Autorité et doit encore être voté.

de procédure du Conseil d'État, plusieurs actes relèvent de ces procédures. Le demandeur a fourni les explications suivantes à ce sujet :

> "Comme indiqué à l'article 31*bis*, alinéa 3, l'introduction et la gestion des procédures contentieuses portées devant le Conseil d'État implique le dépôt, par les parties au litige, de différents actes de procédure accompagnés, le cas échéant de pièces qui y sont annexées.
>
> Ces actes de procédure varient en fonction des procédures et du déroulement de celles-ci et il est donc complexe d'en dresser une liste complète. Ces actes sont toutefois mentionnés dans les lois coordonnées sur le Conseil d'État ainsi que dans les divers arrêtés royaux qui déterminent les procédures applicables devant le Conseil d'État (principalement : le règlement général de procédure, l'arrêté royal du 19 novembre 2024 déterminant la procédure en référé […], ainsi que l'arrêté royal du 30 novembre 2006 déterminant la procédure en cassation devant le Conseil d'État).
>
> À titre d'exemple, nous pouvons toutefois détailler les actes de procédure déposés par les parties à l'occasion d'une procédure en annulation "classique" (sans incidents de procédure et sans mise en œuvre d'une procédure abrégée) :
>
> 1) La partie requérante dépose une requête en annulation.
> 2) La partie adverse prend connaissance de la requête en annulation, dépose le dossier administratif lié à l'acte attaqué ainsi qu'un mémoire en réponse.
> 3) La partie requérante prend connaissance du mémoire en réponse et dépose un mémoire en réplique.
> 4) L'auditeur désigné dépose un rapport sur le recours en annulation.
> 5) La partie à laquelle le rapport de l'auditeur donne tort prend connaissance de celui-ci et dépose une demande de poursuite de la procédure ainsi qu'un dernier mémoire.
> 6) La partie à laquelle le rapport de l'auditeur donne raison prend connaissance du rapport de l'auditeur et du dernier mémoire de l'autre partie au litige. Elle dépose à son tour un dernier mémoire.
>
> Si une partie, autre que la partie requérante ou la partie adverse, souhaite intervenir en cours de procédure, elle doit le faire au moyen d'une requête en intervention. Si l'intervention est accueillie, la partie intervenante déposera également un dernier mémoire.
>
> D'autres actes de procédure peuvent être communiqués par les parties. Il s'agit par exemple d'un désistement d'instance, d'un retrait de l'acte administratif attaqué, ou encore de notes de plaidoirie déposées à l'audience.
>
> Ces différents actes de procédure peuvent être accompagnés de pièces annexées par les parties. Contrairement aux actes de procédure, qui sont limitativement énumérés et définis par les lois coordonnées et ses arrêtés d'exécution mentionnés ci-dessus, la nature des pièces annexées n'est pas définie. Celles-ci varient donc d'une affaire à l'autre en fonction, notamment, de la nature du litige soumis au Conseil d'État.
>
> Ces différents actes et pièces déposés par les parties forment – avec les avis, communications et convocations déposés par le Conseil d'État à l'intention des parties – le dossier électronique de l'affaire tel que défini à l'article 85*bis*, § 2, 2°, nouveau du règlement général de procédure."

10. Concrètement, l'Autorité suppose que la plate-forme électronique envisagée servira pour les notifications, les communications et les dépôts (de requêtes, de conclusions, de mémoires et de pièces, ainsi que des courriers y afférents). Le dossier sur la plate-forme électronique - comme le

décrit le demandeur - se composera des éléments susmentionnés introduits par les parties ainsi que des avis, communications et convocations du Conseil d'État à l'attention des parties[6]. L'Autorité en prend acte.

11. L'Exposé des motifs précise en outre que : "***Les finalités poursuivies*** *par ces traitements de données* ***ne diffèrent pas*** *de celles qui sont poursuivies dans le cadre d'un recours introduit et traité par la procédure "papier".* ***Ces données sont exclusivement traitées*** *par le Conseil d'État* ***afin de lui permettre de gérer les recours, de sauvegarder les intérêts des parties et d'assurer la prévisibilité et l'unité de sa jurisprudence.***"[7]

12. Tout cela pris en considération, l'Autorité estime que les finalités sont déterminées, explicites et légitimes.

c. Minimisation des données/Proportionnalité

13. L'article 5.1.c) du RGPD prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités visées (principe de 'minimisation des données').

14. À cet égard, il découle du projet d'article 31*bis*, § 1er, alinéa 4 que les données à caractère personnel relatives aux utilisateurs[8] de la plate-forme électronique se limitent aux données suivantes :
    - le numéro de Registre national ;
    - les nom et prénoms ;
    - l'adresse courriel ;
    - le numéro de téléphone.

15. Concernant le numéro de Registre national, l'Autorité attire l'attention du demandeur sur le fait que le numéro de Registre national ne peut être utilisé/traité qu'aux conditions définies à l'article 8

---

[6] Y compris les actes de procédure et les notifications en vertu de l'article 85*bis*, § 13 actuellement applicable du règlement de procédure du Conseil d'État.

[7] Exposé des motifs, projet d'article 31*bis*, § 1er, alinéa 4.

[8] À la demande de l'Autorité, il a été spécifié que - à l'exception d'un futur changement minime - le terme '*utilisateurs*' correspond à la définition actuelle figurant à l'article 85*bis*, § 2, 1° du règlement de procédure du Conseil d'État, à savoir "*Pour l'application du présent arrêté, on entend par : 1° utilisateur : toute personne qui intervient dans une procédure électronique.*"

Le demandeur a répondu : "*Le terme "utilisateurs" utilisé dans l'article 31bis du projet correspond bien à la définition d' "utilisateur" donnée par l'article 85bis, § 2, 1° du règlement général de procédure.*

Cette définition est très légèrement modifiée dans le nouvel article 85bis, § 2, 1°, du règlement général de procédure afin de prendre en compte le nouveau système de gestion des utilisateurs au sein duquel les notions de "titulaire d'enregistrement", de "gestionnaire de dossier", et de "délégué" sont supprimées."

de la loi du 8 août 1983 *organisant un registre national des personnes physiques*[9]. **Il est recommandé de mentionner explicitement dans le Projet la base juridique, à savoir l'article 8 de la loi précitée**. L'Autorité rappelle aussi de manière générale que les numéros d'identification unique font l'objet d'une protection particulière. L'article 87 du RGPD prévoit que les États membres qui définissent un numéro d'identification national doivent veiller à ce qu'il ne soit utilisé que sous réserve de garanties appropriées pour les droits et libertés de la personne concernée. Ainsi, la Commission de la protection de la vie privée, prédécesseur en droit de l'Autorité, a déjà attiré précédemment[10] l'attention sur le respect des garanties suivantes en la matière :

- l'utilisation d'un numéro d'identification général doit être limitée aux cas où il est strictement nécessaire étant donné que son utilisation implique des risques en termes d'interconnexion de fichiers ;
- les finalités doivent être précisées clairement et explicitement afin que l'on puisse entrevoir/prévoir les types de traitements visés ;
- la durée de conservation et les éventuelles communications à des tiers doivent également être encadrées ;
- des mesures techniques et organisationnelles doivent encadrer adéquatement l'utilisation sécurisée ; et
- le non-respect des dispositions encadrant l'utilisation doit être sanctionné au moyen de sanctions effectives, proportionnées et dissuasives.

16. Il est ensuite question des "*données à caractère personnel contenues dans les actes de procédure et* [des] *pièces composant un dossier électronique* " - susceptibles d'impliquer également des traitements de catégories particulières de données à caractère personnel, mentionnées aux articles 9.1 (données concernant les convictions religieuses ou philosophiques, la santé, ...) et 10 (données relatives aux condamnations pénales et aux infractions) du RGPD - ce qui , à première vue, ne constitue pas forcément un obstacle.

17. Dans le contexte applicable, à savoir dans le cadre de la juridiction du Conseil d'État, on peut supposer que vu leur nature et leur fonction, de tels actes de procédure et documents contiendront plusieurs types de données à caractère personnel, notamment des catégories particulières de données à caractère personnel. La présence de ces données découle de la nécessité de pouvoir

---

[9] "*L'autorisation d'utiliser le numéro du Registre national est octroyée par le ministre ayant l'Intérieur dans ses attributions aux autorités, aux organismes et aux personnes visés à l'article 5, § 1er, lorsque cette utilisation est nécessaire à l'accomplissement de tâches d'intérêt général.*

L'autorisation d'utiliser le numéro du Registre national implique l'obligation d'utiliser également ce numéro du Registre national dans les contacts avec le Registre national des personnes physiques.

Une autorisation d'utilisation du numéro du Registre national n'est pas requise lorsque cette utilisation est explicitement prévue par ou en vertu d'une loi, un décret ou une ordonnance.".

[10] Voir l'avis n° 19/2018 du 29 février 2018 sur un *avant-projet de loi portant des dispositions diverses "Intérieur"*.

évaluer correctement et complètement les faits et les intérêts des parties, ce qui est nécessaire à l'exécution de la mission d'intérêt public dont est investi le Conseil d'État en tant que juridiction administrative en vertu de l'article 160 de la *Constitution* et des articles 7 à 17 des lois coordonnées sur le Conseil d'État. Dans la mesure où le traitement de ces données à caractère personnel reste limité aux finalités y afférentes, où le traitement de données découlant du Projet reste également limité aux finalités envisagées et où au moins des garanties appropriées comme la confidentialité et la limitation de l'accès sont mises en œuvre, on peut adéquatement parer les risques allant de pair avec ces traitements.

18. Il ressort également de l'Exposé des motifs du projet d'article 31*bis*, § 1er, alinéa 5 qu'en ce qui concerne les catégories de données à caractère personnel, des données de journalisation des activités effectuées par les utilisateurs (*connexion, moment exact du dépôt, moment exact de prise de connaissance d'un dépôt,* ***...***[11]) seront aussi traitées. En l'occurrence, le numéro de Registre national, les nom et prénoms seront récupérés lorsque l'utilisateur s'authentifie via le système CSAM mis en place par le SPF BOSA. Compte tenu du fait que les données à caractère personnel mentionnées au point 14 sont combinées aux données de journalisation - qui, comme cela ressort du point 20, seront toutes deux visibles - et que cette combinaison peut conduire à l' 'identifiabilité' des utilisateurs, on ne peut que conclure que les données de journalisation doivent être qualifiées de données à caractère personnel, conformément à la jurisprudence courante de la Cour de justice[12].

19. Le demandeur a confirmé à cet égard qu'aucune autre donnée que celles énumérées dans le Projet et dans l'Exposé des motifs ne sera traitée : "*Oui, aucune autre donnée à caractère personnel que celles mentionnées dans l'article 31bis et dans l'exposé des motifs ne sera traitée*." Par conséquent, on peut supposer que les "..." de suspension n'impliquent aucun autre élément. Ce qui laisse encore ouverte une question concernant le terme '*connexion*'. Dans la mesure où l'on vise par là autre chose qu'une '*adresse IP*', il semble recommandé de le préciser et d'en motiver la nécessité au moins dans l'Exposé des motifs.

20. Enfin, en vertu du projet d'article 31*bis*, § 1er, alinéa 6, il apparaît que les titulaires de fonction et les collaborateurs du Conseil d'État ont, dans le cadre de leurs fonctions, accès aux données à caractère personnel. À cet égard, le demandeur a précisé ce qui suit concernant :

    a) **les données à caractère personnel des utilisateurs de la plate-forme** électronique : "*En interne au Conseil d'État, les magistrats, greffiers et collaborateurs du greffe notamment auront accès aux données des utilisateurs mais il s'agit ici de*

[11] Mise en gras ajoutée par l'Autorité.

[12] Voir à cet égard CJUE, 19 octobre 2016, affaire C-582/14*Breyer*, EU:C:2016:779.

données dites "utiles", c'est-à-dire nom, prénom, e-mail et téléphone. Le numéro national ne sera pas visible.

Il faut aussi noter que certaines de ces données telles que les noms et prénoms, adresse courriel et numéro de téléphone peuvent également apparaître sur les actes de procédure déposés par les utilisateurs (par exemple les noms, prénoms, adresse courriel et numéro de téléphone de l'avocat, que celui-ci fait apparaître en en-tête d'un acte de procédure)."

b) **les données de journalisation** : "*L'intention est, en effet, d'y donner accès en interne afin que les magistrats, les greffiers et le greffe puissent déterminer ce qui s'est passé sur la plate-forme dans un dossier X à un moment M. Mais ce sont des données "fonctionnelles", c'est-à-dire nécessaires au traitement du dossier sous un angle procédural.*"

c) **les actes de procédure** : "*L'ensemble des titulaires de fonction ont accès aux pièces de procédure. Il en va de même pour les membres du personnel administratif de la section du contentieux administratif qui sont mpliqués dans la fonction juridictionnelle du Conseil d'État et auxquels il est donné accès à Proadmin+ (le personnel administratif du greffe, des chambres et de l'auditorat). Il ne s'agit donc pas de l'ensemble du personnel administratif.*"

21. L'Autorité déduit des explications complémentaires que par 'accès aux données à caractère personnel' figurant dans le projet d'article 31*bis*, § 1er, alinéa 6, on veut dire qu'au sein du Conseil d'État, les magistrats, les greffiers et les collaborateurs du greffe auront accès aux : *a) données à caractère personnel des utilisateurs de la plate-forme électronique ; b) données de journalisation ; c) actes de procédure*. Le demandeur semble toutefois indiquer que toutes les personnes susmentionnées n'ont assurément pas le même accès à chacune de ces trois catégories de données[13]. En vue de la sécurité juridique, il est recommandé de fournir au moins dans l'Exposé des motifs de plus amples explications concernant les personnes relevant précisément des termes 'titulaires de fonction et collaborateurs du Conseil d'État' et d'établir une corrélation entre leur rôle fonctionnel et les données auxquelles ils sont censés avoir accès - sauf exceptions légales.

22. En ce qui concerne les données reprises sous a), il s'agirait de données '*utiles*', à savoir le nom, le prénom, l'e-mail et le numéro de téléphone. Le numéro de Registre national ferait partie du même groupe mais ne serait pas visible. Considérant le traitement envisagé, l'Autorité est plutôt d'avis que ces données doivent être qualifiées de '*nécessaires*'. Si par contre, il s'agissait quand même de données purement '*utiles*' - c'est-à-dire qui ne sont pas nécessaires pour que les finalités du

[13] **Données à caractère personnel des utilisateurs** = magistrats, greffiers et collaborateurs du greffe ; **données de journalisation** = magistrats, greffiers et le greffe ; **actes de procédure** = titulaires de fonction, le personnel administratif du greffe, les chambres et l'auditeur.

traitement puissent être atteintes sans ces données ou au moyen de données anonymisées -, il va de soi que celles-ci ne peuvent pas être traitées. Concernant le numéro de Registre national, il est observé, en remarque, que s'il s'agit là de l'application pratique, il semble indiqué de le préciser au moins dans l'Exposé des motifs. Sans clarification, on pourrait penser, à tort, que le numéro de Registre national est visible pour les personnes susmentionnées.

23. En ce qui concerne les données reprises sous b), il ressort des explications du demandeur que les magistrats, les greffiers et le greffe y ont accès. L'Autorité estime, dans le contexte applicable, qu'il est effectivement nécessaire de savoir quand l'introduction de pièces et les prises de connaissance ont lieu. Néanmoins, à la lumière des finalités, il ne semble pas essentiel que la '*connexion*' soit accessible à toutes les personnes susmentionnées. À cet égard, il est recommandé d'éventuellement utiliser des niveaux d'autorisation de manière à ce que la visibilité des données soit limitée à ce qui est réellement nécessaire à la lumière de la finalité poursuivie.

24. Quant aux actes de procédure, l'Autorité accueille favorablement l'intention de limiter l'accès aux actes de procédure. En la matière, il est fait référence aux points 32 à 34 inclus, qui traitent plus en détail les mesures de protection et de sécurisation possibles.

25. À la question de l'Autorité concernant la connexion de la plate-forme électronique avec d'autres plate-formes, le demandeur a indiqué que ce serait bel et bien le cas. Ainsi, il a été précisé que :

> *"La plate-forme électronique décrite dans l'article 31bis, nommée 'eProadmin', est liée à un outil de consultation et de gestion interne dénommé 'Proadmin+'.*
>
> *La plate-forme eProadmin et l'outil Proadmin+ constituent en réalité les deux volets d'un même outil : eProadmin en est le volet externe (front office), destiné à être utilisé par les utilisateurs tels que définis à l'article 85bis, § 2, 1°, du règlement général de procédure, alors que Proadmin+ est en le volet interne (back office), accessible aux seuls collaborateurs et titulaires de fonction du Conseil d'État.*
>
> *Une connexion avec DPA est envisagée afin que les avocats puissent aussi s'identifier par ce canal-là*."[14]

26. Selon le demandeur, cela n'entraînerait pas d'extension de l'accès aux diverses données à caractère personnel susmentionnées sur la plate-forme. L'accès resterait limité d'une part aux utilisateurs et d'autre part aux titulaires de fonction et collaborateurs du Conseil d'État. L'Autorité en prend acte et renvoie aux points 32 à 34 inclus pour les recommandations relatives aux mesures de protection et de sécurisation.

[14] Digital Platform for Attorneys (DPA).

27. L'intention de prévoir une connexion avec la Digital Platform for Attorneys (DPA) soulève toutefois plusieurs questions. À cet égard, il semble pertinent de faire référence à l'avis n° 78/2018 rendu précédemment et en particulier au point 29, qui contient la remarque suivante :

> "*Dès lors, la conservation, par les organisations professionnelles, des données transmises et déposées dans e-Box et e-Deposit n'est ni légitime ni proportionnée au regard de la finalité de garantir un accès sécurisé aux systèmes e-Box et e-Deposit. Si un acteur souhaite accéder aux données précédemment transmises, il lui suffit de les consulter dans e-Box et e-Deposit, après s'être dûment identifié, si nécessaire par l'intermédiaire de son organisation professionnelle*."[15]

28. Considérant que l'accès à la plate-forme électronique doit se faire via CSAM, où l'authentification est liée au numéro de Registre national de chacun, et vu les informations sur le site Internet de la DPA selon lesquelles à partir de juin 2025, il sera possible de se connecter via l'eID ou itsme, la plus-value d'une connexion avec la DPA, en vue d'une identification, est remise en cause. En effet, selon le site Internet, "*Le numéro de Registre national ou le numéro BIS de l'avocat doit être enregistré auprès du barreau pour pouvoir se connecter avec eID ou itsme*."[16] Dans cette optique, on peut supposer que ces informations sont déjà disponibles ou vérifiables auprès du barreau et dès lors aussi via la plate-forme électronique.

29. L'Autorité réitère ensuite la remarque précédemment formulée, à savoir que pour les organisations professionnelles - en l'espèce la DPA -, il suffit de consulter les données nécessaires sur la plate-forme électronique. En outre, il n'est même pas certain qu'une telle consultation soit nécessaire, vu que la plate-forme électronique contiendra plusieurs applications qui sont proposées via la DPA, contre paiement. De surcroît, les finalités définies dans le Projet ne semblent pas aller dans ce sens. Il appartient au demandeur de veiller à ce que le traitement de données à caractère personnel se déroule de manière licite, à ce que les risques de violations de données soient réduits au maximum et à ce que des connexions inutiles avec des plate-formes externes soient évitées - surtout lorsque des opérations similaires peuvent déjà être réalisées au sein du propre système. À cet égard, la plate-forme électronique du Conseil d'État semble la plus recommandée, vu qu'il s'agit d'une source authentique électronique.

30. Compte tenu de tout ce qui précède, l'Autorité estime que pour la majorité, les catégories de données à caractère personnel mentionnées sont adéquates. Mais pour être pertinentes et limitées, il faut d'abord donner davantage d'explications quant aux personnes concernées qui ont accès aux données à caractère personnel. Dans ce cadre, il semble recommandé de compléter l'Exposé des motifs avec les explications supplémentaires du demandeur, en tenant compte des

---

[15] Pour la position de l'Autorité concernant la DPA, il est renvoyé à l'avis n° 78/2018 dans son intégralité.

[16] DPA, consultée pour la dernière fois le 9 mai 2025, via le lien suivant : https://www.dp-a.be/fr/app/acces.

recommandations des points 21 à 24 inclus. Deuxièmement, il faut vérifier s'il est réellement essentiel que la connexion soit visible pour tous les acteurs. Troisièmement, il est recommandé de fournir des précisions supplémentaires pour certains termes. Enfin, la nécessité d'une connexion avec la DPA est remise en cause, à la lumière des finalités poursuivies.

d. Authentification et disponibilité

31. Le projet d'article 31*bis*, § 3 précise ensuite qu' "*Un arrêté royal délibéré en Conseil des ministres fixe le mode de fonctionnement de cette plate-forme électronique, en ce compris la procédure d'enregistrement, les méthodes d'authentification des utilisateurs, le format et la signature des documents, ainsi que les modalités d'utilisation et de sécurisation* ".

32. L'Autorité accueille favorablement l'intention de définir des mesures de protection et de sécurisation. En la matière, il convient de recommander de travailler avec des mesures d'autorisation, de manière à ce que l'accès à la plate-forme, en particulier le contenu des dossiers, et l'exécution d'opérations ou d'actions soient subordonnés à des compétences liées à l'identité de chacun.

33. Il est également recommandé de conserver les fichiers de journalisation des activités des titulaires de fonction et collaborateurs du Conseil d'État sur la plate-forme[17]. Vu le contexte sensible, il est déconseillé d'opter pour un niveau de protection inférieur à l'authentification à deux facteurs. À cet égard, l'Autorité est favorable à l'utilisation de CSAM en tant que moyen d'identification, comme il ressort de l'Exposé des motifs.

34. En outre, il semble recommandé de mettre en œuvre une structure d'accès hiérarchique, avec plusieurs niveaux de classification - par exemple bas, moyen, élevé ou confidentiel, secret, très secret. De cette façon, selon la nécessité opérationnelle et fonctionnelle, un accès différencié peut être accordé aux données d'utilisateurs, aux données de journalisation et aux actes de procédure, en tenant compte de la tâche fonctionnelle de chacun. Enfin, un chiffrement doit être mis en œuvre pour l'enregistrement et la communication pour assurer la confidentialité des données.

e. Responsable(s) du traitement

35. La désignation du responsable du traitement doit correspondre au rôle que cet acteur jouera dans la pratique et au contrôle qu'il a sur les finalités et les moyens qui seront mis en œuvre pour le

[17] Il appartient au demandeur de définir à cet effet le délai maximal de conservation, en tenant compte de la nécessité des données à la lumière des finalités poursuivies. Celui-ci ne peut en aucun cas être plus long que le délai de conservation du dossier ou de l'affaire sous-jacent(e). Le raisonnement des points 41 à 44 inclus s'applique également ici par analogie.

traitement. Dans la pratique, ceci doit être vérifié pour chaque traitement de données à caractère personnel.

36. Il ressort de l'article 2 du Projet, c'est-à-dire le projet d'article 31*bis*, que le Conseil d'État est désigné comme responsable du traitement pour les traitements de données qui en découlent.

37. L'Autorité en prend acte. Néanmoins, il y a lieu de faire remarquer que lors de l'instauration d'une connexion avec la DPA, voir ci-dessus, plusieurs responsables du traitement sont possibles, avec toutes les conséquences et obligations que cela implique[18].

f. Délai de conservation

38. En vertu de l'article 5.1.e) du RGPD, les données à caractère personnel ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

39. En la matière, l'article 31*bis*, § 1er, alinéa 4 rétabli spécifie que les données à caractère personnel des utilisateurs de la plate-forme électronique seront conservées pendant 30 ans. Ce délai peut, si nécessaire, être prolongé jusqu'à ce que toutes les voies de recours de toute procédure pendante à laquelle se rapportent les données soient épuisées. En outre, l'Exposé des motifs indique aussi que les données de journalisation (mentionnées au point 20) seront aussi conservées. En ce qui concerne ce dernier élément, le demandeur a confirmé que pour ces données aussi, le délai de conservation était fixé à 30 ans, à l'exception d'éventuelles prolongations, comme le précise l'article. Interrogé sur la nécessité d'un délai de conservation de 30 ans, qui pouvait être soumis à une prolongation, le demandeur a répondu ce qui suit :

> "*Comme cela est indiqué dans le commentaire du paragraphe 1er de l'article 31bis, le délai de conservation de trente ans s'inspire du délai identique fixé par l'article 3, alinéa 2, de l'arrêté royal du 16 juin 2016 portant création de la communication électronique conformément à l'article 32ter du Code judiciaire.*
>
> *Ce délai est notamment justifié par le fait que la survenance de certains incidents de procédure – par exemple une inscription de faux, qui doit d'abord être tranchée par le juge judiciaire avant que le Conseil d'État puisse poursuivre l'examen du recours – peut retarder la clôture du dossier devant le Conseil d'État. De la même manière, la solution d'un litige pendant devant le Conseil d'État peut être différée lorsqu'elle dépend de l'issue d'une procédure engagée devant les juridictions judiciaires, lesquelles peuvent nécessiter un temps de traitement particulièrement long.*

[18] Voir dans le même sens l'avis n° 78/2018, points 24-25.

Au vu de ces éléments, il est nécessaire que le Conseil d'État puisse conserver durant trente ans les données liées à l'utilisation de la plate-forme électronique, lesquelles doivent pouvoir être consultées et vérifiées en cas de contestation de la validité de la procédure menée devant le Conseil d'État."

40. Considérant le fait que le demandeur a également indiqué que le délai maximal de conservation de 30 ans était un délai de conservation actif, l'Autorité formule les remarques suivantes :

41. Compte tenu de tout ce qui précède, il est raisonnablement nécessaire de conserver les données jusqu'à ce que les procédures pendantes en justice soient terminées et que toutes les possibilités de recours soient épuisées. Toutefois, cette nécessité est remise en cause pour les dossiers qui sont clôturés dans un délai plus court, c'est-à-dire avant l'expiration du délai de conservation de 30 ans indiqué. En pareils cas, un délai de conservation de trente ans imposé de manière non différenciée semble manquer son objectif.

42. Dans le même sens, la Cour de justice a souligné à plusieurs reprises que "*même un traitement initialement licite de données peut devenir, avec le temps, incompatible avec le règlement 2016/679 lorsque ces données ne sont plus nécessaires à la réalisation de telles finalités [arrêt du 24 septembre 2019, GC e.a. (Déréférencement de données sensibles), C-136/17, EU:C:2019:773, point 74] et que les données doivent être supprimées lorsque lesdites finalités sont réalisées.*"[19]

43. Il est également observé qu'un enregistrement de longue durée non différencié implique aussi des risques quant à l'exactitude des données qui, après un certain temps, sont susceptibles de ne plus être à jour. Il incombe au demandeur de démontrer pour quelles raisons un délai de trente ans est proportionné et nécessaire, ce qui en l'occurrence fait défaut pour les affaires classées sans suite. À la lumière de ces éléments, il est recommandé tout d'abord de reconsidérer ce délai de conservation de manière à ce que toutes les données des utilisateurs et les données de journalisation ne soient pas systématiquement conservées pendant trente ans, à l'exception des prolongations prévues légalement, et deuxièmement de formuler les différents délais sous la forme de délais maximaux. De cette manière, des règles spécifiques de la politique de conservation peuvent être utilisées sur la base du statut d'un dossier (ouvert, fermé, recours, etc.). Par ailleurs, des 'rappels de conservation' (*retention reminders*) peuvent aussi être instaurés pour vérifier si la conservation est encore nécessaire et il est également possible de travailler avec des limitations des accès, l'accès aux données qui sont conservées étant limité à un environnement fermé avec des droits d'accès ; ce qui permet une consultation, en cas de nécessité.

[19] CJUE, 20 octobre 2022, affaire C-77/21, *Digi*, ECLI:EU:C:2022:805, paragraphe 54.

44. En ce qui concerne les données à caractère personnel contenues dans les actes de procédure et les pièces composant un dossier électronique, le projet d'article 31*bis*, § 1er, alinéa 5 précise que "[celles-ci] *sont conservées pendant le temps nécessaire à l'exercice de la mission d'intérêt public dont le Conseil d'État est investi en tant que juridiction administrative*". À cet égard, il appartient au demandeur de s'assurer que le délai de conservation correspond à ce qui est strictement nécessaire en vue d'atteindre les finalités envisagées, dans le cadre de la mission confiée au Conseil d'État[20].

PAR CES MOTIFS,
l'Autorité,

estime qu'au minimum les modifications suivantes s'imposent dans le Projet :

- prévoir un renvoi à l'article 8 de la loi du 8 août 1983 *organisant un registre national des personnes physiques* (voir le point 15) ;
- indiquer dans l'Exposé des motifs que le numéro de Registre national ne sera pas visible (voir le point 22) ;
- spécifier davantage les termes 'titulaires de fonction et collaborateurs du Conseil d'État' et établir une corrélation avec le rôle fonctionnel et les données auxquelles un accès est accordé (voir le point 21) ;
- si le terme 'connexion' se rapporte à autre chose que '*l'adresse IP*', il est recommandé de le préciser au moins dans l'Exposé des motifs (voir le point 19) ;
- prévoir un délai maximal de conservation différencié (voir les points 40-43) ;

souligne l'importance des éléments suivants :

- définir des mesures de protection et de sécurisation considérées comme minimales dans ce contexte (voir les points 32-34) ;
- le principe de licéité et le principe de minimisation des données, en particulier concernant la nécessité d'une connexion avec la DPA (voir les points 28-30).

Pour le Service d'Autorisation et d'Avis,
(sé.) Alexandra Jaspar, Directrice

[20] La Cour constitutionnelle a déjà reconnu que "[le législateur] *pouvait régler de manière générale les conditions de conservation des données à caractère personnel, ainsi que la durée de cette conservation*", arrêt n° 29/2018 du 15 mars 2018, point B.23.