Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n°189/2026 du 31 août 2026

Objet : Avis concernant un avant-projet de loi portant des dispositions diverses en matière de santé (II), article X (ADV-2026-00015).

Mots-clés : assurance maladie – communication de documents relatifs à l'assurance maladie – plateforme eHealth – signature manuscrite – assimilation des signatures digitalisées – principe de prévisibilité.

Version originale

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

Vu la demande d'avis de Franck Vandenbroucke, Vice-premier ministre et Ministre des Affaires sociales et de la Santé publique, chargé de la Lutte contre la pauvreté, reçue le 30 avril 2026 ;

Vu les informations complémentaires reçues les 17 juin et 7 juillet 2026 ;

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité ») émet, le 31 août, l'avis suivant :

L'Autorité ne publie en français et en néerlandais que les avis concernant les projets ou propositions de textes de rang de loi émanant de l'Autorité fédérale, de la Région de Bruxelles-Capitale ou de la Commission Communautaire Commune. La « Version originale » est la version qui a été validée.

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. En date du 30 avril 2026, Monsieur Franck Vandenbroucke, Vice-premier ministre et Ministre des Affaires sociales et de la Santé publique, chargé de la Lutte contre la pauvreté (ci-après le « demandeur ») a sollicité l'avis de l'Autorité sur **l'article X** de l'avant-projet de loi portant des dispositions diverses en matière de santé (II) (ci-après le « Projet »). Cet article fait partie de la Section 1re, intitulée « *Assimilation des signatures digitalisées* », du Chapitre 2 de l'avant-projet de loi précité qui vise à modifier la loi *relative à l'assurance obligatoire soins de santé et indemnités, coordonnée du 14 juillet 1994* (ci-après la « Loi assurance maladie »).

2. Le Projet entend **insérer un nouvel article 9*quinquies*** dans la Loi assurance maladie obligatoire, rédigé comme suit :

   « § 1er. Les documents relatifs à l'assurance soins de santé et indemnités visés dans la présente loi et dans ses arrêtés d'exécution peuvent être échangés de manière sécurisée au moyen de techniques informatiques qui :

   a) permettent d'identifier de manière certaine l'émetteur ;

   b) garantissent l'origine et l'intégrité du contenu des documents au moyen de techniques de sécurisation adaptées ;

   c) permettent de déterminer de manière certaine le moment auquel les documents ont été envoyés.

   La chambre sécurité sociale et santé du Comité de sécurité de l'information approuve ces techniques informatiques.

   § 2. L'échange de documents répondant aux conditions visées au § 1er a le même effet juridique que l'échange de documents pourvus d'une signature manuscrite ou d'une signature électronique qualifiée.

   § 3. Dans ce cas, les originaux des documents échangés sont conservés par l'expéditeur. »

3. Il ressort de l'Exposé des motifs que le Projet s'inscrit dans le processus de digitalisation des échanges entre les dispensateurs de soins et les organismes assureurs qui a commencé il y a quelques années et qui devrait être généralisé à l'ensemble des secteurs au 1er janvier 2030, comme le prévoit la loi-cadre du 30 mai 2026[1]. L'Exposé des motifs indique que « *[c]ependant, certains documents posent des difficultés pour être intégrés dans ce processus* » et qu'il s'agit « *notamment des documents qui doivent impérativement être signés par le patient parce qu'ils comportent des engagements concrets de suivre son traitement pris par ce dernier dont le non-respect peut entrainer l'arrêt de l'intervention de l'assurance obligatoire* ». Il est également précisé que le Projet entend pallier, entre autres, le fait que « *certains patients ne sont pas à même sur le plan pratique de signer électroniquement (oubli des codes de la carte d'identité par exemple)* ». C'est dans ce contexte que le Projet entend insérer un

[1] L'Exposé des motifs se réfère au « *projet de loi-cadre* ». L'Autorité comprend à la lumière des informations complémentaires transmises qu'il s'agit en réalité de la loi-cadre (et non du projet de loi-cadre) du 30 mai 2026 dont l'article 54 a modifié l'article 53, §1er, alinéa 6 de la Loi assurance maladie.

nouvel article 9*quinquies* dans la Loi assurance maladie visant « *à permettre, dans le cas où la signature électronique qualifiée ne peut pas être utilisée, de garantir l'origine et l'intégrité du contenu des documents au moyen de techniques de sécurisation adaptées* ».

4. Il ressort des informations complémentaires transmises[2] que le but du Projet est de **créer un outil digital sécurisé** pour les documents qui sont **signés manuscritement** lorsque la signature électronique qualifiée ne peut pas être utilisée et que cet outil permet de garantir l'origine et l'intégrité du contenu des documents électroniques, au moyen de techniques de sécurisation adaptées, et de leur conférer, lors de leur transmission, la même valeur juridique que celle accordée à la communication de documents par voie papier comportant une signature manuscrite ou par voie électronique comportant une signature électronique qualifiée.

5. Interrogé quant au système ou à l'application qui va être mis en place et dont la validité va être reconnue par le Projet pour effectuer les échanges de documents visés, le demandeur a répondu que « *les documents susceptibles d'être digitalisés […] sont nombreux et susceptibles de suivre un circuit différent (il s'agit d'un circuit de présentation électronique mis en place en vertu de la loi [assurance maladie]) un exemple fréquent est celui d'un document imprimé par le dispensateur, signé manuscritement par le bénéficiaire et qui sera ensuite digitalisé pour rentrer dans les circuits de digitalisation prévu en vertu de l'article 9bis [de la loi assurance maladie]*. »

6. Il ressort également des informations complémentaires reçues que les techniques de sécurité adaptées pour garantir l'origine et l'intégrité du contenu des documents visés (qui sont mentionnées dans les informations complémentaires du demandeur figurant au point 4 ci-dessus), consistent à générer un hachage du fichier et à le faire signer par les services de la plateforme eHealth[3].

---

[2] « *Le but est donc de créer un outil digital sécurisé pour les documents signés manuscritement.*

Onderhavig artikel heeft als doel om de oorsprong en integriteit van de inhoud van niet-gestructureerde elektronische documenten (Word, PDF of andere), waarbij geen gekwalificeerde elektronische handtekening kan worden gebruikt, te garanderen door middel van aangepaste bevei-ligingstechnieken en voor de uitwisseling ervan in hetzelfde rechtsgevolg te voorzien als voor de uitwisseling van documenten met een handgeschreven of een gekwalificeerde elektronische handtekening."

[3] Selon les informations complémentaires communiquées : "*De techniek bestaat erin om een hash te maken van de file en deze te laten tekenen door de diensten van eHealth Platform.*
Een hash van een bestand bezit een aantal essentiële eigenschappen. Ten eerste is het proces deterministisch: hetzelfde bestand resulteert steeds in dezelfde hashwaarde. Voorts kenmerkt de berekening zich door efficiëntie, aangezien deze, ongeacht de bestandsgrootte, snel wordt uitgevoerd.
Daarnaast vertoont de hash het zogenoemde lawine-effect: een marginale wijziging in het bestand, zelfs het aanpassen van één bit, leidt tot een geheel andere en onvoorspelbare hashwaarde. Tot slot is de hash botsingsbestendig: het is praktisch onmogelijk om twee verschillende bestanden te vinden die tot eenzelfde hashwaarde leiden.
Een belangrijke toegevoegde waarde is dat de hash van het bestand door de dienst van eHealth Platform wordt voorzien van een tijdstempel (timestamping). Door de hashwaarde van het bestand te combineren met een betrouwbaar tijdstip, wordt onomstotelijk aangetoond dat het bestand op een bepaald moment in die specifieke vorm heeft bestaan. Dit verschaft sterke bewijskracht en garandeert herleidbaarheid en onweerlegbaarheid van het bestand.
Op grond van deze eigenschappen wordt de hash van een bestand toegepast bij het verifiëren van de integriteit van het bestand, bijvoorbeeld om aan te tonen dat het sinds een bepaald moment niet is gewijzigd."

7. A la lumière de ces informations complémentaires transmises par le demandeur, l'Autorité comprend que le Projet entend mettre en place un **système « hybride »** (qui se trouve entre un flux de données complètement électronique et un flux de données totalement sur support papier) qui permet de transmettre, de manière digitale et sécurisée par le biais de la plateforme eHealth, les documents relatifs à l'assurance soins de santé et indemnités signés manuscritement (par un processus qui répond aux conditions visées au paragraphe 1er du Projet) afin de permettre l'activation de l'intervention de l'assurance maladie, pour laquelle le principe est la production d'un document original sur support papier. Il ne s'agit donc pas ici de mettre en place un nouveau système de signature électronique qualifiée, ce qui a été confirmé par le demandeur[4].

II. EXAMEN DU PROJET

II.1. Rappel des principes de prévisibilité et de nécessité

8. Conformément à l'article 6.3 du RGPD, lu à la lumière du considérant 41[5] du RGPD, le traitement de données à caractère personnel jugé nécessaire au respect d'une obligation légale[6] à laquelle le responsable du traitement est soumis ou 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[7] doit être régi par une réglementation qui soit claire et précise et dont l'application doit être prévisible pour les personnes concernées. En outre, le principe de légalité, consacré à l'article 22 de la Constitution, tel qu'interprété par la Cour Constitutionnelle et le Conseil d'Etat, implique que les éléments essentiels[8] des traitements de données soient déterminés dans une norme de rang de loi et que les circonstances dans lesquelles les traitements de données à caractère personnel sont réalisés soient déterminées de manière suffisamment précise, dans le respect des principes de nécessité et de proportionnalité [9].

---

[4] Interrogé quant à la portée des effets juridiques que le Projet entend conférer à la signature digitalisée mise en place par le Projet, le demandeur a répondu qu' « *il ne s'agit pas ici de créer une nouvelle signature qualifiée mais de permettre la production d'un document comportant la copie d'une signature et de lui permettre d'activer les interventions de l'assurance pour lesquelles le principe est la production d'un document original* ».

[5] « *41. Lorsque le présent règlement fait référence à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l'ordre constitutionnel de l'État membre concerné. Cependant, cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne (ci-après dénommée «Cour de justice») et de la Cour européenne des droits de l'homme* ».

[6] Art. 6.1.c) du RGPD.

[7] Art. 6.1.e) du RGPD.

[8] Il s'agit de la finalité poursuivie par le traitement de données visé, les catégories de données nécessaires à la réalisation de cette finalité, les catégories de personnes concernées à propos desquelles les données sont collectées, les catégories de destinataires des données si la réalisation de la finalité visée nécessite des communications de données et le délai maximal pendant lequel les données devront être conservées pour la réalisation de la finlaité. L'Autorité ajoute également, dans certaines circonstances, l'identification du responsable du traitement.

[9] Voir notamment les arrêts suivants de la Cour Constitutionnelle : arrêt n° 29/2018 du 15 mars 2018, point B.13.2 ; arrêt n° 86/2018 du 5 juillet 2018, point B.7.3.

9. L'Autorité constate tout d'abord une **discordance** entre le **dispositif** du Projet et l'intention qui est reflétée dans **l'Exposé des motifs** en ce qui concerne le champ d'application du Projet, ce qui nuit à la prévisibilité du Projet. En effet, selon le dispositif du Projet, celui-ci est applicable de manière générale à tout échange de « *documents relatifs à l'assurance soins de santé et indemnités visés dans la présente loi et dans ses arrêtés d'exécution* » alors que selon l'Exposé des motifs, le champ d'application serait limité au « *cas où la signature électronique qualifiée ne peut pas être utilisée* »[10]. Il ressort des informations complémentaires transmises par le demandeur[11] que l'intention est bien de limiter l'application de la mesure envisagée par le Projet au cas où la signature électronique ne peut pas être utilisée. Il y a dès lors lieu **d'ajouter cette précision** dans le dispositif du Projet afin qu'il soit en adéquation avec l'intention qui est réellement poursuivie.

10. Ensuite, en ce qui concerne la **détermination des éléments essentiels** des traitements de données à caractère personnel auxquels le Projet donnera lieu, il importe de veiller à ce que ceux-ci soient délimités dans le Projet de **manière suffisamment précise** ; ce qui n'est pas le cas en l'état du Projet pour ce qui concerne les catégories de personnes concernées à propos desquelles les données sont traitées, les catégories de données qui seront traitées ainsi que les catégories de destinataires. En l'état du Projet, **il n'est en effet pas possible de comprendre concrètement quels types de documents pourront être transmis** de manière digitalisée et sécurisée, au moyen des « *techniques informatiques* » visées**, par qui** (patient ? dispensateur de soins ?autre personne ?) **ni à qui** (un organisme assureur ? autre ?).

11. En outre, il y a lieu de rappeler que tout traitement de données à caractère personnel constitue une ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel, consacré à l'article 8 de la CEDH et à l'article 22 de la Constitution. Une telle ingérence n'est admissible que si elle est nécessaire et proportionnée [12] à l'objectif d'intérêt général qu'elle poursuit. L'auteur d'une norme encadrant un traitement de données à caractère personnel doit être à même de démontrer la réalisation de cette **analyse préalable de nécessité et de proportionnalité**.

12. Le demandeur a été interrogé quant à la **plus-value de la mesure envisagée** par le Projet au regard de l'article 9*bis* de la loi assurance maladie qui concerne les mêmes documents que ceux visés par le Projet et qui prévoit que ceux-ci peuvent être présentés sous format électronique pour autant que les données électroniques répondent aux conditions de qualité prévues à l'article 36/1, §1er de la loi du 21

[10] Voir le point 3 ci-dessus.

[11] Voir les informations complémentaires qui ont été reproduites au point 4 ci-dessus.

[12] Si la nécessité du traitement de données à caractère personnel est démontrée, il faut par ailleurs encore démontrer que celui-ci est proportionné (au sens strict) à l'objectif qu'il poursuit, c'est-à-dire qu'il existe un juste équilibre entre les différents intérêts en présence, droits et libertés des personnes concernées ; en d'autres termes, il y a lieu de vérifier que les inconvénients causés par le traitement tel qu'il est envisagé ne sont pas démesurés par rapport à l'objectif poursuivi.

août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions* soient remplies. Il a répondu ce qui suit :

« *L'article 9 bis de la loi SSI prévoit que 'les documents relatifs à l'assurance soins de santé visés par la présente loi ou par ses arrêtés d'exécution peuvent être présentés, dès que disponible, en version électronique, pour autant que celle-ci bénéficie de la force probante conformément à l'article 36/1, § 1er, de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions'.*

Artikel 36/1, §1 van de eHealth-wet van 21 augustus 2008 betreft de bewijswaarde van de documenten an sich, maar regelt niet de problematiek van de elektronische handtekening.

La disposition proposée vise donc à compléter l'article 9bis et l'article 36/1 précités afin de couvrir les cas où une signature manuscrite est utilisée sans empêcher toute transmission électronique. Le texte sera remanié pour expliquer l'articulation avec l'article 9 bis de la loi SSI. » (souligné par l'Autorité)

Il a également été précisé que « *L'article 9quinquies vise à permettre de travailler sur base d'une copie de signature plutôt que sur la signature originale (papier ou digitale) pour les documents produits en version électronique. L'article 9quinquies ne trouvera donc à s'appliquer que pour les documents pour lesquels l'article 9bis a déjà été mis en œuvre.* » (souligné par l'Autorité)

13. L'Autorité prend bonne note de ce que le Projet sera adapté afin que **l'articulation avec l'article 9*bis*** de la Loi assurance obligatoire y soit dûment **reflétée** : ce qui implique qu'il doit ressortir de manière claire du Projet que l'article 9*quinquies* en projet ne s'appliquera que pour des documents en version électronique pour lesquels l'article 9*bis* a déjà été mis en œuvre et qui comportent une signature manuscrite qui a été « *digitalisée* » en vertu de l'article 9*quinquies* en projet.

II.3. Catégorie de personnes concernées

14. L'Autorité constate que le Projet utilise les termes « ***émetteur*** » et « ***expéditeur*** », qui ne sont pas définis par le Projet. Or, il s'agit de **notions fondamentales** en termes de protection des données à caractère personnel dès lors que l'identification de l' « *émetteur* » doit être établie de manière certaine par les « *techniques informatiques* » qui permettent l'échange digitalisé et sécurisé des documents visés et qu'il incombe à l'« *expéditeur* » de conserver les originaux des documents échangés.

15. Le demandeur a dès lors été interrogé sur la portée de ces termes afin de pouvoir identifier quelles sont les personnes qui sont visées concrètement. Il a répondu que « *L'absence de précision quant à la définition 'd' expéditeur' et 'd'émetteur' est un choix conscient. La disposition vise à permettre une transmission digitalisée sécurisée, probante et valide d'une signature manuscrite sans préciser qui doit être le signataire ou l'émetteur afin de permettre une simplification administrative dans un maximum de cas sans imposer systématiquement une signature électronique qualifiée ou en tenant compte du*

fait qu'elle n'est pas toujours matériellement possible. Il serait par exemple envisageable qu'un document signé par un patient soit transmis à un dispensateur de soin ou un organisme assureur. » A la suite de ces explications, l'Autorité a demandé si la personne dont le Projet souhaite permettre l'identification certaine est la personne qui a apposé sa signature manuscrite sur le document en cause ou la personne qui le transmet ? Le demandeur a répondu que *« L'émetteur est la personne qui transmet le document et doit conserver une copie de l'original. La personne 'authentifiée' peut être l'émetteur et/ou une autre personne (dans nombre de cas le patient) qui n'a pas pu signer digitalement. Pour certaines conventions, l'on peut par exemple imaginer que l'émetteur (dispensateur de soins in casu) signera manuscritement en même temps que le patient (pour acter l'accord sur le plan de soin par exemple) et authentifiera les deux signatures lors de la présentation par voie électronique. »* Il a aussi ajouté que « *We zijn ons ervan bewust dat het gebruik van een dubbele terminologie voor eenzelfde partij ('afzender/verzender' – 'émetteur/expéditeur') de leesbaarheid van de wetsbepaling niet ten goed komt en zullen de wetsbepaling aanpassen om deze dubbele terminologie te vermijden*. »

16. L'Autorité prend note de ce que le Projet sera **adapté afin d'éviter l'utilisation de deux termes différents pour désigner la même personne**. De plus, afin de renforcer la prévisibilité du Projet, il conviendrait de **définir la notion** du terme choisi ou d'en **préciser la portée** en des termes clairs. En outre, si **l'objectif du Projet** est de garantir l'identification certaine et l'authentification[13] non seulement de l' « *émetteur* »/ « *expéditeur* » mais aussi d'une **autre personne** (le signataire ? le patient ?), **cela doit être prévu de manière claire dans le Projet afin de satisfaire au principe de prévisibilité** ; ce qui n'est actuellement pas le cas. Par ailleurs, il convient de veiller à ce que la terminologie utilisée soit cohérente avec ce que prévoit l'article 36/1 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions*, lequel se réfère à l'« *auteur* »/ « *rédacteur* » des données électroniques.

II.3. Catégories de données à caractère personnel traitées

17. Il ressort de l'Exposé des motifs que les documents visés sont « *notamment des documents qui doivent impérativement être signés par le patient parce qu'ils comportent des engagements concrets de suivre son traitement pris par ce dernier dont le non-respect peut entraîner l'arrêt de l'intervention de l'assurance obligatoire.* »

18. Les informations complémentaires communiquées par le demandeur révèlent qu'il n'est pas possible de dresser une liste exhaustive des documents visés par le Projet, eu égard à l'évolution constante de la législation et de la réglementation en matière de soins de santé et d'indemnité résultant des choix politiques et des thérapies mises à disposition des patients. A la suite d'une question relative à la

[13] Voir les observations émises ci-dessous en ce qui concerne l'identification certaine et l'authentification de l' « *émetteur* » et/ou du signataire (points 25 et suivants).

fourniture d'une liste exemplative des documents visés, le demandeur a indiqué qu'il s'agissait « *entre autres des documents que le dispensateur de soins doit envoyer au médecin-conseil de l'organisme assureur pour demander un accord de remboursement par l'assurance maladie obligatoire d'une prestation de soins/d'un traitement. Pour le secteur des opticiens il s'agit par exemple de la demande d'accord au médecin-conseil de l'organisme assureur pour le renouvellement anticipé d'une prothèse oculaire qui est accompagnée d'une prescription et d'un rapport médical. Un autre exemple dans le secteur des audiciens est la demande d'accord relative à la fourniture d'un appareillage de correction auditive qui doit être accompagnée d'une prescription, d'un rapport de test établi par l'audicien et parfois d'un questionnaire COSI*. »

19. Tout en étant consciente de la difficulté de lister de manière exhaustive les documents visés par le Projet, il est recommandé afin de respecter au mieux le principe de prévisibilité et de minimisation des données[14], de **préciser**, au moins **dans l'Exposé des motifs**, de la manière la plus exhaustive possible (le cas échéant, sous la forme d'exemples), **les (type de) documents qui peuvent être échangés au moyen des techniques informatiques visées par le Projet et faire l'objet d'une signature « *digitalisée* » au sens de celui-ci**.

II.4. Exigences fonctionnelles – signature

20. L'article 9*quinquies*, §1er, en projet de la Loi assurance maladie établit les exigences fonctionnelles auquel doit répondre l'échange de documents visés afin d'avoir le même effet juridique que « *l'échange de documents pourvus d'une signature manuscrite ou d'une signature électronique qualifiée* ». Ces exigences fonctionnelles sont de :
    a) permettre d'identifier de manière certaine l'émetteur ;
    b) garantir l'origine et l'intégrité du contenu des documents au moyen de techniques de sécurisation adaptées ;
    c) permettre de déterminer de manière certaine le moment auquel les documents ont été envoyés.

21. Il ressort du Projet ainsi que de son économie que le traitement de données à caractère personnel envisagé s'apparente davantage à une **communication ou une transmission** de documents plutôt qu'à un « *échange* » de documents. Il y a lieu d'**adapter** le Projet en ce sens.

22. Dans le cadre d'une demande d'informations complémentaires, le demandeur a été interrogé sur la question de savoir pourquoi le Projet prévoit que la signature envisagée a le même effet juridique

[14] Ce principe, consacré à l'article 5.1.c) du RGPD, requiert que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

qu'une signature électronique qualifiée, si l'intention du Projet n'est pas de viser une signature électronique qualifiée au sens du Règlement (UE) n° 910/2014 (Règlement eIDAS). Il a répondu que « *La disposition proposée ne donne pas d'effet juridique spécifique à la signature. Elle vise à doter un document d'une force probante suffisante quant à la digitalisation de la signature manuscrite pour que les droits et obligations qui en dépendent puissent être déployés en cas de présentation en version électronique, tout en maintenant des exigences de conservation cohérentes avec les règles actuellement en vigueur.* » Il a aussi été précisé qu' *« il ne s'agit pas ici de créer une nouvelle signature qualifiée mais de permettre la production d'un document comportant la copie d'une signature et de lui permettre d'activer les interventions de l'assurance pour lesquelles le principe est la production d'un document original* ».

23. Dans ces conditions, dès lors que l'intention du Projet n'est pas de donner un effet qualifié, tel que visé par le Règlement eIDAS, à la signature « *digitalisée* » envisagée par le Projet (ni de créer une nouvelle signature qualifiée au sens du Règlement eIDAS), **le Projet prête à confusion lorsqu'il mentionne que l'échange de documents répondant aux conditions visées au paragraphe 1 a le même effet juridique que l'échange de documents pourvus d'une signature électronique qualifiée**. En effet, une telle référence peut être interprétée comme conférant à la signature « *digitalisée* » visée un niveau de confiance élevé conforme aux exigences prévues par le Règlement eIDAS ; ce qui n'est pas l'objectif du Projet et ne pourrait pas l'être dès lors qu'une loi ne peut pas supplanter le règlement eIDAS. Il est dès lors recommandé de **supprimer** cette mention afin d'éviter tout risque de confusion.

24. De plus, l'Autorité comprend, à la lumière des informations complémentaires transmises que l'objectif du Projet est de conférer au document visé qui est signé de manière manuscrite par le patient et/ou le dispensateur de soins et est ensuite « *digitalisé* » et présenté par la voie électronique, **la force probante suffisante à l'intervention de l'assurance soins de santé et indemnité,** pour laquelle le principe est la transmission d'un document original sous format papier comportant une signature manuscrite. En d'autres termes, le respect des exigences fonctionnelle établies à l'article 9*quinquies*, §1er, en projet par la communication de documents envisagé, vise à assurer une équivalence fonctionnelle à la communication de ces documents sur support papier uniquement pour conférer la force probante suffisante à l'octroi de l'intervention de l'assurance soins de santé et indemnité. L'objectif du Projet n'est donc pas de conférer auxdits documents « *digitalisés* » une équivalence fonctionnelle totale aux documents sur format papier puisque l'article 9*quinquies*, §3 en projet impose à l' « *expéditeur* » de conserver les originaux. Il y a dès lors lieu d'**adapter l'article 9quinquies, §2** en projet en ce sens afin qu'y soit **reflété de manière claire l'effet juridique conféré** aux documents visés par le Projet. Une telle approche contribuera également à la détermination de la finalité poursuivie par les communications de données envisagées ainsi que de la catégorie de destinataires (les organismes assureurs) desdits documents.

25. En ce qui concerne **l'exigence relative à l'identification certaine de l' « *émetteur* »**, il ressort des informations complémentaires transmises par le demandeur que cette identification sera effectuée à l'aide d'un certificat d'authentification qui peut être lié à l'eID ou un autre système d'authentification reconnu conformément aux règles applicables.

26. L'Autorité rappelle que l'identification permet de connaître l'identité d'une personne, c'est-à-dire de déterminer l'identité d'un individu au sein d'une certaine population, alors que l'authentification est un processus qui consiste à vérifier cette identité, c'est-à-dire à s'assurer que l'individu est bien la personne qu'il prétend être. Elle peut, de manière générale, être réalisée au moyen de différents facteurs d'authentification (qui peuvent être combinés) : soit, par une information que la personne concernée est la seule à connaître, tel un mot de passe, soit par une information qu'elle est la seule à détenir, tel qu'un token ou un badge, soit par une information qui la caractérise, telle qu'une caractéristique biométrique. Dans la mesure où le Projet vise également à garantir **l'authentification** de l' « *émetteur* », cela devrait être **reflété** dans le Projet.

27. S'agissant de l'authentification de l' « *émetteur* », ainsi que cela ressort des informations complémentaires reprises au point 25 ci-dessus, celle-ci sera réalisée au moyen du certificat d'authentification qui est lié à l' eID ou à un autre système d'authentification reconnu conformément aux règles applicables et se combine avec l'obligation de conservation du document original. Le demandeur a également précisé que « *Die afzender/verzender wordt met zekerheid geïdentificeerd dankzij de informaticatechnieken die ook toelaten om de oorsprong en integriteit van de inhoud van de documenten te verzekeren alsook het tijdstip van de verzending van het document.*
De authenticatie van de afzender/verzender is noodzakelijk om de toegang tot de dienst van eHealth platform te beperken tot de toegelaten partijen en te garanderen dat enkel een rechtmatig eigenaar van een archief zijn eigen gegevens kan opvragen.
Binnen de context van deze dienst werden geen andere toegangscontrolemaatregelen nodig geacht."
L'Autorité prend note de ces explications. Elle estime que, dès lors que la transmission de documents en cause interviendra nécessairement pour des documents dont l'article 9*bis* de la Loi assurance maladie a déjà été mis en œuvre et pour autant que l'articulation entre l'article 9*quinquies* en projet et l'article 9*bis* précité soit dûment reflétée[15], il n'est pas nécessaire de préciser dans le Projet par quels moyens l'authentification de l' « *émetteur* » sera effectuée.

[15] Voir les points 12 et 13 ci-dessus. L'article 9*bis* de la Loi assurance maladie renvoie à l'article 36/1, §1er de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions,* lequel prévoit que les données électroniques ont le même force probante que celle qu'elles auraient eue si elle étaient communiquées sur un support papier pour autant que notamment « *les données électroniques mentionnent l'identité de l'auteur de ces données, authentifiée soit à l'aide du certificat d'identité présent sur la carte d'identité électronique ou d'un autre certificat qui satisfait aux dispositions du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, soit à l'aide d'une procédure dont la chambre sécurité sociale et santé du comité de sécurité de l'information a constaté qu'elle offre les mêmes garanties* ».

28. En outre, il convient de veiller à ce qu'il **ressorte de manière claire du Projet de quelle personne** (dispensateur de soins ? émetteur/ expéditeur ? patient ?) **émane la signature manuscrite** qui a été apposée sur le document communiqué en vertu du Projet. En effet, il ressort des informations complémentaires transmises que dans certaines situations l'émetteur ne sera pas nécessairement la (seule) personne qui a apposé sa signature manuscrite sur le document en cause et que dans ce cas, l'émetteur (à savoir le dispensateur de soins) signera manuscritement ledit document en même temps que le patient et authentifiera les deux signatures lors de la présentation du document par voie électronique. Le Projet doit être **adapté** afin de prévoir que dans l'hypothèse où l' « *émetteur* » n'est pas la même personne que le signataire (la personne qui a apposé la signature manuscrite sur le document en cause), l'authentification de cette dernière personne sera effectuée par l' « *émetteur* » lors de la présentation du document concerné dans le circuit électronique.

29. S'agissant des mesures mises en place par le Projet afin de garantir **l'authenticité de la signature manuscrite** (qui est « *digitalisée* » en vertu du Projet) apposée sur les documents visés, en particulier dans l'hypothèse où le signataire est le patient et est donc une personne différente de l' « *émetteur* »/l' *« expéditeur* », les informations complémentaires communiquées par le demandeur indiquent que « *l'ensemble des éléments mis en place (authentification de l'expéditeur, transmission sécurisée, horodatage, combiné avec l'obligation de conservation de l'original comportant la signature manuscrite et le cas échéant la date de signature si le document à produire le requiert)* » entend permettre de garantir une telle authentification. L'Autorité en prend note.

II.4. Approbation par le Comité de sécurité de l'information (« CSI ») des « *techniques informatiques* » qui devront être utilisées

30. L'article 9*quinquies*, §1er, alinéa 2 en projet prévoit qu'il revient à la chambre sécurité sociale et santé du CSI d'approuver les techniques informatiques visées audit paragraphe 1.

31. L'article 22 de la Constitution interdit au législateur de renoncer à la possibilité de définir lui-même les ingérences qui peuvent venir restreindre le droit au respect de la vie privée. En ce qui concerne plus particulièrement les **délibérations du CSI**, la Cour constitutionnelle a rappelé ce principe, dans son arrêt n° 110/2022[16] rendu le 22 septembre 2022, en confirmant que c'est au législateur lui-même qu'il appartient de définir les éléments essentiels du traitement de données et que cela ne peut pas se faire par une délibération du CSI. Dans ce contexte, l'Autorité tient aussi à rappeler son avis n° 268/2022[17]

[16] Voir en particulier les points B.35 à B.40 dont les points de vue en la matière sont résumés comme suit dans le communiqué de presse de la Cour constitutionnelle : « *La Cour rappelle que l'article 22 de la Constitution réserve au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée et familiale. Une habilitation à un autre pouvoir est cependant admissible, pour autant qu'elle soit définie de manière suffisamment précise et que le législateur ait lui-même fixé les éléments essentiels. [….]* »

[17] https://www.autoriteprotectiondonnees.be/publications/avis-n-268-2022.pdf

rendu le 21 décembre 2022, en particulier, ses points 31, 32 et le dispositif qui portent sur l'étendue de l'habilitation conférée au CSI et desquels il ressort que dans le cadre de ses délibérations, le CSI ne peut être **habilité qu'à fixer des éléments purement techniques**, si cela s'avère nécessaire pour assurer une protection des données dès la conception et par défaut et pour autant que la détermination de ces éléments techniques emporte uniquement l'exercice d'un pouvoir discrétionnaire très limité. L'Autorité se réfère aussi à l'article 46, §2 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale,* qui dispose ce qui suit :
« *Les délibérations du comité de sécurité de l'information ne peuvent pas être contraires aux normes juridiques supérieures et les parties qui participent à la communication des données à caractère personnel respectent les mesures contenues dans la délibération.*
Les délibérations du comité de sécurité de l'information ont une ***portée limitée et technique*** *et décrivent pour une situation déterminée et pendant une période déterminée* ***l'application des éléments essentiels*** *du traitement, qui sont définis dans les bases juridiques visées à l'article 6 du 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. […] »*[18] (mis en gras par l'Autorité)

32. En l'occurrence, **l'habilitation** conférée au CSI est rédigée de **manière très large** (« *approuver les techniques informatiques* » visées au paragraphe 1), ce qui peut être interprété comme permettant audit Comité de compléter ou modifier les éléments essentiels déterminés dans le Projet (par exemple en créant de nouveaux flux de données et/ou en déterminant de nouveaux destinataires des données/documents). Il y a dès lors lieu de **revoir la formulation** de l'habilitation confiée au CSI afin qu'elle soit **clairement limitée** à l'approbation des modalités purement techniques des « *techniques informatiques* » visées afin de garantir une transmission sécurisée des documents visés. Il convient également de **préciser** dans le Projet que les délibérations par lesquelles ces techniques seront approuvées seront des délibérations, telles que visées à l'article 46, §2 de la loi précitée du 15 janvier 1990.

33. En outre, l'Autorité relève que selon le règlement d'ordre intérieur[19] du CSI, les collaborateurs de la Banque Carrefour de la sécurité sociale et de la plateforme eHealth qui ont préparé les dossiers peuvent assister aux réunions de la chambre sécurité sociale et santé du CSI avec un pouvoir consultatif. L'Autorité y voit un potentiel **conflit d'intérêts** dans la mesure où les collaborateurs de la plateforme eHealth prépareraient pour le CSI des délibérations portant approbation de « *techniques informatiques* » mises en oeuvre et utilisées par la plateforme eHealth. Il doit être remédié à cette situation.

---

[18] L'article 46, §2, dernier alinéa de la loi précitée du 15 janvier 1990 dispose également que « *Les délibérations du comité de sécurité de l'information constituent des mesures administratives, qui peuvent être contestées auprès de la section du contentieux administratif du Conseil d'Etat, sur la base de l'article 14 des lois coordonnées sur le Conseil d'Etat.*»

[19] Voir l'article 4, §2, alinéa 2 de l'arrêté royal du 5 décembre 2023 portant approbation du règlement d'ordre intérieur du comité de sécurité de l'information.

34. Par ailleurs, le demandeur a été interrogé sur le point de savoir si les trois services de signature électronique qualifiés existant en Belgique (itsme, eID et le portefeuille d'identité numérique) pourront toujours être utilisés par les personnes concernées dans la mesure où le Projet s'appliquera dans les situations où la signature électronique qualifiée ne peut pas être utilisée et que les techniques informatiques qui permettront l'échange de documents, tel que visé par le Projet, devront être approuvées par le CSI. Le demandeur a répondu ce qui suit : « *De diensten Itsme, de eID en de digitale portefeuille kunnen vanzelfsprekend verder worden gebruikt voor het plaatsen van gekwalificeerde elektronische handtekeningen (zonder goedkeuring van het IVC). Het IVC moet enkel goedkeuring verlenen voor vermelde alternatieve oplossing pour les situations où justement ces modes de signatures ne peuvent pas être appliqués*. » L'Autorité en prend note.

II.5. Conservation des documents originaux

35. Il convient de **compléter** le Projet afin que la durée de conservation des documents transmis visés par le Projet soit mentionnée.

PAR CES MOTIFS,
L'Autorité recommande de/d':

1. préciser dans le Projet que son champ d'application est limité aux situations dans lesquelles la signature électronique qualifiée ne peut pas être utilisée (**cons. 9**) ;
2. adapter le Projet afin que l'articulation avec l'article 9*bis* de la Loi assurance maladie soit dûment reflétée (**cons. 13**) ;
3. éviter d'utiliser deux termes différents (« *émetteur* »/ « *expéditeur* ») pour désigner la même personne et définir la notion du terme choisi ou en préciser la portée en des termes clairs et veiller à ce que l'identification certaine et l'authentification de toutes les personnes concernées soient mentionnée dans le Projet (**cons. 16**) ;
4. préciser, au moins dans l'Exposé des motifs, de la manière la plus exhaustive possible, les (type de) documents qui peuvent être échangés en vertu du Projet (**cons. 19**) ;
5. adapter le Projet afin qu'il soit fait référence à une communication ou une transmission de documents plutôt qu'à un « *échange* » de documents (**cons. 21**) ;
6. supprimer la mention relative au même effet juridique que l'échange de documents pourvus d'une signature électronique qualifiée (**cons. 23**) ;
7. préciser dans le Projet l'effet juridique conféré aux documents visés, à savoir donner la force probante suffisante à l'intervention de l'assurance soins de santé et indemnité (**cons. 24**) ;

8. préciser au paragraphe 1, a), du Projet que l'authentification de l' « *émetteur* » est aussi visée (**cons. 26**) ;

9. prévoir que dans l'hypothèse où l' « *émetteur* » n'est pas la même personne que le signataire (la personne qui a apposé la signature manuscrite sur le document en cause), l'authentification de cette dernière personne sera effectuée par l' « *émetteur* » lors de la présentation du document concerné dans le circuit électronique (**cons. 28**) ;

10. revoir la formulation de l'habilitation confiée au CSI afin qu'elle soit clairement limitée à l'approbation des modalités purement techniques des « *techniques informatiques* » visées et préciser dans le Projet que les délibérations par lesquelles ces techniques seront approuvées seront des délibérations, telles que visées à l'article 46, §2 de la loi précitée du 15 janvier 1990 (**cons. 32**) ;

11. remédier au potentiel conflit d'intérêts existant entre la plateforme ehealth et le CSI dans la mesure où les collaborateurs de la plateforme eHealth prépareraient pour le CSI des délibérations portant approbation de « *techniques informatiques* » mises en oeuvre et utilisées par la plateforme eHealth (**cons. 33**) ;

12. mentionner la durée de conservation des documents visés par le Projet (**cons. 35**).

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