

**Art. 2.** L'article 16, § 6, du même arrêté est retiré.

**Art. 3.** L'article 16, § 8, du même arrêté est remplacé comme suit :

"L'article 22, alinéas 1<sup>er</sup>, 4 et 5, de l'arrêté royal du 3 mai 2007 susvisé, tel qu'il était d'application avant le 1<sup>er</sup> janvier 2015, reste d'application à partir du 1<sup>er</sup> janvier 2015 aux travailleurs qui :

1° soit ont demandé, avant le 1<sup>er</sup> janvier 2015, pour la première fois des allocations de chômage avec complément d'entreprise;

2° soit ont été licenciés avant le 1<sup>er</sup> janvier 2015.

L'article 22, alinéas 2 à 5, de l'arrêté royal du 3 mai 2007 susvisé, tel qu'il était d'application avant le 1<sup>er</sup> janvier 2015, reste d'application à partir du 1<sup>er</sup> janvier 2015 aux travailleurs qui ont été licenciés en vue de l'obtention du statut de chômeur avec complément d'entreprise en application du chapitre 7 de l'arrêté royal du 3 mai 2007 précité, si la date du début de la période de reconnaissance visée à l'article 18, § 1<sup>er</sup>, alinéa 1<sup>er</sup> ou 2, de l'arrêté royal du 3 mai 2007 précité, est située avant le 9 octobre 2014.

L'article 22, alinéa 6, de l'arrêté royal du 3 mai 2007 susvisé, tel qu'il était d'application avant le 1<sup>er</sup> janvier 2015, reste d'application à partir du 1<sup>er</sup> janvier 2015 :

1° aux travailleurs qui ont été licenciés avant le 1<sup>er</sup> janvier 2015;

2° aux travailleurs qui ont été licenciés dans le cadre d'un licenciement collectif annoncé avant le 9 octobre 2014.

Le chômeur visé au présent paragraphe peut, par dérogation à l'article 45, alinéa 1<sup>er</sup>, 1<sup>o</sup>, de l'arrêté royal du 25 novembre 1991 portant réglementation du chômage, effectuer, pour son propre compte et sans but lucratif, toute activité qui concerne ses biens propres."

**Art. 4.** Le présent arrêté produit ses effets à partir du 1<sup>er</sup> janvier 2015.

**Art. 5.** Le Ministre qui a l'Emploi dans ses attributions est chargé de l'exécution du présent arrêté.

Donné à Bruxelles, le 1<sup>er</sup> juin 2015.

PHILIPPE

Par le Roi :

Le Ministre de l'Emploi  
K. PEETERS

**Art. 2.** Artikel 16, § 6, van hetzelfde besluit wordt ingetrokken.

**Art. 3.** Artikel 16, § 8, van hetzelfde besluit wordt vervangen als volgt :

"Artikel 22, eerste, vierde en vijfde lid, van het voormeld koninklijk besluit van 3 mei 2007, zoals van toepassing vóór 1 januari 2015, blijft vanaf 1 januari 2015 van toepassing op de werknemers die :

1° ofwel vóór 1 januari 2015 voor de eerste keer werkloosheidsuitkeringen met bedrijfstoeslag hebben gevraagd;

2° ofwel vóór 1 januari 2015 zijn ontslagen.

Artikel 22, tweede tot vijfde lid, van het voormeld koninklijk besluit van 3 mei 2007, zoals van toepassing vóór 1 januari 2015, blijft vanaf 1 januari 2015 van toepassing op de werknemers die zijn ontslagen met het oog op het verkrijgen van het statuut van werkloze met bedrijfstoeslag in toepassing van hoofdstuk 7 van het voormeld koninklijk besluit van 3 mei 2007, indien de begindatum van de periode van erkenning bedoeld in artikel 18, § 1, eerste of tweede lid, van het voormeld koninklijk besluit van 3 mei 2007, gelegen is vóór 9 oktober 2014.

Artikel 22, zesde lid, van het voormeld koninklijk besluit van 3 mei 2007, zoals van toepassing vóór 1 januari 2015, blijft vanaf 1 januari 2015 van toepassing :

1° op de werknemers die vóór 1 januari 2015 werden ontslagen;

2° op de werknemers die werden ontslagen in het kader van een collectief ontslag aangekondigd vóór 9 oktober 2014.

De werkloze bedoeld in de huidige paragraaf mag, in afwijking van artikel 45, eerste lid, 1<sup>o</sup>, van het koninklijk besluit van 25 november 1991 houdende de werkloosheidsreglementering, voor eigen rekening en zonder winstoogmerk elke activiteit uitoefenen die betrekking heeft op zijn eigen bezit."

**Art. 4.** Dit besluit heeft uitwerking vanaf 1 januari 2015.

**Art. 5.** De Minister bevoegd voor Werk is belast met de uitvoering van dit besluit.

Gegeven te Brussel, le 1 juni 2015.

FILIP

Van Koningswege :

De Minister van Werk,  
K. PEETERS

SERVICE PUBLIC FEDERAL  
SECURITE SOCIALE

[2015/202705]

10 MAI 2015. — Arrêté royal relatif à la force probante des données enregistrées, traitées, communiquées au moyen de techniques photographiques et optiques par les hôpitaux, ainsi qu'à leur reproduction sur papier ou sur tout autre support lisible pour l'application dans les soins de santé

RAPPORT AU ROI

Sire,

L'arrêté royal que j'ai l'honneur de soumettre à la signature de Votre Majesté est pris en exécution de l'article 36/1, § 2, de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions.

Aux termes de cet article 36/1, § 2, le Roi s'est vu confier par le législateur la mission de déterminer les conditions selon lesquelles une force probante jusqu'à preuve du contraire peut être attribuée à des données enregistrées, traitées ou communiquées au moyen de techniques photographiques et optiques, ainsi qu'à leur reproduction sur papier ou sur tout autre support lisible pour l'application dans les soins de santé.

Les acteurs du secteur des soins de santé, et en particulier les hôpitaux - auxquels le présent projet est limité -, traitent de plus en plus les informations qui leur sont nécessaires pour remplir leurs missions au moyen de techniques photographiques et optiques. Cette façon de procéder présente, en effet, plusieurs avantages. Ainsi, par exemple, il

FEDERALE OVERHEIDSDIENST  
SOCIALE ZEKERHEID

[2015/202705]

10 MEI 2015. — Koninklijk besluit betreffende de bewijskracht van de gegevens die door de ziekenhuizen worden opgeslagen, verwerkt of meegedeeld door middel van een optische en fotografische techniek, evenals van weergave op papier of op elke andere leesbare drager, voor de toepassing in de gezondheidszorg

VERSLAG AAN DE KONING

Sire,

Het ontwerp van koninklijk besluit waarvan ik de eer heb het ter ondertekening aan Uwe Majesteit voor te leggen, wordt genomen in uitvoering van artikel 36/1, § 2, van de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen.

Overeenkomstig artikel 36/1, § 2, van die wet kreeg de Koning van de wetgever de opdracht om de voorwaarden te bepalen volgens welke een bewijskracht tot bewijs van het tegendeel kan worden toegekend aan gegevens die door middel van een optische en fotografische techniek worden opgeslagen, verwerkt of meegedeeld, evenals aan hun weergave op papier of op elke andere leesbare drager, voor de toepassing in de gezondheidszorg.

De actoren in de gezondheidszorg en in het bijzonder de ziekenhuizen - waartoe dit ontwerp beperkt is - verwerken de gegevens die zij nodig hebben voor het vervullen van hun opdrachten steeds meer door middel van een optische en fotografische techniek. Deze werkwijze biedt immers een aantal voordelen. Zo kan het bijvoorbeeld nuttig zijn

peut s'avérer utile de numériser des documents papier pour notamment faciliter leur gestion et leur accès, pour les préserver d'éventuelles menaces ou encore pour tout simplement gagner de la place en détruisant les documents papier.

L'introduction de ces procédés soulève cependant une question juridique relative à la force probante.

L'existence de cette force probante est néanmoins nécessaire pour garantir le bon fonctionnement du secteur des soins de santé.

Le présent projet a pour objectif de définir les conditions auxquelles les procédures d'enregistrement, de traitement, de communication et de reproduction utilisées par les hôpitaux doivent satisfaire pour être suffisamment sûres.

Dans la mesure où les procédures utilisées par les hôpitaux répondent aux critères énoncés dans le projet, les données enregistrées, traitées ou communiquées au moyen de techniques photographiques et optiques, ainsi que leur reproduction sur papier ou sur tout autre support lisible reçoivent force probante, jusqu'à preuve du contraire.

Lors de l'élaboration du présent arrêté royal, il a été tenu compte de normes internationalement reconnues et éprouvées. Le cadre de référence est (partiellement) basé sur la liste de normes non-exhaustive suivante :

- la norme ISO 13028 (Information et documentation - Mise en œuvre des lignes directrices pour la numérisation des enregistrements);
- la norme de sécurité ISO/IEC 27002, Technologies de l'information - Techniques de sécurité;
- le code de bonne pratique pour le management de la sécurité de l'information;
- la norme ISO 15489 (Information et documentation — « Records management »);
- le MoReq2 (Model Requirements for the management of electronic records);
- la norme ISO 15801 : 2009, Images électroniques - Stockage électronique d'informations - Recommandations pour les informations de valeur et leur fiabilité;
- la norme NF Z 42-013 d'AFNOR (Association française de normalisation);
- PDF/A (Portable Document Format Archivable, connu aussi comme la norme ISO 19005-1);
- la norme ISO 23081 : 2006 (Processus de gestion des enregistrements - Métadonnées pour les enregistrements);
- la norme ISO 14721 : 2002 (modèle de référence pour un OAIS).

Le RODIN (Referentiekader Opbouw Digitaal Informatiebeheer), un instrument pour l'organisation des environnements de gestion numériques, qui a été mis au point par le Nederlandse Landelijk Overleg van Provinciale Archiefinspecteurs (LOPAI) constitue également une importante référence pour le présent arrêté royal.

#### COMMENTAIRES DES ARTICLES

**Art. 1.** Cet article définit le champ d'application matériel des dispositions proposées par le projet.

**Art. 2.** Cet article prévoit que les informations enregistrées, traitées ou communiquées selon des procédés photographiques et optiques ainsi que leur reproduction sur papier ou sur tout autre support lisible ont force probante, jusqu'à preuve du contraire, si la procédure fixée par l'hôpital pour leur enregistrement, leur traitement, leur communication ou leur reproduction satisfait aux conditions énumérées dans le présent projet et si les données sont enregistrées, traitées ou communiquées conformément à cette procédure.

Le second alinéa dispose que les données numérisées ne peuvent être privées de leur validité juridique au seul motif qu'il est contesté que la procédure réellement suivie réponde aux conditions du présent arrêté si celui qui a recours à ces données est en mesure de montrer par tous les moyens de droit que la dérogation par rapport aux conditions du présent arrêté n'a pas remis en question la fiabilité des données.

Dans son avis n° 57.117/3 du 18 mars 2015, le Conseil d'Etat constate que plusieurs conditions prévues dans les articles 4 à 11 (actuels) du projet portent non seulement sur les exigences intrinsèques auxquelles doivent répondre les données numérisées, mais aussi sur l'organisation proprement dite des systèmes informatiques des hôpitaux. La compétence résiduaire des pouvoirs fédéraux de définir le régime de preuve pour des données ne devrait pas être interprétée de manière aussi large que cela implique que la détermination des conditions de la procédure d'enregistrement, de traitement, de communication ou de reproduction

om papieren documenten te digitaliseren om het beheer van en de toegang tot deze documenten te vereenvoudigen, ze te beschermen tegen eventuele risico's of om eenvoudigweg ruimte te winnen door papieren documenten te vernietigen.

De invoering van deze technieken roept echter een juridische vraag op met betrekking tot de bewijskracht.

Het bestaan van deze bewijskracht is echter noodzakelijk om de goede werking van de sector van de gezondheidszorg te waarborgen.

Het doel van dit ontwerp van koninklijk besluit is om de voorwaarden te bepalen waaraan de procedures die het ziekenhuis gebruikt voor de opslag, de verwerking, de mededeling en de weergave moeten voldoen om voldoende veilig te zijn.

Voor zover de gebruikte procedures in de ziekenhuizen voldoen aan de criteria die in het ontwerp vermeld worden, hebben de gegevens die door middel van een optische en fotografische techniek opgeslagen, verwerkt of meegedeeld worden, alsook de weergave van deze gegevens op papier of op elke andere leesbare drager, bewijskracht tot bewijs van het tegendeel.

Voor de uitwerking van dit koninklijk besluit werd rekening gehouden met internationaal erkende en bewezen standaarden. Het referentiekader is gebaseerd op (delen) van de volgende niet-exhaustieve lijst van normen :

- ISO 13028 (Information and documentation - Implementation guidelines for digitization of records);
- de beveiligingsnorm ISO/IEC 27002, Information technology - Security techniques;
- code of practice for information security management;
- ISO 15489 (Information and documentation — Records management/informatie- en archiefmanagement);
- MoReq2 (Model Requirements for the management of electronic records);
- ISO 15801 : 2009, Document management — Information stored electronically — Recommendations for trustworthiness and reliability;
- de norm NF Z 42-013 van AFNOR (l'Association française de normalisation);
- PDF/A (Portable Document Format Archivable, ook bekend als ISO 19005-1);
- ISO 23081 : 2006 (Processen voor informatie- en archiefmanagement);
- ISO-14721 : 2002 (referentiemodel voor digitale depots OAIS).

Een belangrijke referentie voor dit koninklijk besluit is tevens RODIN (Referentiekader Opbouw Digitaal Informatiebeheer), een instrument voor het inrichten van digitale beheersomgevingen opgesteld door het Nederlandse Landelijk Overleg van Provinciale Archiefinspecteurs (LOPAI).

#### BESPREKING VAN DE ARTIKELEN

**Art. 1.** Dit artikel bepaalt het materieel toepassingsgebied van de bepalingen van het ontwerp.

**Art. 2.** In dit artikel wordt bepaald dat de gegevens die door middel van een optische en fotografische techniek opgeslagen, verwerkt of meegedeeld worden, alsook de weergave van deze gegevens op papier of op elke andere leesbare drager, bewijskracht hebben tot bewijs van het tegendeel, indien de door het ziekenhuis vastgestelde procedure voor hun opslag, verwerking, mededeling of weergave voldoet aan de voorwaarden die in dit ontwerp vermeld worden en de gegevens in overeenstemming met die procedure werden opgeslagen, verwerkt of meegedeeld.

Het tweede lid bepaalt dat de gedigitaliseerde gegevens echter geen rechtsgeldigheid kan worden ontzegd op de enkele grond dat betwist wordt dat de werkelijk gevolgde procedure aan de voorwaarden van dit besluit voldoet, als diegene die zich op deze gegevens beroept kan aantonen, met alle middelen van recht, dat de afwijking van de voorwaarden in dit besluit de betrouwbaarheid van de gegevens niet in het gedrang heeft gebracht.

De Raad van State stelt in zijn advies nr. 57.117/3 van 18 maart 2015 vast dat verscheidene voorwaarden bedoeld in de (huidige) artikelen 4 tot 11 van het ontwerp niet louter betrekking hebben op de intrinsieke vereisten waaraan de gedigitaliseerde gegevens zelf moeten voldoen maar ook betrekking hebben op de eigenlijke organisatie van de informaticasystemen in de ziekenhuizen. De residuaire bevoegdheid van de federale overheid om een bewijsregeling voor gegevens vast te stellen, zou niet zo ruim kunnen worden begrepen dat zij door het bepalen van de voorwaarden van de procedure voor de opslag, de

de données numérisées dans les hôpitaux règle également l'organisation générale de leurs systèmes informatiques, ceci étant une compétence des communautés.

Les conditions prévues dans les articles en question sont toutefois indistinctement essentielles pour garantir que les données numérisées soient conformes à la réalité. Afin de garantir la sécurité juridique, la force probante ne peut être accordée aux données numérisées que si des mesures strictes ont été appliquées lors de la numérisation. Bien que les conditions imposées aient certes, dans une certaine mesure, un impact sur la manière dont les hôpitaux gèrent leurs systèmes informatiques, ces conditions visent uniquement la qualité des données numérisées. Conformément aux articles 4, 5 et 10 (précédemment 3, 4 et 9), les hôpitaux qui souhaitent avoir recours au régime doivent développer à cet effet une procédure minutieusement documentée qui ne laisse aucun doute quant à la concordance complète entre les données initiales et les données numérisées. L'article 6 (précédemment 5) dispose explicitement que l'hôpital applique ses propres règles pour l'accès aux données numérisées. Les articles 7 et 8 (précédemment 6 et 7) visent un enregistrement parfait des données numérisées. L'article 9 (précédemment 8) vise le traitement correct des données numérisées : ces données peuvent uniquement être traitées conformément à la réglementation stricte de l'Union européenne en matière de protection de la vie privée. Finalement, l'article 11 (précédemment 10) dispose que l'hôpital est tenu de développer une politique de sécurité de l'information répondant à certaines conditions.

Il est à noter que l'application du régime proposé est tout à fait libre. Les hôpitaux ne sont pas obligés d'y avoir recours. Or s'ils l'appliquent, ils sont tenus de respecter les conditions précitées.

**Art. 3.** Le système prévu dans le présent projet concernant la force probante des données enregistrées, traitées ou communiquées au moyen de techniques photographiques et optiques, ainsi que leur reproduction sur papier ou sur tout autre support lisible s'appliquera à toutes les informations que les hôpitaux sont amenés à traiter dans le cadre de leurs missions.

**Art. 4.** Cette disposition énonce les conditions générales auxquelles les procédures doivent satisfaire. Ainsi, l'hôpital s'assurera que la procédure mise en œuvre prévoit l'enregistrement systématique et sans lacunes des données. L'hôpital veillera également, compte tenu du volume des données numérisées à conserver, à les organiser et les rationaliser avec soin afin de pouvoir les retrouver au moment opportun. L'intégrité des informations, ainsi que leur lisibilité devront être garanties durant toute la période de conservation. A cet égard, il est renvoyé aux règles en matière de délai de conservation prévues par les réglementations en vigueur.

**Art. 5.** L'hôpital doit disposer d'une documentation détaillée et actualisée de la procédure utilisée contenant au minimum les éléments énoncés dans cette disposition.

Le présent projet autorise la sous-traitance (complète ou partielle). En ce domaine, il peut en effet être intéressant de recourir au savoir-faire d'un tiers. Cela ne pourra cependant avoir lieu qu'à la condition d'encadrer son intervention de certaines garanties contractuelles relatives notamment aux mesures de sécurité mises en place (article 11 du présent projet). En cas de sous-traitance (complète ou partielle), la documentation mentionnera le nom, l'adresse, le numéro d'identification à la T.V.A. du tiers concerné.

Concernant la dénomination du logiciel utilisé, il semble opportun que celle-ci soit la plus complète possible (nom, numéro de version, date de release, fournisseur et, le cas échéant, les services packs ou les patches installés).

Quant aux contrôles de qualité dont il est question au 6°, il est utile que ce processus de contrôle soit systématique et permanent.

Toutes les modifications apportées à la procédure utilisée devront être consignées sans délai dans la documentation. Ainsi par exemple, les éventuelles migrations d'un système vers un autre système (interne ou externe à l'hôpital) devront faire l'objet d'une documentation qui devra être ajoutée à la documentation de la procédure utilisée.

Aux termes de l'article 5, alinéa 4, toute procédure utilisée par un hôpital peut faire l'objet d'un contrôle a posteriori du Comité sectoriel de la sécurité sociale et de la santé.

**Art. 6.** Seules les personnes physiques habilitées à consulter les données numérisées pourront y avoir accès. Cette habilitation se justifie notamment par la profession de l'utilisateur.

verwerking, de mededeling of de weergave van gedigitaliseerde gegevens in ziekenhuizen ook de algemene organisatie van hun informaticasystemen zou kunnen regelen, een bevoegdheid die de gemeenschappen toekomt.

De in de betrokken artikelen opgenomen voorwaarden zijn evenwel zonder onderscheid essentieel om het waarheidsgetrouwe karakter van de gedigitaliseerde gegevens te waarborgen. Er kan, met het oog op de rechtszekerheid, slechts bewijskracht aan de gedigitaliseerde gegevens worden toegekend indien bij het digitaliseren strenge maatregelen werden toegepast. Hoewel de opgelegde voorwaarden inderdaad enige impact hebben op de wijze waarop de ziekenhuizen hun informaticasystemen in het algemeen beheren, beogen zij uitsluitend de kwaliteit van de gedigitaliseerde gegevens. Overeenkomstig de artikelen 4, 5 en 10 (voorheen 3, 4 en 9) moeten ziekenhuizen die een beroep willen doen op de regeling daartoe een grondig gedocumenteerde procedure ontwikkelen die geen twijfels kan doen rijzen aangaande de volledige overeenstemming tussen de oorspronkelijke gegevens en de gedigitaliseerde gegevens. Artikel 6 (voorheen 5) bepaalt uitdrukkelijk dat het ziekenhuis voor de toegang tot de gedigitaliseerde gegevens gebruik maakt van de eigen regels. Met de artikelen 7 en 8 (voorheen 6 en 7) wordt een perfecte opslag van de gedigitaliseerde gegevens beoogd. Ook artikel 9 (voorheen 8) heeft de correcte verwerking van de gedigitaliseerde gegevens tot doel : zij mogen enkel worden verwerkt overeenkomstig de strikte regeling van de Europese Unie tot bescherming van de persoonlijke levenssfeer. Artikel 11 (voorheen 10), ten slotte, stelt dat het ziekenhuis zelf een informatieveiligheidsbeleid moet ontwikkelen dat aan bepaalde voorwaarden voldoet.

Het weze overigens benadrukt dat de toepassing van de voorgestelde regeling louter vrijwillig is. Ziekenhuizen zijn niet verplicht om er een beroep op te doen maar als ze dat willen, moeten ze wel de voormelde voorwaarden respecteren.

**Art. 3.** Het systeem zoals bepaald in dit ontwerp van koninklijk besluit betreffende de bewijskracht van gegevens die door middel van een optische en fotografische techniek opgeslagen, verwerkt of meegedeeld worden, alsook de weergave van deze gegevens op papier of op elke andere leesbare drager, is van toepassing op alle gegevens die de ziekenhuizen in het kader van hun opdrachten moeten verwerken.

**Art. 4.** In deze bepaling worden de algemene voorwaarden vermeld waaraan de procedures moeten voldoen. Zo verzekert het ziekenhuis dat de uitgevoerde procedure voorziet in een systematische gegevensopslag zonder lacunes. Het ziekenhuis ziet, rekening houdend met de hoeveelheid gegevens die bewaard moeten worden, tevens toe op de zorgvuldige organisatie en rationalisatie van deze gegevens om ze op het juiste moment te kunnen terugvinden. De integriteit en de leesbaarheid van de gegevens moeten gedurende de volledige bewaartermijn gewaarborgd worden. Hiertoe wordt verwezen naar de regels inzake de bewaartermijn die door de geldende voorschriften worden bepaald.

**Art. 5.** Het ziekenhuis moet over een gedetailleerde en geactualiseerde documentatie beschikken met betrekking tot de gehanteerde procedure met op zijn minst de onderdelen die in deze bepaling opgesomd worden.

In dit ontwerp wordt de (volledige of gedeeltelijke) onderaanneming gemachtigd. Op dat vlak kan het immers interessant zijn om een beroep te doen op de vakkennis van een derde. Dit kan echter enkel gebeuren indien de tussenkomst kadert binnen bepaalde contractuele garanties o.a. met betrekking tot de uitgevoerde veiligheidsmaatregelen (artikel 11 van dit ontwerp). Bij (volledige of gedeeltelijke) onderaanneming worden de naam, het adres en het btw-identificatienummer van de betrokken derde meegedeeld in de documentatie.

Wat de benaming van de gebruikte software betreft, lijkt het aangewezen dat die benaming zo volledig mogelijk is (naam, versienummer, releasedatum, leverancier en in voorkomend geval de service packs of de geïnstalleerde patches).

Wat de kwaliteitscontrole betreft waarvan sprake onder punt 6°, dient dit controleproces systematisch en permanent te zijn.

Alle aan de gebruikte procedure aangebrachte wijzigingen moeten onverwijld in de documentatie opgenomen worden. Zo moeten de eventuele migraties van het ene systeem naar het andere (in het ziekenhuis of daarbuiten) vermeld worden in een documentatie die aan de documentatie van de gebruikte procedure toegevoegd moet worden.

Overeenkomstig artikel 5, vierde lid, kan elke procedure die gebruikt wordt door een ziekenhuis, a posteriori gecontroleerd worden door het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid.

**Art. 6.** Enkel de natuurlijke personen die gemachtigd zijn om de gedigitaliseerde gegevens te raadplegen, hebben er toegang toe. Deze machtiging wordt in het bijzonder gerechtvaardigd door het beroep van de gebruiker.

Toute opération (création, consultation, modification des métadonnées,...) sur les données numérisées sera conservée dans un fichier reprenant l'identité de la personne qui a effectué cette opération.

**Art. 7.** Les données numérisées pourront uniquement être conservées dans des formats de fichiers ayant fait l'objet d'une normalisation internationale. Les formats devront également être documentés et permettre une conservation à long terme des fichiers (e.a. TIFF, PDF/A-1,...). De préférence, le format respectera un standard ouvert, c'est-à-dire un format dont la spécification est publiquement accessible.

Si le recours à un format de fichier compressé ou le passage par un format intermédiaire est nécessaire, cela devra se faire sans entraîner aucune perte relevante de données ou de qualité.

**Art. 8.** Les données numérisées sont conservées dans une infrastructure de stockage au plus tard le jour où elles sont mises en forme. Durant cette période de mise en forme des données, la donnée numérisée et son original devront rester liés par un identificateur unique jusqu'à la destruction de l'original. Ceci permettra notamment d'effectuer des contrôles de qualité.

**Art. 9.** Cette disposition prévoit que le traitement des données numérisées ne peut avoir lieu que dans un pays membre de l'Union européenne ou, comme proposé par le Conseil d'État dans son avis n° 57.117/3 du 18 mars 2015, dans un Etat tiers auquel la libre circulation des services a été étendue et qui s'est engagé à respecter la réglementation de l'Union européenne relative au traitement de données à caractère personnel dans le cadre d'un accord international avec l'Union européenne.

**Art. 10.** Devront être garantis pendant toute la durée de conservation : l'intégrité, l'accessibilité et la lisibilité des données numérisées. Les données numérisées devront être conservées sur un support durable. Dans la mesure où aucun support de stockage ne peut assurer une pérennité absolue (supports obsolètes ou altérés), il y aura lieu d'opter pour celui qui offre la meilleure garantie de durabilité.

Bien indexer les données numérisées est capital. En effet, si l'indexation est mal réalisée, il sera impossible de retrouver la donnée en question dans le futur.

Ainsi, pour assurer le repérage des données numérisées, il est essentiel de pouvoir les identifier de façon détaillée et significative. L'ajout d'éléments d'identification ("métadonnées") facilitera donc l'identification, le repérage, l'utilisation des données numérisées, ainsi que le maintien de leur intégrité. Il est donc primordial de garantir également l'intégrité, la lisibilité et l'accessibilité des métadonnées durant la période de conservation.

**Art.11.** Cette disposition énonce les mesures minimales que l'hôpital doit mettre en place en vue de garantir la sécurité des données numérisées.

Cette disposition indique également que la politique de sécurité de l'information de l'hôpital doit être établie sur la base de normes et/ou lignes directrices reconnues par une instance nationale ou internationale. Les normes de la série ISO 27000 en sont un exemple.

J'ai l'honneur d'être,

Sire,  
de Votre Majesté,  
le très respectueux  
et très fidèle serviteur,

La Ministre des Affaires sociales et de la Santé publique,  
Mme M. DE BLOCK

CONSEIL D'ÉTAT

Section de législation, avis 57.117/3 du 18 mars 2015 sur un projet d'arrêté royal « relatif à la force probante des données enregistrées, traitées, communiquées au moyen de techniques photographiques et optiques, ainsi qu'à leur reproduction sur papier ou sur tout autre support lisible pour l'application dans les soins de santé ».

Le 12 février 2015, le Conseil d'État, section de législation, a été invité par la Ministre de la Santé publique à communiquer un avis, dans un délai de trente jours, sur un projet d'arrêté royal 'relatif à la force probante des données enregistrées, traitées, communiquées au moyen

Elke bewerking (aanmaak, raadpleging, wijziging van de metagegevens,...) van de gedigitaliseerde gegevens wordt in een bestand bewaard waarin de identiteit van de bewerker wordt opgenomen.

**Art. 7.** De gedigitaliseerde gegevens mogen enkel bewaard worden in bestandsformaten die internationaal genormeerd werden. De formaten moeten ook gedocumenteerd worden en een langetermijnbewaring van de bestanden (bv. TIFF, PDF/A-1,...) mogelijk maken. In het formaat wordt een open standaard nagestreefd, d.w.z. een formaat waarvan de specificatie toegankelijk is voor het publiek.

Als er een gecompromeerd bestandsformaat of een tussenformaat gebruikt moet worden, mag er geen enkel relevant informatie- of kwaliteitsverlies optreden.

**Art. 8.** De gedigitaliseerde gegevens worden ten laatste op de dag van hun opmaak in een opslaginfrastructuur bewaard. Wanneer de gegevens opgemaakt worden, moeten de gedigitaliseerde gegevens en de originele gegevens blijvend met elkaar gelinkt worden via een unieke identifier tot op het moment waarop de originele gegevens vernietigd worden. Hierdoor kunnen onder meer kwaliteitscontroles uitgevoerd worden.

**Art. 9.** Volgens deze bepaling mogen de gedigitaliseerde gegevens enkel verwerkt worden in een lidstaat van de Europese Unie of, zoals voorgesteld door de Raad van State in zijn advies nr. 57.117/3 van 18 maart 2015, in een derde staat waarnaar het vrij verkeer van diensten is uitgebreid en die zich er in het kader van een internationaal akkoord met de Europese Unie toe heeft verbonden om de regelgeving van de Europese Unie betreffende de verwerking van persoonsgegevens te respecteren.

**Art. 10.** Gedurende de volledige bewaartermijn moet het volgende gewaarborgd worden : de integriteit, de toegankelijkheid en de leesbaarheid van de gedigitaliseerde gegevens. De gedigitaliseerde gegevens moeten bewaard worden op een duurzame drager. Aangezien geen enkel opslagmedium een absolute duurzaamheid kan waarborgen (verouderde of beschadigde dragers), dient er gekozen te worden voor het medium dat de beste duurzaamheidsgarantie biedt.

Een goede indexatie van de gedigitaliseerde gegevens is essentieel. Als de indexatie slecht uitgevoerd wordt, is het immers onmogelijk om het betrokken gegeven in de toekomst terug te vinden.

Om aldus de gedigitaliseerde gegevens te kunnen achterhalen, is het essentieel ze gedetailleerd en betekenisvol te kunnen identificeren. Door toevoeging van identificatie-elementen ("metagegevens") wordt het eenvoudiger om de gedigitaliseerde gegevens te gebruiken, te achterhalen en te identificeren en om de integriteit ervan te bewaren. Het is dus van het allergrootste belang om tevens de integriteit, de leesbaarheid en de toegankelijkheid van de metagegevens te waarborgen gedurende de bewaartermijn.

**Art.11.** Deze bepaling vermeldt de minimale maatregelen die het ziekenhuis moet treffen om de veiligheid van de gedigitaliseerde gegevens te waarborgen.

Deze bepaling geeft tevens aan dat het informatieveiligheidsbeleid van het ziekenhuis gebaseerd moet zijn op de normen en/of richtlijnen die door een nationale of internationale organisatie erkend worden. De reeks ISO 27000-normen is hier een voorbeeld van.

Ik heb de eer te zijn,

Sire,  
van Uwe Majesteit,  
de zeer eerbiedige  
en zeer getrouwe dienaar,

De Minister van Sociale Zaken en Volksgezondheid,  
Mevr. M. DE BLOCK

RAAD VAN STATE

Afdeling Wetgeving, advies 57.117/3 van 18 maart 2015 over een ontwerp van koninklijk besluit 'betreffende de bewijskracht van de gegevens die worden opgeslagen, verwerkt of meegedeeld door middel van een optische en fotografische techniek, evenals hun weergave op papier of op elke andere leesbare drager, voor de toepassing in de gezondheidszorg'.

Op 12 februari 2015 is de Raad van State, afdeling Wetgeving, door de Minister van Volksgezondheid verzocht binnen een termijn van dertig dagen een advies te verstrekken over een ontwerp van koninklijk besluit 'betreffende de bewijskracht van de gegevens die worden

de techniques photographiques et optiques, ainsi qu'à leur reproduction sur papier ou sur tout autre support lisible pour l'application dans les soins de santé'.

Le projet a été examiné par la troisième chambre le 10 mars 2015. La chambre était composée de Jo BAERT, président de chambre, Jan SMETS et Jeroen VAN NIEUWENHOVE, conseillers d'État, Jan VELAERS, assesseur, et Annemie GOOSSENS, greffier.

Le rapport a été présenté par Tim CORTHAUT, auditeur.

La concordance entre la version française et la version néerlandaise de l'avis a été vérifiée sous le contrôle de Jeroen VAN NIEUWENHOVE, conseiller d'État.

L'avis, dont le texte suit, a été donné le 18 mars 2015.

1. En application de l'article 84, § 3, alinéa 1<sup>er</sup>, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973, la section de législation a fait porter son examen essentiellement sur la compétence de l'auteur de l'acte, le fondement juridique et l'accomplissement des formalités prescrites.

\*

#### PORTEE DU PROJET

2. Le projet soumis pour avis entend instaurer un régime de preuve concernant les données enregistrées, traitées ou communiquées par les hôpitaux au moyen de procédés photographiques et optiques, ainsi qu'à leur reproduction sur papier ou sur tout autre support lisible.

L'article 11 du projet prévoit que les données enregistrées, traitées ou communiquées selon des procédés photographiques et optiques ainsi que leur reproduction sur papier ou sur tout autre support lisible ont « force probante »<sup>(1)</sup>, jusqu'à preuve du contraire, si la procédure déterminée par l'hôpital conformément à l'article 2 du projet pour leur enregistrement, leur traitement, leur communication ou leur reproduction satisfait aux conditions fixées par les articles 3 à 10 du projet.

<sup>(1)</sup> *Il semble préférable de se conformer à la terminologie utilisée dans la disposition procurant le fondement juridique en utilisant de manière cohérente le terme « bewijswaarde » au lieu du terme « bewijskracht » dans la version néerlandaise du projet. Dans le texte français, on utilisera de préférence les termes « valeur probante ».*

#### COMPÉTENCE DE L'AUTORITÉ FÉDÉRALE

3.1. Dans l'avis 51.401/1/2/3 du 20 juin 2012, le Conseil d'État a formulé les observations suivantes à propos de la compétence de l'autorité fédérale concernant l'article 36/1, § 2, de la loi du 21 août 2008 'relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions'<sup>(2)</sup>, dans lequel le fondement juridique de l'arrêté en projet est recherché :

<sup>(2)</sup> *Inscrit par l'article 59 de la loi du 19 mars 2013 'portant des dispositions diverses en matière de santé (I)'*

« Reste à savoir si la détermination de la valeur probante des 'données gérées dans le cadre de la politique de santé' est une matière qui, en tant que telle, relève de la compétence fédérale (résiduelle), ou bien s'il s'agit d'une matière qui constitue un élément des matières qui relèvent des compétences matérielles respectives de l'autorité fédérale, des communautés et des régions.

Les règles concernant la preuve littérale, parallèlement à celles relatives à la preuve testimoniale, aux présomptions, à l'aveu des parties et au serment figurent dans le chapitre VI du livre III du titre III du Code civil (articles 1315 à 1369), sous l'intitulé 'De la preuve des obligations, et de celle du paiement'.

Dans l'arrêt n° 29/2010 du 18 mars 2010, la Cour constitutionnelle a constaté, à propos des articles 4 et 5, 1<sup>o</sup>, de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth, que la mission de celle-ci portait uniquement sur les aspects de la politique de la santé qui relèvent des compétences des autorités fédérales et que les prestations de services effectuées par la plate-forme eHealth au profit des communautés devaient faire l'objet d'un accord de coopération. La Cour constitutionnelle a néanmoins jugé qu'en chargeant la plate-forme eHealth de promouvoir la communication électronique des informations entre les praticiens de l'art médical, le législateur fédéral n'avait pas excédé sa compétence<sup>(3)</sup>.

<sup>(3)</sup> *Note 19 de l'avis cité : Cour constitutionnelle, 18 mars 2010, n° 29/2010, B.43.1 - B.43.2.*

Bien qu'il soit inséré dans la loi du 21 août 2008, l'article 36bis, en projet, a cependant un champ d'application bien plus large que cette loi elle-même<sup>(4)</sup>. Il vise à fixer des règles de fond concernant la valeur probante des données relatives à la santé ou à la politique de la santé,

opgeslagen, verwerkt of meegedeeld door middel van een optische en fotografische techniek, evenals hun weergave op papier of op elke andere leesbare drager, voor de toepassing in de gezondheidszorg'.

Het ontwerp is door de derde kamer onderzocht op 10 maart 2015. De kamer was samengesteld uit Jo BAERT, kamervoorzitter, Jan SMETS en Jeroen VAN NIEUWENHOVE, staatsraden, Jan VELAERS, assessor, en Annemie GOOSSENS, griffier.

Het verslag is uitgebracht door Tim CORTHAUT, auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Jeroen VAN NIEUWENHOVE, staatsraad.

Het advies, waarvan de tekst hierna volgt, is gegeven op 18 maart 2015.

1. Met toepassing van artikel 84, § 3, eerste lid, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, heeft de afdeling Wetgeving zich toegespitst op het onderzoek van de bevoegdheid van de steller van de handeling, van de rechtsgrond, alsmede van de vraag of aan de te vervullen vormvereisten is voldaan.

\*

#### STREKKING VAN HET ONTWERP

2. Het voor advies voorgelegde ontwerp strekt ertoe een regeling in te voeren op het vlak van het bewijs voor gegevens die door ziekenhuizen worden opgeslagen, verwerkt of meegedeeld door middel van een optische en fotografische techniek, evenals hun weergave op papier of elke andere leesbare drager.

Artikel 11 van het ontwerp bepaalt dat de gegevens die door middel van een optische en fotografische techniek worden opgeslagen, verwerkt of meegedeeld, alsook de weergave van deze gegevens op papier of op elke andere leesbare drager, "bewijskracht"<sup>(1)</sup> hebben tot bewijs van het tegendeel, indien de door het ziekenhuis overeenkomstig artikel 2 van het ontwerp vastgelegde procedure voor de opslag, de verwerking, de mededeling of de weergave van deze gegevens voldoet aan de voorwaarden die worden bepaald in de artikelen 3 tot 10 van het ontwerp.

<sup>(1)</sup> *Het lijkt verkieslijk om aan te sluiten bij de terminologie die in de rechtsgrondbepaling wordt gebruikt, door in de Nederlandse tekst van het ontwerp consequent het woord "bewijswaarde" in plaats van "bewijskracht" te vermelden. In de Franse tekst gebruikte men bij voorkeur de woorden "valeur probante".*

#### BEVOEGDHEID VAN DE FEDERALE OVERHEID

3.1. In advies 51.401/1/2/3 van 20 juni 2012 heeft de Raad van State het volgende uiteengezet aangaande de bevoegdheid van de federale overheid met betrekking tot artikel 36/1, § 2, van de wet van 21 augustus 2008 'houdende de oprichting en organisatie van het eHealth platform en diverse bepalingen',<sup>(2)</sup> waarin de rechtsgrond voor het ontworpen besluit wordt gezocht :

<sup>(2)</sup> *Ingevoegd bij artikel 59 van de wet van 19 maart 2013 'houdende diverse bepalingen inzake gezondheid (I)'.*

"De vraag rijst of het regelen van de bewijswaarde van 'gegevens beheerd in het kader van het gezondheidsbeleid' een aangelegenheid op zich is, die behoort tot de (residuaire) federale bevoegdheid, dan wel een aangelegenheid die een onderdeel vormt van de aangelegenheden die behoren tot de respectieve materiële bevoegdheden van de federale overheid, de gemeenschappen en de gewesten.

Regels inzake het schriftelijk bewijs zijn, samen met regels inzake het bewijs door getuigen, de vermoedens, de bekendenis van partijen en de eed, bepaald in hoofdstuk VI van Boek III van titel III van het Burgerlijk Wetboek (artikelen 1315-1369), onder het opschrift 'Bewijs van de verbintenissen en bewijs van de betaling'.

In het arrest nr. 29/2010 van 18 maart 2010 heeft het Grondwettelijk Hof, in verband met de artikelen, 4 en 5, 1<sup>o</sup>, van de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform, vastgesteld dat de missie van het eHealth-platform enkel betrekking had op de aspecten van het gezondheidsbeleid die tot de bevoegdheid van de federale overheid behoorden, en dat het verlenen van diensten door het eHealth-platform aan de gemeenschappen een samenwerkingsakkoord vereiste. Niettemin was het Grondwettelijk Hof van oordeel dat de federale wetgever zijn bevoegdheid niet had overschreden door het eHealth-platform te belasten met de opdracht om de elektronische communicatie van informatie tussen beoefenaars van de geneeskunst te bevorderen.<sup>(3)</sup>

<sup>(3)</sup> *Voetnoot 19 van het geciteerde advies : Grondwettelijk Hof, 18 maart 2010, nr. 29/2010, B.43.1 - B.43.2.*

Het ontworpen artikel 36bis heeft echter, hoewel het wordt ingevoegd in de wet van 21 augustus 2008, een veel breder toepassingsgebied dan die wet zelf.<sup>(4)</sup> Er wordt mee beoogd een inhoudelijke regeling vast te stellen voor de bewijswaarde van gegevens die verband houden

indépendamment de l'utilisation de la plate-forme eHealth. L'arrêt de la Cour constitutionnelle précitée ne porte pas sur ces règles.

<sup>(4)</sup> Note 20 de l'avis cité : Voir également l'observation 24 relative à l'article 58 du projet.

Il apparaît au Conseil d'État que le pouvoir de régler la valeur probante de données peut être considéré, d'une manière générale, comme une matière qui relève de la compétence résiduelle de l'autorité fédérale.

Sur ce point, le Conseil d'État aperçoit une analogie avec le pouvoir de fixer des règles en matière de responsabilité civile. De l'avis du Conseil d'État, cette matière relève également de la compétence résiduelle de l'autorité fédérale. Rien n'empêche toutefois que les communautés et les régions puissent édicter des règles spécifiques dans ce domaine. C'est le cas lorsque ces règles peuvent être considérées comme propres à une matière qui est attribuée aux communautés ou aux régions, ce qui suppose un lien étroit avec celle-ci. Les législateurs communautaires et régionaux peuvent en effet estimer que l'élaboration de telles règles spécifiques est nécessaire pour pouvoir mener efficacement la politique qu'elles souhaitent en cette matière. Le cas échéant, ils peuvent s'écarter du droit commun (fédéral). Il est alors requis que le principe de proportionnalité soit respecté, ce qui implique qu'ils ne peuvent prendre des mesures tellement extrêmes qu'elles rendraient impossible ou exagérément difficile l'exercice efficace par l'autorité fédérale de sa politique en matière de responsabilité civile<sup>(5)</sup>.

<sup>(5)</sup> Note 21 de l'avis cité : Avis C.E. 33.334/VR du 24 juin 2003 sur une proposition d'ordonnance 'relative à l'assainissement des sols', Doc. parl., C.R.B.C., 2002-03, n° A-221/1, pp. 4-5, n° 6-8. Voir également avis C.E. 42.505/VR/3 du 17 avril 2007 sur un projet devenu le décret du 21 décembre 2007 'complétant le décret du 5 avril 1995 contenant des dispositions générales concernant la politique de l'environnement par un titre XV Dommages environnementaux, convertissant [lire : transposant] la Directive 2004/35/CE du Parlement européen et du Conseil du 21 avril 2004 sur la responsabilité environnementale en ce qui concerne la prévention et la réparation des dommages environnementaux', Doc. parl., Parl. fl., 2006-07, n° 1252/1, (173), pp. 179-180, n° 3.2 et note 4.

De la même manière, on peut considérer que l'autorité fédérale est compétente pour fixer des règles générales en ce qui concerne la valeur probante de données électroniques et de données enregistrées au moyen de techniques photographiques et optiques. Cette compétence peut également être exercée à l'égard des aspects de la politique de la santé qui relèvent de la compétence des communautés. En ce qui concerne ces aspects, il incombe cependant à l'autorité fédérale de respecter le principe de proportionnalité en faveur des communautés. Cette compétence de l'autorité fédérale ne s'oppose en outre pas à ce que les communautés élaborent des règles spécifiques concernant la valeur probante des données visées, pour autant que la fixation de ces règles soit étroitement liée à une matière qui relève de leurs compétences. À cet égard, elles pourraient même déroger aux règles générales, fixées par l'autorité fédérale, pour autant qu'elles respectent le principe de proportionnalité en faveur de celle-ci.

Le Conseil d'Etat est ainsi amené à conclure qu'en adoptant l'article 60 du projet, le législateur fédéral n'excéderait pas sa compétence ».<sup>(6)</sup>

<sup>(6)</sup> Avis C.E. 51.401/1/2/3 du 20 juin 2012 sur un avant-projet devenu notamment la loi précitée du 19 mars 2013, Doc. parl., Chambre, 2012-13, n° 53-2600/001, (134), pp.147-148, n° 29.2.

3.2.Plusieurs des conditions visées aux articles 3 à 10 du projet, auxquelles doit satisfaire la procédure qui doit être déterminée par les hôpitaux conformément à l'article 2 du projet, concernent non seulement les exigences intrinsèques auxquelles doivent répondre les données numérisées proprement dites, mais également l'organisation des systèmes informatiques utilisés dans les hôpitaux pour enregistrer, traiter ou communiquer des données numérisées.

met de gezondheid of het gezondheidsbeleid, los van het gebruik van het eHealth-platform. Het genoemde arrest van het Grondwettelijk Hof heeft geen betrekking op een dergelijke regeling.

<sup>(4)</sup> Voetnoot 20 van het geciteerde advies : Zie ook opmerking 24 in verband met artikel 58 van het ontwerp.

Het komt de Raad van State voor dat de bevoegdheid om de bewijswaarde van gegevens te regelen in het algemeen beschouwd kan worden als een aangelegenheid die behoort tot de residuaire bevoegdheid van de federale overheid.

Op dit punt ziet de Raad van State een analogie met de bevoegdheid inzake het regelen van de burgerlijke aansprakelijkheid. Ook wat die aangelegenheid betreft, is de Raad van State van oordeel dat zij behoort tot de residuaire bevoegdheid van de federale overheid. Dit neemt evenwel niet weg dat de gemeenschappen en de gewesten op dit vlak specifieke regels kunnen uitvaardigen. Dit is het geval wanneer die regels kunnen worden beschouwd als eigen aan een aangelegenheid die aan de gemeenschappen of de gewesten is toegewezen, wat een nauwe band met die aangelegenheid veronderstelt. De gemeenschappen en gewestwetgevers kunnen immers van mening zijn dat het aannemen van zulke specifieke regels nodig is om het door hen gewenste beleid in die aangelegenheid op een doeltreffende wijze te voeren. In voorkomend geval kunnen zij afwijken van het (federale) gemeenrecht. Vereist is dan wel dat zij het evenredigheidsbeginsel in acht nemen, hetgeen betekent dat zij geen zo verregaande maatregelen mogen nemen dat het voor de federale overheid onmogelijk of overdreven moeilijk wordt om haar beleid inzake burgerlijke aansprakelijkheid doelmatig te voeren.<sup>(5)</sup>

<sup>(5)</sup> Voetnoot 21 van het geciteerde advies : Adv.RvS 33.334/VR van 24 juni 2003 over een voorstel van ordonnantie betreffende de bodemsanering, Parl.St. Br.H.R. 2002-03, nr. A-221/2, pp. 4-5, nrs. 6-8. Zie ook Adv.RvS 42.505/VR/3 van 17 april 2007 over een ontwerp dat geleid heeft tot het decreet van 21 december 2007 'tot aanvulling van het decreet van 5 april 1995 houdende algemene bepalingen inzake milieubeleid met een titel XV Milieuschade, tot omzetting van de Richtlijn 2004/35/EG van het Europees Parlement en de Raad van 21 april 2004 betreffende de milieuaansprakelijkheid met betrekking tot het voorkomen en herstellen van milieuschade', Parl.St. Vl.Parl. 2006-07, nr. 1252/1, (173), pp. 179-180, nr. 3.2 en noot 4.

In dezelfde zin kan worden aangenomen dat de federale overheid bevoegd is voor het bepalen van algemene regels inzake de bewijswaarde van elektronische gegevens en van gegevens die door middel van fotografische en optische technieken worden opgeslagen. Die bevoegdheid kan worden uitgeoefend, ook met betrekking tot aspecten van het gezondheidsbeleid waarvoor de gemeenschappen bevoegd zijn. Voor die aspecten dient de federale overheid wel het evenredigheidsbeginsel ten gunste van de gemeenschappen in acht te nemen. Die bevoegdheid van de federale overheid belet bovendien niet dat de gemeenschappen specifieke regels inzake de bewijswaarde van de bedoelde gegevens vaststellen, in zoverre het vaststellen van dergelijke regels nauw verbonden is met een aangelegenheid waarvoor de gemeenschappen bevoegd zijn. Zij zouden daarbij zelfs kunnen afwijken van de algemene, federaal vastgestelde regels, mits zij het evenredigheidsbeginsel ten gunste van de federale overheid in acht nemen.

De Raad van State komt aldus tot de conclusie dat de federale wetgever, door artikel 60 van het ontwerp aan te nemen, zijn bevoegdheid niet zou overschrijden.<sup>(6)</sup>

<sup>(6)</sup> Adv.RvS 51.401/1/2/3 van 20 juni 2012 over een voorontwerp dat onder meer geleid heeft tot de voornoemde wet van 19 maart 2013, Parl.St. Kamer 2012-13, nr. 53-2600/001, (134) 147-148, nr. 29.2.

3.2. Verscheidene van de voorwaarden bedoeld in de artikelen 3 tot 10 van het ontwerp, waaraan de procedure moet voldoen die door de ziekenhuizen moet worden vastgelegd overeenkomstig artikel 2 van het ontwerp, hebben niet alleen betrekking op de intrinsieke vereisten waaraan de gedigitaliseerde gegevens zelf moeten voldoen, maar ook op de organisatie van de informaticasystemen die in de ziekenhuizen worden gebruikt voor het opslaan, verwerken of meedelen van gedigitaliseerde gegevens.

La compétence résiduelle précitée de l'autorité fédérale relative au régime de preuve concernant les données en général ne peut s'entendre de manière à ce point large que l'autorité fédérale pourrait, en fixant les conditions auxquelles la procédure d'enregistrement, de traitement, de communication ou de reproduction des données numérisées doit satisfaire, également régler l'organisation générale des systèmes informatiques concernés. En effet, un tel régime doit en principe<sup>(7)</sup> relever de la compétence des communautés en matière de normes d'agrément des hôpitaux<sup>(8)</sup>. En tout état de cause, l'autorité fédérale doit tenir compte du principe de proportionnalité, qui implique que le dispositif en projet ne peut pas rendre impossible ou exagérément difficile l'exercice des compétences communautaires précitées.

<sup>(7)</sup> Pour autant qu'un tel régime ne porte pas sur la législation organique, pour laquelle l'autorité fédérale est demeurée compétente (article 5, § 1<sup>er</sup>, I, alinéa 1<sup>er</sup>, 1<sup>o</sup>, a), de la loi spéciale du 8 août 1980 'de réformes institutionnelles') et qui a été définie de manière plus détaillée dans les travaux préparatoires comme étant les « caractéristiques de base des (...) hôpitaux » (Doc. parl., Sénat, 2012-13, n° 5-2232/1, pp. 34-36).

<sup>(8)</sup> A ce jour, l'arrêté royal du 23 octobre 1964 'portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre' ne comporte pas un tel régime général relatif aux systèmes informatiques.

Le Conseil d'Etat ne dispose pas des connaissances techniques requises lui permettant de déterminer l'impact réel des conditions précitées, visées aux articles 3 à 10 du projet, sur la manière dont les hôpitaux gèrent leurs systèmes informatiques en général. Il appartient dès lors aux auteurs du projet d'examiner si chacune de ces conditions présente un lien nécessaire avec la compétence résiduelle de l'autorité fédérale de déterminer d'une manière générale le régime de preuve concernant les données numérisées. En outre, il est conseillé de compléter le rapport au Roi à cet égard par une justification, à la lumière de cet examen, de la compétence de l'autorité fédérale en ce qui concerne le régime en projet<sup>(9)</sup>.

<sup>(9)</sup> Conformément à l'article 3, § 1<sup>er</sup>, alinéa 1<sup>er</sup>, quatrième phrase, des lois sur le Conseil d'Etat, le présent avis doit être publié au Moniteur belge en même temps que le rapport au Roi et l'arrêté envisagé.

3.3. Dans un souci de bonne compréhension du fondement du régime en projet, au regard de la répartition des compétences, il est en tous les cas recommandé d'insérer l'article 11 du projet, qui en constitue la disposition essentielle, entre les articles 1<sup>er</sup> et 2 actuels, afin qu'il apparaisse plus clairement qu'il faut lire les conditions visées aux articles 3 à 10 dans le prolongement du dispositif de l'article 11 actuel.

## FONDEMENT JURIDIQUE

4. L'arrêté en projet trouve son fondement juridique dans l'article 36/1, § 2, de la loi du 21 août 2008. Cette disposition légale confère au Roi le pouvoir, après avis de la plate-forme eHealth, de déterminer dans quelles conditions les données enregistrees, traitées ou communiquées au moyen de techniques photographiques et optiques, ainsi que leur reproduction sur papier ou sur tout autre support lisible, ont, pour l'application dans les soins de santé, la même force probante (lire : valeur probante) que les données originales.

## EXAMEN DU TEXTE

### Intitulé

5. Dès lors que le régime en projet n'est applicable qu'aux hôpitaux, il est conseillé, dans un souci de sécurité juridique, de l'exprimer également dans l'intitulé.

### Article 8

6. Conformément à l'article 8 du projet, le traitement des données numérisées a lieu dans un Etat membre de l'Union européenne. Le fait que le traitement de ces données, qui concerneront généralement aussi des données à caractère personnel, doit avoir lieu conformément aux garanties en matière de protection des droits fondamentaux dans l'Union européenne<sup>(10)</sup>, même lorsque ce traitement est sous-traité à l'étranger, n'empêche pas que d'autres pays non membres de l'Union européenne soient également liés par cette norme, à savoir des pays tiers auxquels s'étend la libre circulation des services et qui se sont engagés, dans le cadre d'un accord d'association, à respecter ces garanties<sup>(11)</sup>.

<sup>(10)</sup> Voir la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

De zo-even geschetste residuaire bevoegdheid van de federale overheid inzake de bewijsregeling voor gegevens in het algemeen kan niet zo ruim worden begrepen dat de federale overheid door middel van de voorwaarden waaraan de procedure voor de opslag, de verwerking, de mededeling of de weergave van de gedigitaliseerde gegevens moet voldoen, ook de algemene organisatie van de betrokken informaticasystemen kan regelen. Een dergelijke regeling moet immers in beginsel<sup>(7)</sup> tot de bevoegdheid van de gemeenschappen inzake de erkenningsnormen voor ziekenhuizen worden gerekend.<sup>(8)</sup> In elk geval moet de federale overheid het evenredigheidsbeginsel in acht nemen, hetgeen inhoudt dat de ontworpen regeling de uitoefening van de zo-even geschetste gemeenschapsbevoegdheden niet onmogelijk of overdreven moeilijk mag maken.

<sup>(7)</sup> Voor zover een dergelijke regeling geen betrekking heeft op de organieke wetgeving, waarvoor de federale overheid bevoegd is gebleven (artikel 5, § 1, I, eerste lid, 1<sup>o</sup>, a), van de bijzondere wet van 8 augustus 1980 'tot hervorming der instellingen') en die in de parlementaire voorbereiding nader is omschreven als de "basissenmerken van de (...) ziekenhuizen" (Parl.St. Senaat 2012-13, nr. 5-2232/1, 34-36).

<sup>(8)</sup> Tot dusver bevat het koninklijk besluit van 23 oktober 1964 'tot bepaling van de normen die door de ziekenhuizen en hun diensten moeten worden nageleefd' geen dergelijke algemene regeling met betrekking tot informaticasystemen.

De Raad van State beschikt niet over het vereiste technische inzicht om te kunnen uitmaken wat de reële impact is van de zo-even geschetste voorwaarden, bedoeld in de artikelen 3 tot 10 van het ontwerp, op de wijze waarop de ziekenhuizen hun informaticasystemen in het algemeen beheren. Het staat dan ook aan de stellers van het ontwerp om te onderzoeken of elk van deze voorwaarden een noodzakelijk verband vertonen met de residuaire bevoegdheid van de federale overheid om op algemene wijze de bewijsregeling te bepalen voor gedigitaliseerde gegevens. Tevens is het raadzaam om het verslag aan de Koning dienaangaande aan te vullen met een verantwoording van de bevoegdheid van de federale overheid voor de ontworpen regeling in het licht van dat onderzoek.<sup>(9)</sup>

<sup>(9)</sup> Overeenkomstig artikel 3, § 1, eerste lid, vierde zin, van de wetten op de Raad van State, moet dit advies samen met dat verslag aan de Koning en het te nemen besluit in het Belgisch Staatsblad worden bekendgemaakt.

3.3. Ter wille van een goed begrip van de bevoegdheidsrechtelijke grondslag van de ontworpen regeling verdient het in elk geval aanbeveling om artikel 11 van het ontwerp, dat de kernbepaling ervan vormt, tussen het huidige artikel 1 en artikel 2 op te nemen, zodat duidelijker naar voor komt dat de voorwaarden bedoeld in de artikelen 3 tot 10 moeten worden gelezen in het verlengde van de regeling in het huidige artikel 11.

## RECHTSGROND

4. Het ontworpen besluit vindt rechtsgrond in artikel 36/1, § 2, van de wet van 21 augustus 2008. Aan die wetsbepaling ontleent de Koning de bevoegdheid om, na advies van het eHealth-platform, te bepalen onder welke voorwaarden gegevens die door middel van fotografische en optische techniek worden opgeslagen, verwerkt of meegedeeld, evenals hun weergave op papier of op elke andere leesbare drager, voor de toepassing in de gezondheidszorg, dezelfde bewijswaarde hebben als de originele gegevens.

## ONDERZOEK VAN DE TEKST

### Opschrift

5. Aangezien de ontworpen regeling enkel van toepassing is op ziekenhuizen, is het ter wille van de rechtszekerheid raadzaam om dit ook in het opschrift tot uiting te laten komen.

### Artikel 8

6. Overeenkomstig artikel 8 van het ontwerp gebeurt de verwerking van de gedigitaliseerde gegevens in een lidstaat van de Europese Unie. Het gegeven dat de verwerking van die gegevens, die veelal ook persoonsgegevens zullen betreffen, moet gebeuren conform de waarborgen inzake grondrechtenbescherming in de Europese Unie,<sup>(10)</sup> ook wanneer die verwerking uitbesteed wordt in het buitenland, neemt niet weg dat er ook andere landen zijn dan de lidstaten van de Europese Unie die gebonden zijn door die standaard, namelijk derde landen waarnaar het vrij verkeer van diensten is uitgebreid en die zich er in het kader van een associatieakkoord toe verbonden hebben om deze waarborgen te respecteren.<sup>(11)</sup>

<sup>(10)</sup> Zie richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 'betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens'.

<sup>(11)</sup> *A cet égard, il s'agit en premier lieu des pays EEE, mais des accords d'association ou des accords de pré-adhésion ont également été conclus avec d'autres pays ou sont en cours d'élaboration.*

Le délégué s'est rallié à ce point de vue :

« De bepaling heeft tot doel om te waarborgen dat de verwerking van de persoonsgegevens te allen tijde geschiedt met inachtnaam van een afdoend niveau van bescherming en beveiliging. Voor zover dat ook buiten de Europese Unie kan worden gegarandeerd - bijvoorbeeld door het uitdrukkelijk engagement van een niet-lidstaat om de regelgeving dienaangaande van de Europese Unie te respecteren of te implementeren in de eigen nationale regelgeving - lijken er geen bezwaren om de huidige formulering van artikel 8 aan te passen ».

Mieux vaudrait dès lors rédiger l'article 8 du projet comme suit :

« Le traitement des données numérisées a lieu dans un État membre de l'Union européenne ou dans un État tiers auquel est étendue la libre circulation des services et qui s'est engagé, dans le cadre d'un accord international avec l'Union européenne, à respecter la réglementation de l'Union en matière de traitement des données à caractère personnel ».

#### Article 11

7.1. A l'article 11, alinéa 1<sup>er</sup>, du projet, mieux vaudrait mentionner « la procédure fixée par l'hôpital conformément à l'article 2 » plutôt que « la procédure adoptée ».

7.2. L'article 11, alinéa 2, du projet prévoit qu'en tous les cas, la donnée numérisée ne pourra pas être privée de son efficacité juridique et que cette donnée ne pourra être refusée comme preuve en justice. Cette disposition prête à confusion. Tout d'abord, on pourrait en déduire que les données numérisées qui ne répondent pas aux conditions fixées par l'arrêté en projet (compte tenu des mots « [e]n tous les cas ») peuvent néanmoins être utilisées comme preuve dans le cadre de procédures judiciaires, et ce indépendamment de leur fiabilité. En outre, on n'aperçoit pas clairement la différence entre la notion « ne pas pouvoir être privé de l'efficacité juridique » et la notion « ne pas pouvoir être refusé comme preuve en justice ». On n'aperçoit pas non plus comment ces deux notions s'articulent avec le dispositif de l'article 11, alinéa 1<sup>er</sup>, du projet. À cet égard, le délégué a déclaré ce qui suit :

« De bepaling is geïnspireerd door een gelijkaardige bepaling uit het koninklijk besluit van 22 maart 1993 betreffende de bewijskracht, ter zake van de sociale zekerheid, van de door instellingen van sociale zekerheid opgeslagen, bewaarde of weergegeven informatiegegevens. Ingevolge dat koninklijk besluit hebben de door een instelling van sociale zekerheid overeenkomstig een door de Minister van Sociale Zaken erkende procedure opgeslagen, bewaarde of weergegeven informatiegegevens, evenals hun weergave op een leesbare drager, voor de toepassing van de sociale zekerheid bewijskracht tot bewijs van het tegendeel. Voor zover de procedure door de Minister van Sociale Zaken werd erkend (na een voorafgaand advies van het sectoraal comité van de sociale zekerheid en van de gezondheid) heeft de betrokken instelling van sociale zekerheid voldoende waarborgen over de bewijskracht van de volgens die procedure verwerkte persoonsgegevens en mag ze desgevallend de originele papieren documenten vernietigen.

In het voorliggende geval is het echter niet mogelijk gebleken om een erkenningsstelsel in te voeren. Dat betekent dat elk ziekenhuis voor zichzelf moet nagaan of het al dan niet aan de voorwaarden van het koninklijk besluit voldoet, hetgeen onzekerheid met zich kan brengen en daarmee gepaard gaand ook de twijfel over de mogelijkheid en wenselijkheid tot het vernietigen van de (vaak heel omvangrijke) papieren archieven. Het tweede lid van artikel 11 moet enigszins aan die bezorgdheid tegemoet komen : voor zover een ziekenhuis er zelf van overtuigd is dat het aan de voorwaarden van het koninklijk besluit voldoet, kunnen de gedigitaliseerde persoonsgegevens niet meer zomaar als bewijsmiddel worden verworpen maar kan de rechter in voorkomend geval - na een onderzoek ter zake en de vaststelling dat aan één of meerdere geldende voorwaarden niet is voldaan - wel bepalen dat de omkering van de bewijslast geen toepassing vindt (de gedigitaliseerde gegevens mogen dus steeds worden voorgelegd maar het ziekenhuis zal eventueel moeten aantonen dat de voorwaarden wel degelijk werden nageleefd of dat de gedigitaliseerde persoonsgegevens wel degelijk voldoende kwalitatief zijn) ».

Même compte tenu de cette explication, une certaine ambiguïté subsiste quant à la valeur probante précise des données numérisées en cas de différend relatif à l'application correcte du régime en projet. Si la procédure visée à l'article 2 du projet a été correctement suivie et si elle satisfait aux conditions fixées par les articles 3 à 10, la présomption réfragable visée à l'article 11, alinéa 1<sup>er</sup>, s'applique. Or, l'article 11,

<sup>(11)</sup> *Het gaat daarbij in de eerste plaats om de EER-landen, maar er zijn ook associatieakkoorden of pre-toetredingsakkoorden met andere landen gesloten of in voorbereiding.*

De gemachtigde sloot zich aan bij die zienswijze :

« De bepaling heeft tot doel om te waarborgen dat de verwerking van de persoonsgegevens te allen tijde geschiedt met inachtnaam van een afdoend niveau van bescherming en beveiliging. Voor zover dat ook buiten de Europese Unie kan worden gegarandeerd - bijvoorbeeld door het uitdrukkelijk engagement van een niet-lidstaat om de regelgeving dienaangaande van de Europese Unie te respecteren of te implementeren in de eigen nationale regelgeving - lijken er geen bezwaren om de huidige formulering van artikel 8 aan te passen ».

Artikel 8 van het ontwerp kan dan ook beter als volgt worden geformuleerd :

« De verwerking van de gedigitaliseerde gegevens gebeurt in een lidstaat van de Europese Unie of in een derde staat waarnaar het vrij verkeer van diensten is uitgebreid en die zich er in het kader van een internationaal akkoord met de Europese Unie toe heeft verbonden om de uniale regelgeving betreffende de verwerking van persoonsgegevens te respecteren ».

#### Artikel 11

7.1. In artikel 11, eerste lid, van het ontwerp kan in plaats van naar "de goedgekeurde procedure" beter worden verwezen naar "de procedure die het ziekenhuis overeenkomstig artikel 2 heeft vastgesteld".

7.2. In artikel 11, tweede lid, van het ontwerp wordt bepaald dat de gedigitaliseerde gegevens in ieder geval geen rechtsgeldigheid kan worden ontzegd en dat deze gegevens niet kunnen worden geweigerd als bewijsmiddel in gerechtelijke procedures. Die bepaling leidt tot verwarring. Vooreerst zou men eruit kunnen afleiden dat gedigitaliseerde gegevens die niet voldoen aan de voorwaarden vervat in het ontworpen besluit (gelet op de woorden "in ieder geval"), toch gebruikt kunnen worden als bewijsmiddel in gerechtelijke procedures, ongeacht de betrouwbaarheid van die gegevens. Bovendien is niet duidelijk wat het verschil is tussen de notie dat er geen rechtsgeldigheid kan worden ontzegd en de notie van het niet kunnen weigeren als bewijsmiddel in gerechtelijke procedures. Evenmin is duidelijk hoe deze beide noties zich verhouden tot de regeling vervat in artikel 11, eerste lid, van het ontwerp. De gemachtigde verklaarde hierover het volgende :

« De bepaling is geïnspireerd door een gelijkaardige bepaling uit het koninklijk besluit van 22 maart 1993 betreffende de bewijskracht, ter zake van de sociale zekerheid, van de door instellingen van sociale zekerheid opgeslagen, bewaarde of weergegeven informatiegegevens. Ingevolge dat koninklijk besluit hebben de door een instelling van sociale zekerheid overeenkomstig een door de Minister van Sociale Zaken erkende procedure opgeslagen, bewaarde of weergegeven informatiegegevens, evenals hun weergave op een leesbare drager, voor de toepassing van de sociale zekerheid bewijskracht tot bewijs van het tegendeel. Voor zover de procedure door de Minister van Sociale Zaken werd erkend (na een voorafgaand advies van het sectoraal comité van de sociale zekerheid en van de gezondheid) heeft de betrokken instelling van sociale zekerheid voldoende waarborgen over de bewijskracht van de volgens die procedure verwerkte persoonsgegevens en mag ze desgevallend de originele papieren documenten vernietigen.

In het voorliggende geval is het echter niet mogelijk gebleken om een erkenningsstelsel in te voeren. Dat betekent dat elk ziekenhuis voor zichzelf moet nagaan of het al dan niet aan de voorwaarden van het koninklijk besluit voldoet, hetgeen onzekerheid met zich kan brengen en daarmee gepaard gaand ook de twijfel over de mogelijkheid en wenselijkheid tot het vernietigen van de (vaak heel omvangrijke) papieren archieven. Het tweede lid van artikel 11 moet enigszins aan die bezorgdheid tegemoet komen : voor zover een ziekenhuis er zelf van overtuigd is dat het aan de voorwaarden van het koninklijk besluit voldoet, kunnen de gedigitaliseerde persoonsgegevens niet meer zomaar als bewijsmiddel worden verworpen maar kan de rechter in voorkomend geval - na een onderzoek ter zake en de vaststelling dat aan één of meerdere geldende voorwaarden niet is voldaan - wel bepalen dat de omkering van de bewijslast geen toepassing vindt (de gedigitaliseerde gegevens mogen dus steeds worden voorgelegd maar het ziekenhuis zal eventueel moeten aantonen dat de voorwaarden wel degelijk werden nageleefd of dat de gedigitaliseerde persoonsgegevens wel degelijk voldoende kwalitatief zijn) ».

Zelfs in het licht van deze uitleg blijft er dubbelzinnigheid bestaan over de precieze bewijswaarde van gedigitaliseerde gegevens wanneer er betwisting ontstaat over de correcte toepassing van de ontworpen regeling. Wanneer de procedure bedoeld in artikel 2 van het ontwerp correct werd gevolgd en die procedure voldoet aan de voorwaarden vervat in de artikelen 3 tot 10, geldt het weerlegbare vermoeden



alinéa 2, du projet laisse penser que les données numérisées concernées peuvent néanmoins encore produire certains effets au niveau de la preuve si cette présomption est réfutée, autrement dit si l'on peut démontrer que la procédure n'a pas été correctement suivie ou ne satisfait pas aux conditions. Peut-être les auteurs du projet entendent-ils ainsi créer un filet de sécurité, mais la question se pose de savoir si, dans de telles circonstances, la fiabilité des données numérisées concernées n'est pas trop compromise pour y attacher ces effets qui sont, de surcroît, réglées de manière incertaine sur le plan de la sécurité juridique.

7.3. Par conséquent, le Conseil d'État suggère aux auteurs du projet la proposition de texte suivante pour l'article 11 du projet, qui tient compte des observations précitées, ainsi que de la remarque terminologique formulée dans la note infrapaginale 1 :

« Art.11. Les données enregistrées, traitées ou communiquées selon des procédés photographiques et optiques ainsi que leur reproduction sur papier ou sur tout autre support lisible ont valeur probante, jusqu'à preuve du contraire, si la procédure fixée par l'hôpital conformément à l'article 2 pour leur enregistrement, leur communication, leur traitement ou leur reproduction satisfait aux conditions énumérées dans le présent arrêt et si les données ont été enregistrées, traitées ou communiquées conformément à cette procédure.

Toutefois, les données numérisées ne pourraient pas être privées de leur efficacité juridique au seul motif qu'il est contesté que la procédure réellement suivie répond aux conditions du présent arrêté, si celui qui se prévaut de ces données peut démontrer, par tous les moyens de droit, que le fait de déroger aux conditions du présent arrêté n'a pas compromis la fiabilité des données ».

S'il est soutenu que la procédure n'a pas été correctement suivie ou ne satisfait pas aux conditions, la valeur probante des données numérisées concernées peut encore être garantie, étend entendu que la charge de la preuve de la fiabilité des données incombe alors à l'hôpital. La notion « ne pas pouvoir être refusé comme preuve en justice » a été supprimée, parce qu'il apparaît au Conseil d'État que cette notion est incluse dans la disposition prévoyant que la donnée numérisée ne peut être privée de son efficacité juridique. Si les auteurs du projet ne sont pas de cet avis, ils devront faire toute la clarté sur ce point dans le texte et dans le rapport au Roi.

Le greffier,  
Annemie Goossens

Le Président,  
Jo Baert

**10 MAI 2015. — Arrêté royal relatif à la force probante des données enregistrées, traitées, communiquées au moyen de techniques photographiques et optiques par les hôpitaux, ainsi qu'à leur reproduction sur papier ou sur tout autre support lisible pour l'application dans les soins de santé**

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions, l'article 36/1, § 2, inséré par la loi du 19 mars 2013 portant des dispositions diverses en matière de santé (I);

Vu l'avis du Comité de gestion de la plate-forme eHealth, donné le 8 octobre 2013;

Vu l'avis du Comité de l'assurance soins de santé, donné le 3 février 2014;

Vu l'avis 57.117/3 du Conseil d'État, donné le 18 mars 2015, en application de l'article 84, § 1<sup>er</sup>, alinéa 1<sup>er</sup>, 2<sup>o</sup>, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973;

Sur la proposition de la Ministre des Affaires sociales et de la Santé publique,

Nous avons arrêté et arrêtons :

**Article 1<sup>er</sup>.** Pour l'application du présent arrêté, l'on entend par :

1<sup>o</sup> l'hôpital : l'hôpital au sens de la loi du 10 juillet 2008 relative aux hôpitaux et à d'autres établissements de soins;

2<sup>o</sup> la procédure : l'ensemble des procédures, architectures (matérielle et logicielle) et processus utilisés;

3<sup>o</sup> les données numérisées : les données enregistrées, traitées, communiquées au moyen de techniques photographiques et optiques;

bedoeld in artikel 11, eerste lid. Artikel 11, tweede lid, van het ontwerp wekt echter de indruk dat er aan de betrokken gedigitaliseerde gegevens toch nog een zeker gevolg op het vlak van het bewijs kan worden toegekend indien dat vermoeden wordt weerlegd, met andere woorden indien kan worden aangetoond dat de procedure niet correct werd gevolgd of niet voldoet aan de voorwaarden. Mogelijkerwijs beogen de stellers van het ontwerp hiermee een vangnetregeling, maar de vraag rijst of de betrouwbaarheid van betrokken gedigitaliseerde gegevens in dergelijke omstandigheden niet teveel gecompromitteerd is om er dat gevolg aan te verlenen dat dan bovendien nog op rechtsonzekere wijze is geregeld.

7.3. De Raad van State geeft de stellers van het ontwerp dan ook het volgende tekstvoorstel voor artikel 11 van het ontwerp ter overweging, waarin rekening wordt gehouden met hetgeen hiervoor is uiteengezet, alsook met de terminologische opmerking in voetnoot 1 :

"Art.11. De gegevens die door middel van een optische en fotografische techniek opgeslagen, verwerkt of meegedeeld worden, alsook de weergave van deze gegevens op papier of op elke andere leesbare drager, hebben bewijswaarde tot bewijs van het tegendeel, indien de procedure die het ziekenhuis overeenkomstig artikel 2 heeft vastgesteld voor de opslag, de mededeling, de verwerking of de weergave van deze informatie voldoet aan de voorwaarden opgesomd in dit besluit en de gegevens in overeenstemming met die procedure werden opgeslagen, verwerkt of meegedeeld.

De gedigitaliseerde gegevens kan echter geen rechtsgeldigheid worden ontzegd op de enkele grond dat betwist wordt dat de werkelijk gevolgde procedure aan de voorwaarden van dit besluit voldoet, als diegene die zich op deze gegevens beroept kan aantonen, met alle middelen van recht, dat de afwijking van de voorwaarden in dit besluit de betrouwbaarheid van de gegevens niet in het gedrang heeft gebracht."

Indien wordt aangevoerd dat de procedure niet correct werd gevolgd of niet voldoet aan de voorwaarden, kan de bewijswaarde van de betrokken gedigitaliseerde gegevens alsnog worden gevrijwaard, zij het dat de bewijslast over de betrouwbaarheid van de gegevens dan bij het ziekenhuis ligt. De notie van het niet kunnen weigeren als bewijsmiddel in gerechtelijke procedures werd achterwege gelaten omdat het de Raad van State voorkomt dat die notie is begrepen in de bepaling dat er geen rechtsgeldigheid kan worden ontzegd. Indien de stellers van het ontwerp dat anders zien, moeten zij daarover duidelijkheid scheppen in de tekst en in het verslag aan de Koning.

De griffier,  
Annemie Goossens

De voorzitter,  
Jo Baert

**10 MEI 2015. — Koninklijk besluit betreffende de bewijskracht van de gegevens die door de ziekenhuizen worden opgeslagen, verwerkt of meegedeeld door middel van een optische en fotografische techniek, evenals hun weergave op papier of op elke andere leesbare drager, voor de toepassing in de gezondheidszorg**

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen, op artikel 36/1, § 2, ingevoegd bij de wet van 19 maart 2013 houdende diverse bepalingen inzake gezondheid (I);

Gelet op het advies van het Beheerscomité van het eHealth-platform, gegeven op 8 oktober 2013;

Gelet op het advies van het Comité van de verzekering voor geneeskundige verzorging, gegeven op 3 februari 2014;

Gelet op het advies 57.117/3 van de Raad van State, gegeven op 18 maart 2015, met toepassing van artikel 84, § 1, eerste lid, 2<sup>o</sup>, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;

Op de voordracht van de Minister van Sociale Zaken en Volksgezondheid,

Hebben Wij besloten en besluiten Wij :

**Artikel 1.** Voor de toepassing van voorliggend besluit verstaat men onder :

1<sup>o</sup> 'ziekenhuis' : ziekenhuis in de zin van de wet van 10 juli 2008 betreffende de ziekenhuizen en andere verzorgingsinrichtingen;

2<sup>o</sup> 'de procedure' : alle gebruikte procedures, processen en de gehanteerde architectuur (hardware en software);

3<sup>o</sup> 'gedigitaliseerde gegevens' : gegevens die opgeslagen, verwerkt en meegedeeld worden door middel van een optische en fotografische techniek;

4° le format : le code sous lequel les données numérisées sont enregistrées sur un support de données;

5° la compression : l'opération permettant de réduire la taille de la présentation digitale des images afin de limiter la capacité de stockage et d'accélérer la transmission de données;

6° les métadonnées : le set d'informations décrivant le contexte, le contenu et la structure des données numérisées;

7° le système : l'ensemble du matériel et des logiciels d'exploitation et d'application;

8° le datacenter : la salle dans laquelle se trouve physiquement le matériel d'information et de communication (matériel IT) sur lequel les données numérisées sont traitées et/ou stockées.

**Art. 2.** Les données enregistrées, traitées ou communiquées selon des procédés photographiques et optiques ainsi que leur reproduction sur papier ou sur tout autre support lisible ont force probante, jusqu'à preuve du contraire, si la procédure fixée par l'hôpital conformément à l'article 3 pour leur enregistrement, leur communication, leur traitement ou leur reproduction satisfait aux conditions énumérées dans le présent arrêté et si les données ont été enregistrées, traitées ou communiquées conformément à cette procédure.

Toutefois, les données numérisées ne pourraient pas être privées de leur validité juridique au seul motif qu'il est contesté que la procédure réellement suivie répond aux conditions du présent arrêté, si celui qui se prévaut de ces données peut démontrer, par tous les moyens de droit, que le fait de déroger aux conditions du présent arrêté n'a pas compromis la fiabilité des données.

**Art. 3.** Les hôpitaux déterminent la procédure selon laquelle ils enregistrent, traitent ou communiquent au moyen de procédés photographiques et optiques, les informations dont ils disposent ou qui leur sont transmises, pour l'application dans les soins de santé, ainsi que la procédure selon laquelle ils assurent la reproduction de ces informations sur papier ou sur tout autre support lisible, conformément au présent arrêté.

**Art. 4.** L'hôpital utilise une procédure qui permet :

1° l'enregistrement systématique et sans lacunes des informations;

2° la reproduction fidèle, durable et complète des informations;

3° la conservation avec soin des informations, leur classement systématique et leur protection contre toute altération;

4° l'intégrité des informations et leur lisibilité durant l'entière durée du délai de conservation.

**Art. 5.** L'hôpital dispose d'une documentation détaillée, régulièrement mise à jour, relative à la procédure utilisée.

Cette documentation contient, à tout le moins, les éléments suivants :

1° les données d'identification de l'éventuel sous-traitant auquel l'hôpital fait appel, ainsi que le nom et l'adresse du propriétaire du matériel et du logiciel utilisé;

2° la marque et le type de matériel utilisé ainsi que la dénomination du logiciel utilisé;

3° la description précise du matériel et du logiciel utilisés, avec la mention des principales caractéristiques techniques des modes d'enregistrement, de traitement et de communication au moyen de techniques optiques ou photographiques utilisés;

4° la documentation de l'infrastructure de stockage utilisée;

5° la description de la façon dont l'intégrité des données numérisées est garantie et peut être contrôlée;

6° la description des contrôles de qualité effectués;

7° la documentation du logiciel d'amélioration de la qualité des images et du logiciel de reconnaissance;

8° la description de la façon dont sont garanties la disponibilité et l'accessibilité des données numérisées;

9° une description de la façon dont les données numérisées sont protégées contre l'accès non autorisé;

10° une description de la politique de sauvegarde.

Toute modification apportée à la procédure utilisée est immédiatement ajoutée à la documentation détaillée.

L'hôpital est capable de soumettre à tout moment la documentation dont il est question à l'alinéa 1<sup>er</sup> au comité sectoriel de la sécurité sociale et de la santé.

La documentation de la procédure, ainsi que le lien entre celle-ci et les données numérisées, sont conservées pendant toute la période de conservation.

**Art. 6.** L'accès aux données numérisées se déroule conformément aux règles et aux procédures en vigueur dans l'hôpital.

Toute opération effectuée sur les données numérisées, ainsi que l'identité de l'opérateur, est consignée dans un journal.

4° 'het formaat' : de code waaronder gedigitaliseerde gegevens zijn opgeslagen op een gegevensdrager;

5° 'compressie' : de bewerking waarbij de digitale voorstelling van de afbeeldingen in grootte beperkt worden om opslagcapaciteit te besparen en datatransmissie te versnellen;

6° 'metagegevens' : de gegevensset die de context, de inhoud en de structuur van de gedigitaliseerde gegevens beschrijft;

7° 'het systeem' : het geheel van apparatuur en besturings- en toepassingsprogrammatuur;

8° 'het datacenter' : de ruimte waarin de informatie- en communicatieapparatuur (IT-apparatuur) zich fysiek bevindt waarop de gedigitaliseerde gegevens verwerkt en/of opgeslagen worden.

**Art. 2.** De gegevens die door middel van een optische en fotografische techniek opgeslagen, verwerkt of meegedeeld worden, alsook de weergave van deze gegevens op papier of op elke andere leesbare drager, hebben bewijskracht tot bewijs van het tegendeel, indien de procedure die het ziekenhuis overeenkomstig artikel 3 heeft vastgesteld voor de opslag, de verwerking, de mededeling of de weergave van deze gegevens voldoet aan de voorwaarden opgesomd in dit besluit en de gegevens in overeenstemming met die procedure werden opgeslagen, verwerkt of meegedeeld.

De gedigitaliseerde gegevens kan echter geen rechtsgeldigheid worden ontzegd op de enkele grond dat betwist wordt dat de werkelijk gevolgde procedure aan de voorwaarden van dit besluit voldoet, als diegene die zich op deze gegevens beroept kan aantonen, met alle middelen van recht, dat de afwijking van de voorwaarden in dit besluit de betrouwbaarheid van de gegevens niet in het gedrang heeft gebracht.

**Art. 3.** De ziekenhuizen leggen de procedure vast volgens welke ze de gegevens waarover ze beschikken of die ze doorgestuurd krijgen, door middel van een optische en fotografische techniek opslaan, verwerken of meedelen voor de toepassing ervan in de gezondheidszorg, alsook de procedure volgens welke ze deze gegevens op papier of op elke andere leesbare drager weergeven, overeenkomstig dit besluit.

**Art. 4.** Het ziekenhuis gebruikt een procedure voor :

1° de systematische en volledige opslag van gegevens;

2° de getrouwe, duurzame en volledige weergave van de informatie;

3° de zorgvuldige bewaring, de systematische classificatie en de beveiliging van de gegevens tegen elke vorm van vervalsing;

4° de integriteit en de leesbaarheid van de gegevens gedurende de volledige bewaartermijn.

**Art. 5.** Het ziekenhuis beschikt over een gedetailleerde documentatie m.b.t. de gehanteerde procedure die regelmatig bijgewerkt wordt.

Deze documentatie bevat minstens de volgende onderdelen :

1° de identificatiegegevens van de eventuele verwerker op wie het ziekenhuis een beroep doet, evenals de naam en het adres van de eigenaar van de gebruikte hardware en software;

2° het merk en het type van de gebruikte hardware en de benaming van de gebruikte software;

3° de nauwkeurige beschrijving van de hardware en software, met vermelding van de voornaamste technische kenmerken van de wijze van opslag, verwerking en mededeling door middel van de gebruikte optische en fotografische techniek;

4° de documentatie van de gebruikte opslaginfrastructuur;

5° de beschrijving van de wijze waarop de integriteit van de gedigitaliseerde gegevens wordt verzekerd en kan worden gecontroleerd;

6° de beschrijving van de uitgevoerde kwaliteitscontroles;

7° de documentatie van de software voor de verbetering van de beeldkwaliteit en de herkenningsoftware;

8° de beschrijving van de wijze waarop de beschikbaarheid en de toegankelijkheid van de gedigitaliseerde gegevens worden verzekerd;

9° een beschrijving van de wijze waarop de gedigitaliseerde gegevens worden beveiligd tegen onbevoegde toegang;

10° een beschrijving van het back-upbeleid.

Elke aangebrachte wijziging aan de gebruikte procedure wordt onmiddellijk aan de gedetailleerde beschrijving toegevoegd.

Het ziekenhuis kan op elk moment de documentatie waarvan sprake in het eerste lid voorleggen aan het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid.

Zowel de documentatie van de procedure als de link tussen deze documentatie en de gedigitaliseerde gegevens wordt bijgehouden gedurende de volledige bewaartermijn.

**Art. 6.** De toegang tot de gedigitaliseerde gegevens verloopt conform de regels en procedures in voege in het ziekenhuis.

Elke bewerking van de gedigitaliseerde gegevens wordt samen met de identiteit van de bewerker in een logboek bijgehouden.

**Art. 7.** Les données numérisées sont conservées dans des formats de fichiers normalisés, validables et dûment documentés qui conviennent à une conservation à long terme.

Si un format intermédiaire est utilisé, aucune perte de qualité relevante ne peut se manifester lors de la conversion du format intermédiaire vers le format final.

La compression est autorisée uniquement si elle n'entraîne aucune perte de données relevante.

**Art. 8.** Les données numérisées sont stockées le jour de leur mise en forme dans une infrastructure de stockage garantissant l'intégrité et la pérennité des données.

La donnée numérisée et son original non numérisé restent liés par un identificateur unique jusqu'au moment de la destruction de l'original.

**Art. 9.** Le traitement des données numérisées a lieu dans un État membre de l'Union européenne ou dans un État tiers auquel est étendue la libre circulation des services et qui s'est engagé, dans le cadre d'un accord international avec l'Union européenne, à respecter la réglementation de l'Union en matière de traitement des données à caractère personnel.

**Art. 10.** L'intégrité du contenu, la durabilité, l'accessibilité et la lisibilité des données numérisées et des métadonnées y afférentes est garantie pendant tout le délai de conservation imposée par la réglementation applicable.

Les métadonnées sont attribuées de manière consistante et structurée.

Le lien entre la donnée numérisée et les métadonnées y afférentes peut être reconstruit durant toute le délai de conservation.

Toute donnée numérisée peut être retrouvée, dans un délai raisonnable, sur la base de métadonnées y afférentes et être rendues visible ou lisible dans le respect des autorisations données.

Le système utilisé importe, convertit, migre et exporte les données numérisées et les métadonnées y afférentes tout en garantissant leur confidentialité, leur intégrité et leur exploitabilité.

**Art. 11.** Les mesures de sécurité mises en œuvre pour garantir l'intégrité des données sont établies en conformité avec la politique de sécurité de l'information de l'hôpital.

L'hôpital réalise une analyse des risques systématique relative, entre autres, au traitement des données, aux systèmes, au personnel et aux exigences de sécurité.

L'hôpital dispose d'une politique en matière de sécurité de l'information reprenant l'ensemble des stratégies et mesures retenues pour sécuriser les données.

La politique mentionnée à l'alinéa précédent est établi sur la base de normes et/ou de lignes directrices reconnues par des instances nationales ou internationales.

Ainsi, au minimum, l'hôpital :

1° dispose d'un aperçu des mesures de sécurité utilisées et exécute une évaluation périodique (externe ou non) afin de vérifier si les mesures de sécurité mises en place sont encore adéquates ou non;

2° dispose d'une politique de sauvegarde adéquate et documentée, ainsi que d'un plan de reprise en cas de sinistres;

3° prend toutes les mesures nécessaires afin d'éviter la perte partielle ou totale des données numérisées pendant le délai de conservation. À cet égard, l'hôpital effectue des sauvegardes périodiques de toutes les données numérisées et les conserve dans un autre endroit sécurisé;

4° teste régulièrement et, le cas échéant, adapte les plans de sauvegarde et de reprise;

5° dispose d'une politique actualisée de contrôle des accès en vue d'octroyer, de modifier et de supprimer des droits d'accès au système;

6° fixe, en cas de sous-traitance, les exigences de sécurité pour ce tiers dans un contrat;

**Art. 7.** De gedigitaliseerde gegevens worden bewaard in valideerbare, genormeerde en volledig gedocumenteerde bestandsformaten geschikt voor bewaring op lange termijn.

Indien er gebruik gemaakt wordt van een tussenformaat, dan mag er geen relevant kwaliteitsverlies optreden bij de omzetting van het tussenformaat naar het uiteindelijke formaat.

Compressie is alleen toegestaan indien aantoonbaar geen relevant informatieverlies optreedt.

**Art. 8.** De gedigitaliseerde gegevens worden op de dag van hun opmaak opgeslagen in een opslaginfrastructuur die de integriteit en de duurzaamheid van de gegevens verzekert.

De gedigitaliseerde gegevens en de niet gedigitaliseerde originele gegevens worden blijvend met elkaar gelinkt via een unieke identifier tot op het moment waarop het origineel vernietigd wordt.

**Art. 9.** De verwerking van de gedigitaliseerde gegevens gebeurt in een lidstaat van de Europese Unie of in een derde staat waarnaar het vrij verkeer van diensten is uitgebreid en die zich er in het kader van een internationaal akkoord met de Europese Unie toe heeft verbonden om de regelgeving van de Unie betreffende de verwerking van persoonsgegevens te respecteren.

**Art. 10.** De integriteit van de inhoud, de duurzaamheid, de toegankelijkheid en de leesbaarheid van de gedigitaliseerde gegevens en de hieraan verbonden metagegevens worden gewaarborgd gedurende de door de toepasselijke reglementering opgelegde bewaartermijn.

Metagegevens worden op een consistente en gestructureerde wijze toegekend.

De koppeling tussen de gedigitaliseerde gegevens en de bijbehorende metagegevens kan gedurende de volledige bewaartermijn worden gereconstrueerd.

Elk van de gedigitaliseerde gegevens kan binnen een redelijke termijn worden teruggevonden aan de hand van de bijbehorende metagegevens en kan waarneembaar of leesbaar gemaakt worden, met inachtneming van de autorisaties.

Het gebruikte systeem importeert, converteert, migreert en exporteert de gedigitaliseerde gegevens en de bijbehorende metagegevens met behoud van de betrouwbaarheid, de integriteit en de bruikbaarheid ervan.

**Art. 11.** De veiligheidsmaatregelen die de gegevensintegriteit waarborgen, zijn opgesteld overeenkomstig het informatieveiligheidsbeleid van het ziekenhuis.

Het ziekenhuis voert een systematische risicoanalyse uit o.a. betreffende de gegevensverwerking, de systemen, het personeel en de veiligheidseisen.

Het ziekenhuis beschikt over een informatieveiligheidsbeleid dat het geheel van strategieën en gekozen maatregelen voor de gegevensbeveiliging bevat.

Het in het vorige lid vermelde beleid is gebaseerd op de normen en/of richtlijnen die door nationale en internationale instanties erkend worden.

Aldus doet het ziekenhuis minstens het volgende :

1° het heeft een overzicht van de gehanteerde veiligheidsmaatregelen en toetst periodiek (extern of niet) of de ingevoerde veiligheidsmaatregelen nog passend zijn of niet;

2° het beschikt over een gedocumenteerd en passend back-upbeleid, calamiteiten- en herstelplan;

3° het treft alle nodige maatregelen om te voorkomen dat de gedigitaliseerde gegevens gedeeltelijk of geheel verloren zouden gaan gedurende de bewaartermijn. Hiertoe maakt het ziekenhuis periodiek back-ups van alle gedigitaliseerde gegevens en bewaart het deze back-ups op een andere beveiligde locatie;

4° het test op regelmatige basis de back-up- en herstelplannen en past ze indien nodig aan;

5° het beschikt over een geactualiseerd toegangscontrolebeleid voor het toekennen, het wijzigen en het verwijderen van toegangsrechten tot het systeem;

6° het stelt in geval van onderaanneming veiligheidseisen aan deze derde via een contract;

7° détruit, à l'issue du délai de prescription utilisé par l'institution concernée (qui est au moins équivalent au délai de prescription légal), les données numérisées à l'aide d'un processus documenté. S'il s'agit de données sensibles, des méthodes de destruction sécuritaires devront être mises en œuvre;

8° dispose d'un datacenter dûment sécurisé et équipé d'un système d'air conditionné, d'une alarme et d'un équipement de détection d'incendie, d'un contrôle des accès, d'un câblage ordonné et d'une source d'énergie électrique de secours;

9° prévoit la redondance dans l'infrastructure de stockage;

10° stocke les supports de données, ainsi que les sauvegardes dans un endroit physique sécurisé;

11° dispose de suffisamment de collaborateurs dont les connaissances et compétences sont suffisantes pour pouvoir assumer l'ensemble des tâches et responsabilités de l'organisation en ce qui concerne la gestion des données numérisées;

12° en cas de migrations vers de nouveaux formats, les transferts vers les supports de données sont réalisés à temps, afin d'assurer l'intégrité et l'accès permanent aux données numérisées, et ce pendant tout le délai de conservation.

Les mesures de sécurité minimales dont il est question à l'alinéa précédent restent d'application pour le processus de migration documenté mis en œuvre par l'hôpital.

**Art. 12.** Le ministre qui a les Affaires sociales dans ses attributions et le ministre qui a la Santé publique dans ses attributions sont chargés, chacun en ce qui les concerne, de l'exécution du présent arrêté.

Donné à Bruxelles, le 10 mai 2015.

PHILIPPE

Par le Roi :

La Ministre des Affaires sociales et de la Santé publique,  
Mme M. DE BLOCK

7° na afloop van de door de instelling gehanteerde verjaringstermijn (die ten minste de wettelijke verjaringstermijn moet zijn), vernietigt het de gedigitaliseerde gegevens aan de hand van een gedocumenteerd proces. Indien het gevoelige gegevens betreft, moeten er veilige vernietigingsmethodes uitgevoerd worden;

8° het beschikt over een goed beveiligd datacenter met onder meer klimaatbeheersing, een alarm en een brandmeldvoorziening, een toegangscontrole, een ordelijke bekabeling en een noodstroomvoorziening;

9° het voorziet in redundantie in de opslaginfrastructuur;

10° het slaat de informatiedragers en back-ups in een fysiek beveiligde plaats op;

11° het beschikt over voldoende medewerkers, met voldoende kennis en competenties, om al zijn taken en verantwoordelijkheden op het gebied van het beheer van gedigitaliseerde gegevens te kunnen uitvoeren;

12° in geval van migraties naar nieuwe bestandsformaten worden de overdrachten naar gegevensdragers tijdig uitgevoerd om de integriteit en de permanente toegang tot de gedigitaliseerde gegevens gedurende de volledige bewaartermijn te kunnen verzekeren.

De minimale veiligheidsmaatregelen waarvan sprake in het vorige lid blijven van kracht voor het gedocumenteerde migratieproces dat door het ziekenhuis uitgevoerd wordt.

**Art. 12.** De minister bevoegd voor Sociale Zaken en de minister bevoegd voor Volksgezondheid zijn, ieder wat hem betreft, belast met de uitvoering van dit besluit.

Gegeven te Brussel, 10 mei 2015.

FILIP

Van Koningswege :

De Minister van Sociale Zaken en Volksgezondheid,  
Mevr. M. DE BLOCK

#### SERVICE PUBLIC FEDERAL INTERIEUR ET SERVICE PUBLIC FEDERAL JUSTICE

[C - 2015/00200]

29 MAI 2015. — Arrêté royal exécutant l'article 67, 2° à 4°, de la loi du 26 avril 2002 relative aux éléments essentiels du statut des membres du personnel des services de police et portant diverses autres dispositions relatives aux services de police

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la loi du 26 avril 2002 relative aux éléments essentiels du statut des membres du personnel des services de police et portant diverses autres dispositions relatives aux services de police, l'article 67, 2° à 4°, modifié par la loi du 20 juin 2006 et la loi du 26 mars 2014;

Vu l'arrêté royal du 30 mars 2001 portant la position juridique du personnel des services de police (PJPo);

Vu l'avis de l'Inspecteur général des Finances, donné le 31 mars 2014;

Vu l'accord du Ministre du Budget, donné le 2 avril 2014;

Vu le protocole de négociation n° 343/3 du comité de négociation pour les services de police, conclu le 12 mai 2014;

Vu l'accord du Secrétaire d'Etat à la Fonction publique, donné le 14 juillet 2014;

Vu l'article 8, § 1<sup>er</sup>, 4°, de la loi du 15 décembre 2013 portant des dispositions diverses concernant la simplification administrative, le présent arrêté est dispensé d'analyse d'impact de la réglementation, s'agissant d'autorégulation;

Vu l'avis 56.063/2 du Conseil d'Etat, donné le 12 mai 2014, en application de l'article 84, § 1<sup>er</sup>, alinéa 1<sup>er</sup>, 2°, des lois sur le Conseil d'Etat, coordonnées le 12 janvier 1973;

Sur la proposition du Ministre de l'Intérieur et du Ministre de la Justice et l'avis des Ministres qui en ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

**Article 1<sup>er</sup>.** Dans l'annexe 3 PJPo, modifiée par l'arrêté royal du 16 avril 2002, l'arrêté royal du 18 septembre 2008 et l'arrêté royal du 23 mai 2013, la note de bas de page est remplacée par ce qui suit :

#### FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN EN FEDERALE OVERHEIDSDIENST JUSTITIE

[C - 2015/00200]

29 MEI 2015. — Koninklijk besluit ter uitvoering van artikel 67, 2° tot 4°, van de wet van 26 april 2002 houdende de essentiële elementen van het statuut van de personeelsleden van de politiediensten en houdende diverse andere bepalingen met betrekking tot de politiediensten

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de wet van 26 april 2002 houdende de essentiële elementen van het statuut van de personeelsleden van de politiediensten en houdende diverse andere bepalingen met betrekking tot de politiediensten, artikel 67, 2° tot 4°, gewijzigd bij de wet van 20 juni 2006 en de wet van 26 maart 2014;

Gelet op het koninklijk besluit van 30 maart 2001 tot regeling van de rechtspositie van het personeel van de politiediensten (RPPo);

Gelet op het advies van de Inspecteur-generaal van financiën, gegeven op 31 maart 2014;

Gelet op de akkoordbevinding van de Minister van Begroting, d.d. 2 april 2014;

Gelet op het protocol van onderhandelingen nr. 343/3 van het onderhandelingscomité voor de politiediensten, gesloten op 12 mei 2014;

Gelet op de akkoordbevinding van de Staatssecretaris voor Ambt-narenzaken, d.d. 14 juli 2014;

Gelet op artikel 8, § 1, 4°, van de wet van 15 december 2013 houdende diverse bepalingen inzake administratieve vereenvoudiging is dit besluit vrijgesteld van een regelgevingsimpactanalyse omdat het autoregulering betreft;

Gelet op advies 56.063/2 van de Raad van State, gegeven op 12 mei 2014, met toepassing van artikel 84, § 1, eerste lid, 2°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;

Op de voordracht van de Minister van Binnenlandse Zaken en de Minister van Justitie en op het advies van de in Raad vergaderde Ministers,

Hebben Wij besloten en besluiten Wij :

**Artikel 1.** In bijlage 3 RPPo, gewijzigd bij het koninklijk besluit van 16 april 2002, het koninklijk besluit van 18 september 2008 en het koninklijk besluit van 23 mei 2013, wordt de voetnoot vervangen als volgt :