Comité de sécurité de l'information
chambres réunies
(chambre sécurité sociale et santé/chambre autorité fédérale)[1]

DELIBERATION N° 23/003 DU 7 MARS 2023 RELATIVE A LA MISE A DISPOSITION DE LA CARTE ISI+ ET DES CERTIFICATS COVID NUMERIQUES DE L'UE A LA PERSONNE CONCERNEE VIA LE PORTEFEUILLE NUMERIQUE

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, en particulier l'article 15, § 2 ;

Vu la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions*, en particulier l'article 11, premier alinéa ;

Vu la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, en particulier l'article 42 ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 111 et 114 ;

Vu la loi du 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, en particulier les articles 97 et 98 ;

Vu la demande relative à la mise à disposition de la carte ISI+ et les Certificats COVID Numériques de l'UE via le portefeuille numérique ;

Vu le rapport d'auditorat de la Banque Carrefour de la Sécurité Sociale et du service public fédéral Stratégie et Appui;

Vu le rapport de M. VIAENE et M. HACHÉ.

[1] Cette délibération ne s'applique qu'en tant que délibération des **chambres réunies** (chambre sécurité sociale et santé et chambre autorité fédérale) pour la communication des données à caractère personnel relatives à la carte ISI+ par les organismes d'assurance (via la BCSS) au service public fédéral Stratégie et Appui (en tant que intégrateur des services fédéral) en vue de la mise à disposition du titulaire du droit dans le portefeuille numérique.
La communication des données à caractère personnel concernant les Certificats COVID Numériques de l'UE en vue de la mise à disposition au titulaire des droits relève de la compétence de **la chambre sécurité sociale et santé du Comité de la sécurité de l'information**.

I. OBJET DE LA DEMANDE

1. Le service public fédéral Stratégie et Appui développe le portefeuille numérique pour le compte du gouvernement fédéral[2]. Le portefeuille numérique est une application (app) pour appareils mobiles, à la fois pour les systèmes d'exploitation iOS et Android, qui permet aux citoyens de prouver leur identité de manière mobile, de demander et/ou de recevoir des messages, des certificats et des documents, et de les stocker.

2. Avec le portefeuille numérique, la Belgique se prépare à la future obligation européenne selon laquelle chaque État membre doit offrir un tel portefeuille numérique[3]. Il est actuellement prévu qu'une fois le règlement modifiant le règlement eIDAS adopté à cet égard, les États membres devront mettre en œuvre le portefeuille numérique dans un certain délai, probablement 12 mois.

3. Les fonctionnalités du portefeuille numérique belge sont développées par le service public fédéral Stratégie et Appui en plusieurs phases. **A terme**, le portefeuille numérique pourra contenir les fonctionnalités suivantes[4]:

- **Identité mobile** : le portefeuille numérique stocke les composants nécessaires pour prouver l'identité numérique de la personne concernée.

- **eSign** : la possibilité pour le citoyen d'apposer sa signature électronique via le certificat de signature de sa carte d'identité numérique.

- **Messages eBox via My eBox** : dans le portefeuille numérique, la personne concernée peut voir ses messages et documents eBox, dès qu'elle en a donné l'autorisation. Il sera averti lorsqu'un nouveau message ou document sera envoyé.

- **eLoket/eGuichet** : la personne concernée peut demander et stocker des certificats, permis, copies ou extraits officiels ainsi que le permis de conduire numérique via des applications auprès des autorités affiliées.

- **eSafe** : les documents reçus peuvent être stockés localement et en toute sécurité.

- **MyData** : la personne concernée peut accéder aux informations mises à disposition via MyData via le portefeuille numérique. Via MyData, le citoyen aura accès aux données que les institutions publiques participantes détiennent à son sujet.

- **Fonction de numérisation** : les codes QR qui font partie des documents inclus dans le portefeuille numérique d'une personne peuvent être numérisés à partir du portefeuille numérique d'une autre personne grâce à cette fonctionnalité. Dans la mesure où les codes répondent aux critères à déterminer (par exemple, signature électronique valide, format de code QR, etc.), leur exactitude peut être confirmée. A terme, par exemple, il sera possible de vérifier l'exactitude du code QR d'un permis de conduire numérique.

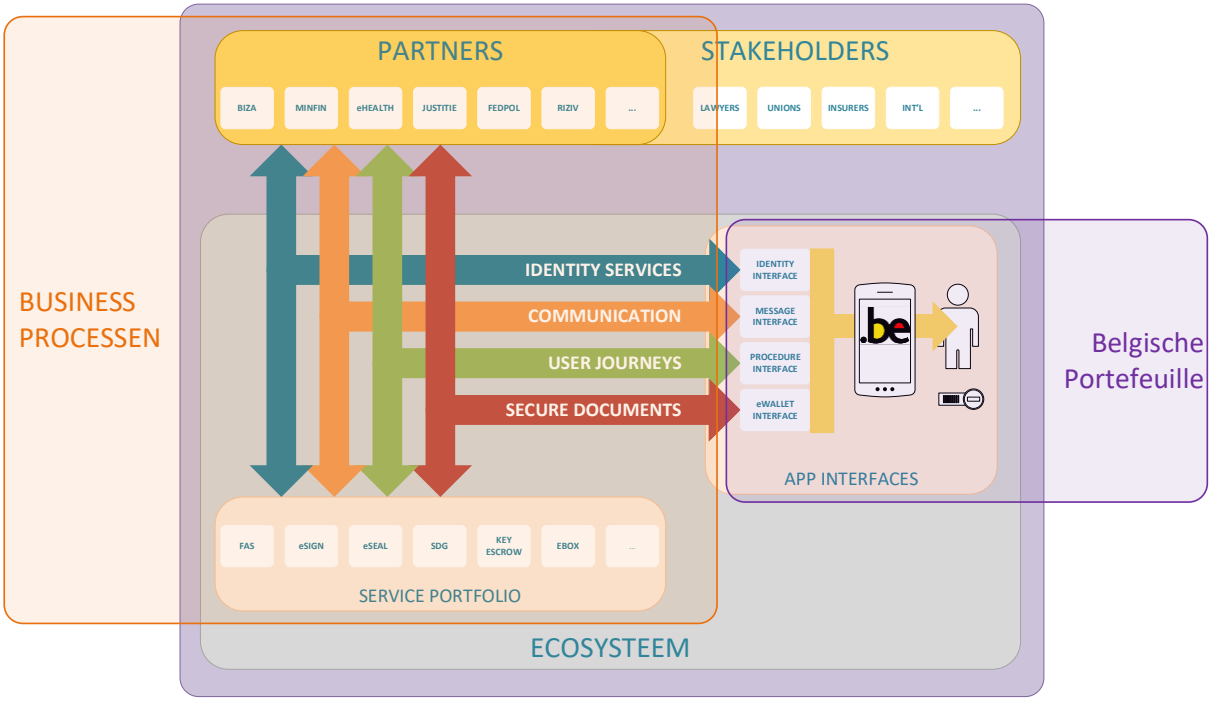
---

[2] Dans la présente délibération, l'application mobile est dénommée « le portefeuille numérique », par analogie avec la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 sur un cadre européen pour une identité numérique. Le nom de l'application mobile est sujet à changement.

[3] Proposition de Règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52021PC0281

[4] Les modalités concrètes et les noms des futures fonctionnalités, ainsi que le nom du portefeuille numérique peuvent encore changer.

4. Le portefeuille numérique est donc une plate-forme générique qui permet d'offrir des services du secteur public aux citoyens sur des appareils mobiles de manière standard. La plate-forme se compose d'une application mobile, sous le contrôle de la personne concernée, et de composants data center, sous la direction du service public fédéral Stratégie et Appui. L'installation et l'utilisation des fonctionnalités du portefeuille numérique sont volontaires. La personne concernée doit accepter les conditions d'utilisation et la déclaration de confidentialité qui lui seront présentées après l'installation et l'activation.

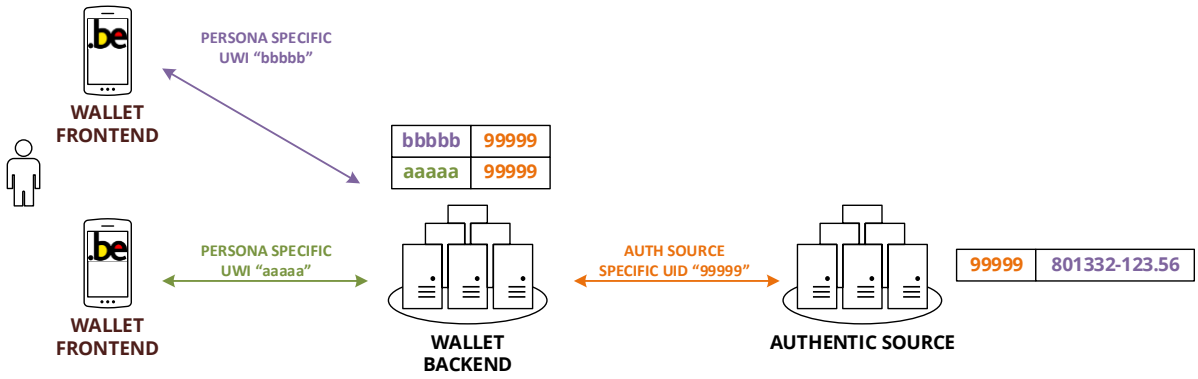


5. On travaille dans une logique de privacy by design basée sur les principes de base suivants, qui s'appliquent à toutes les fonctions du portefeuille numérique :
- Les composants data center du portefeuille numérique ne contiennent que des références techniques pour faire fonctionner l'écosystème. En dehors des numéros d'identification pseudonymisés, aucune donnée à caractère personnel de l'utilisateur n'est stockée dans les composants data center et aucune référence croisée n'est possible.
- L'application mobile ne s'adresse pas directement aux sources authentiques. L'échange de données s'effectue via les composants data center du portefeuille numérique de manière sécurisée.
- Les données destinées à l'application mobile peuvent être cryptées à la source (c'est-à-dire en dehors du portefeuille numérique), après quoi la garantie est offerte qu'elles ne peuvent être lues que par la bonne instance d'application[5], sur le bon appareil et par le bon utilisateur.
- Les données stockées dans le portefeuille numérique peuvent être stockées cryptées sur le téléphone de la même manière.

---

[5] L'*instance* est une application installée. Sur Android, il est possible de créer plusieurs utilisateurs sur 1 appareil. S'il y a 2 utilisateurs sur un appareil, chacun ayant installé l'application, cela est considéré comme 2 instances.

6. Pour activer le portefeuille numérique, il doit être lié à une personne réelle. Lors de l'activation, le portefeuille numérique génère des secrets[6] et des identifiants aléatoires. Ceux-ci sont ensuite liés à une source à une personne réelle sur la base d'un identifiant neutre.



Le portefeuille numérique n'a pas besoin d'avoir les attributs personnels que la source authentique gère pour que l'écosystème fonctionne (dans l'exemple : 801332-123.56).

L'identifiant utilisé pour identifier un utilisateur du portefeuille numérique à la source authentique[7] est interne et ne peut être utilisé qu'à cette fin et uniquement entre ces parties (dans l'exemple : 99999).

L'identifiant utilisé pour distinguer les applications actives et les appareils disponibles pour un utilisateur n'est disponible que pour les composants applicatifs et de centre de données du portefeuille numérique (dans l'exemple : aaaaa et bbbbb).

Un ensemble différent de secrets est généré pour chaque combinaison d'utilisateur, d'application, d'appareil et de ressource actifs. Les identifiants aaaaa et bbbbb sont donc uniques par utilisateur, application installée, appareil utilisé et la source avec laquelle l'utilisateur est activé.

Les identifiants utilisés par source (99999) sont uniques par source. Les ressources ne peuvent pas utiliser ces données pour détecter les utilisateurs connus sur les deux.

7. Le portefeuille numérique offre un certain nombre de services de base qui permettent aux partenaires d'offrir des données et des services à l'utilisateur. Ces données et services restent sous le contrôle du service concerné et/ou de l'utilisateur final à tout moment.

- Le portefeuille numérique peut être utilisé pour authentifier et/ou identifier l'utilisateur (comme clé numérique), mais seule la source authentique (i.e. le Registre National) dispose des données personnelles nécessaires pour faire le lien avec une personne physique. La source authentique peut le déverrouiller via le Federal Authentication System (FAS) ou directement à la partie qui souhaite déverrouiller les données via le portefeuille numérique.[8]

---

[6] Il s'agit des paires de clés asymétriques.

[7] En principe chaque source authentique peut attribuer un identifiant à l'utilisateur. Dans le cadre de l'activation du portefeuille numérique et de la création du clé numérique il s'agit du Registre National.

[8] A terme, le portefeuille numérique contiendra également les éléments de la carte d'identité électronique numérique, à délivrer par le SPF Intérieur, avec laquelle les citoyens pourront s'identifier et s'authentifier vis-à-vis

- Les données peuvent être sécurisées de bout en bout (end-2-end). Dans ce cas, la partie qui souhaite déverrouiller les données via le portefeuille numérique peut crypter ces données sur la base des clés de cryptage générées par le portefeuille numérique sur l'appareil. Seul le bon utilisateur peut alors déchiffrer ces données sur le bon appareil avec le bon corps du portefeuille numérique.

- Les données stockées sur l'appareil mobile sont stockées cryptées, après quoi seul le bon utilisateur sur le bon appareil avec le bon corps du portefeuille numérique peut revoir ces données.

8. **Cette délibération vise exclusivement et spécifiquement la mise à disposition de la carte ISI+ et des certificats numériques COVID de l'UE (vaccination, test et récupération)** par les institutions responsables concernées via le portefeuille numérique aux titulaires de droits. Les personnes concernées pourront demander ces documents via une application dans le portfolio numérique. Elles sont ensuite récupérées via l'intégrateur de services fédéral à partir des sources authentiques en question et transférées dans le portefeuille numérique de la personne concernée. Tant la carte ISI+ que les certificats numériques COVID de l'UE concernent la mise à disposition aux personnes concernées elles-mêmes ou, dans le cas de mineurs, à leurs parents ou représentants légaux.

9. **Concernant la carte ISI+** : Les adultes et les enfants à partir de 12 ans peuvent s'inscrire auprès d'un pharmacien, d'un médecin ou d'un hôpital avec leur carte d'identité électronique ou eID. Avec l'eID, le prestataire de soins peut consulter la base de données en ligne de la caisse d'assurance maladie. Ainsi, les prestataires de soins disposent toujours des informations les plus récentes disponibles et il est possible de vérifier si la personne concernée a droit à un remboursement de la caisse d'assurance maladie. Ceux qui ne peuvent pas obtenir d'eID recevront **une carte ISI+**. La carte ISI+ peut être utilisée chez le pharmacien, le médecin ou à l'hôpital, tout comme une eID. La carte ISI+ n'est pas une carte d'identité : elle permet uniquement de s'identifier auprès des prestataires de soins et de l'organisme assureur.

10. La carte ISI+ est délivrée par les organismes assureurs, conformément aux dispositions de la loi du 29 janvier 2014 *portant dispositions sur la carte d'identité sociale et la carte ISI+* et de l'arrêté d'exécution du 26 février 2014. La Banque Carrefour de la Sécurité Sociale gère le base de données centrale des cartes ISI+. Le fichier central des cartes ISI+ vise à délivrer, renouveler, remplacer et utiliser les cartes ISI+ de manière sécurisée et contient les informations nécessaires à cet effet.

11. **Concernant les certificats COVID numériques de l'UE :** depuis la pandémie de COVID, les citoyens - selon les règles applicables - sont tenus de prouver leur statut en termes de vaccination, de test ou de récupération au moyen de certificats. Au moyen d'un accord de coopération entre les gouvernements fédéral et régionaux[9], des accords ont été conclus

---

des tiers (au moyen du certificat d'authentification de l'eID numérique) et les documents peuvent signer (à l'aide du certificat de signature de l'eID numérique). En attendant cette carte d'identité électronique numérique, le citoyen créera une clé numérique avec laquelle il pourra s'authentifier en ligne auprès des autorités connectées au Federal Authentication System (FAS) du SPF BOSA.

[9] Accord de coopération du 14 juillet 2021, modifié à plusieurs reprises, entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement des données liées au certificat COVID numérique de l'UE et au COVID Safe Ticket, le PLF et le traitement des données à caractère personnel des

concernant la préparation, la délivrance et la vérification du certificat numérique EU-COVID. Les certificats COVID numériques de l'UE sont créés via une application sur un appareil mobile (l'application COVIDSafe) ou via les sites Web de certaines instances publiques.

12. Conformément à l'article 6, § 2, de l'Accord de coopération du 14 juillet 2021, modifié à plusieurs reprises, l'agence flamande Digitaal Vlaanderen, à la demande de la plateforme e-Health, a été chargée de fournir des services opérationnels pour le développement de l'application COVIDSafe ainsi que l'application COVIDScan (sur la base de laquelle les certificats respectifs sont lisibles numériquement), l'agance flamande Digitaal Vlaanderen agissant en tant que sous-traitant. L'agence flamande Digitaal Vlaanderen ne décide pas quelle application est mise à disposition du citoyen, ni sur les modalités et l'heure de désactivation de l'application COVIDSafe et COVIDScan. L'agence flamande Digitaal Vlaanderen n'agit que *sur instruction de la plateforme e-Health*.

II. TRAITEMENT DE LA DEMANDE

A. RECEVABILITE ET COMPETENCE DU COMITE

13. Conformément à l'article 15, §2, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* **toute communication de données sociales à caractère personnel par la Banque-carrefour de la sécurité sociale ou une institution de sécurité sociale** visée à l'article 2, alinéa 1er, 2°, a), **à un service public fédéral**, à un service public de programmation ou à un organisme fédéral d'intérêt public autre qu'une institution de sécurité sociale doit faire l'objet d'une délibération préalable des **chambres réunies** du comité de sécurité de l'information dans la mesure où les responsables du traitement de l'instance qui communique, de l'instance destinatrice et de la Banque-carrefour de la sécurité sociale ne parviennent pas, en exécution de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à un accord concernant la communication ou au moins un de ces responsables du traitement demande une délibération et en a informé les autres responsables du traitement. Dans les cas mentionnés, la demande est introduite d'office conjointement par les responsables du traitement concernés.

14. En ce qui concerne la communication des données de **la carte ISI+**, il y a la communication des données à caractère personnel par les organismes d'assurance et la Banque Carrefour de la Sécurité Sociale à l'intégrateur de services fédéral (SPF BOSA) afin de mettre la carte ISI+ à la disposition des titulaires des droits, en particulier la personne concernée elle-même ou, dans le cas de mineurs, aux parents ou aux représentants légaux. Les chambres réunies du Comité de la sécurité de l'information s'estiment donc compétentes pour se prononcer à ce sujet.

15. Conformément à l'article 11 de la loi du 21 août 2008 *à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions*, toute communication de données à caractère personnel par ou à destination de la plateforme eHealth nécessite une autorisation de principe de **la chambre sécurité sociale et santé** du Comité de sécurité de l'information.

---

travailleurs salariés et des travailleurs indépendants vivant ou résidant à l'étranger qui effectuent des activités en Belgique et Accord de coopération d'exécution du 15 octobre 2021.

16. En outre, conformément à l'article 42 de la loi du 13 décembre 2006 *portant des dispositions diverses relatives à la santé*, la chambre sécurité sociale et santé est compétente pour accorder une autorisation de principe à l'égard de toute communication de données personnelles relatives à la santé, sous réserve de les exceptions prévues par la loi précitée.

17. Conformément à l'art. 6, § 2, de l'Accord de coopération du 14 juillet 2021 l'agence flamande Digitaal Vlaanderen, en tant que sous-traitant, traite les données à caractère personnel à la demande et sur les instructions de la plateforme eHealth en le contexte des services opérationnels pour le développement de l'application COVIDSafe et de l'application COVIDScan (au moyen desquels les certificats respectifs sont lisibles numériquement). La communication des données concernant les certificats numériques COVID de l'UE via l'application COVIDSafe à l'intégrateur de services fédéral est une communication à la demande et sur instruction de la plateforme eHealth. La chambre sécurité sociale et santé du comité de la sécurité de l'information s'estime donc compétente pour se prononcer à ce sujet. Par souci d'exhaustivité, le comité de sécurité de l'information précise qu'il ne se prononce pas sur la composition des certificats ou l'utilisation des certificats. Dans le cadre de cette délibération, il ne concerne que la manière dont les certificats numériques COVID de l'UE peuvent être mis à la disposition de la personne concernée ou, s'il s'agit d'un mineur, des parents ou des représentants légaux.

B. QUANT AU FOND

B.1. RESPONSABILITE

18. Conformément à l'article 5.2 du règlement général sur la protection des données[10], ci-après 'RGDP'), les organismes assureurs, la Banque Carrefour de la Sécurité Sociale et la plate-forme eHealth (instances communicantes) et le SPF BOSA (instance réceptrice en qualité d'intégrateur de services fédéral et de fournisseur du portefeuille numérique) – en tant que responsables du traitement – sont responsables du respect des principes énoncés à l'article 5, paragraphe 1, du RGPD et doivent être en mesure de le démontrer [11].

---

[10] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*.

[11] Les données à caractère personnel doivent être:

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);
b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);
c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);
d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);
e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou

19. Le RGPD impose toute une série d'obligations qui incombent aux responsables de traitement. A cet égard, le présent rapport passe en revue les principales obligations qui sont prévues explicitement par le RGPD mais rappelle et insiste à ce stade-ci de son analyse sur celle qui impose à tout responsable du traitement de tenir un registre des activités de traitement conformément et dans le respect des modalités prévues à l'article 30 du RGPD.

B.2. LICEITE

20. Conformément à l'article 5.1 a), du RGPD, les données à caractère personnel doivent être traitées de manière licite. Cela signifie que le traitement envisagé doit être fondé sur l'une des bases de licéité énoncées à l'article 6 du RGPD ou, en ce qui concerne le traitement des données de santé, sur l'une des exceptions énumérées à l'article 9 du RGPD.

21. La création et la délivrance de la carte ISI+ sont régies par la loi du 29 janvier 2014 *portant dispositions sur la carte d'identité sociale et la carte ISI+* et l'arrêté d'exécution du 26 février 2014. Celle-ci stipule que les organismes assureurs délivrent la carte ISI+ et que le Carrefour Banque de la sécurité sociale gère la base de données centrale des cartes ISI+, qui vise à délivrer, renouveler, remplacer et utiliser les cartes ISI+ de manière sécurisée.

22. En ce qui concerne le rôle du service public fédéral Stratégie et Appui, l'article 2, premier alinéa, 33°, de l'arrêté royal du 22 février 2017 confie expressément au SPF Stratégie et Appui la mission de « *développer et gérer les services numériques et des plateformes d'interaction numérique avec les citoyens et les entreprises et entre les administrations* ». Le rôle du SPF Stratégie et Appui en tant qu'intégrateur de services fédéral est régi par la loi du 15 août 2012 *portant création et organisation d'un intégrateur de services fédéral*, plus spécifiquement par les articles 4, 5 et suivants. Compte tenu de ce qui précède, le traitement de données à caractère personnel dans le cadre de la mise à disposition de la carte ISI+ via le portefeuille numérique à la personne concernée elle-même ou, dans le cas d'un mineur, à ses parents ou représentants légaux, est nécessaire pour respecter une obligation légale incombant aux responsables du traitement (art. 6.1 c) RGPD).

23. La création et la délivrance des Certificats COVID numériques de l'UE sont régies par l'accord de coopération du 14 juillet 2021 sur la base duquel l'application COVIDSafe a été développée par l'agence flamande Digitaal Vlaanderen sur instruction de la plate-forme eHealth. L'accord de coopération stipule explicitement que l'agence flamande Digitaal Vlaanderen, à la demande de la plateforme eHealth, est chargée de fournir des services opérationnels pour le développement de l'application COVIDSafe et de l'application COVIDScan (sur la base de laquelle les certificats respectifs sont lisibles numériquement), dans lequel l'agence flamande agit en tant que sous-traitant. Conformément à l'accord de coopération, la plate-forme eHealth est donc autorisée à émettre les instructions nécessaires au développement de l'application COVIDSafe, y compris la manière dont les certificats COVID numériques de l'UE sont mis à la disposition de la personne concernée elle-même

---

historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

ou, dans le cas d'un mineur, aux parents ou au représentant légal doit être compris. Etant donné qu'il s'agit d'un traitement de données de santé, il peut être établi que le traitement remplit l'une des conditions dans lesquelles l'interdiction de traitement de telles données en vertu de l'article 9.2 du RGPD est écartée. En effet, le traitement est nécessaire pour des raisons d'intérêt public dans le domaine de la santé publique, telles que la protection contre les menaces transfrontières graves pour la santé, sur la base du droit de l'Union ou du droit d'un État membre qui prévoit des mesures appropriées et spécifiques pour protéger la droits et libertés de la personne concernée, notamment du secret professionnel. À cet égard, il convient donc de se référer à l'accord de coopération du 14 juillet 2021.

B.2. LIMITATIONS DE FINALITES

24. Article 5.1 b) RGPD ne permet le traitement de données à caractère personnel que pour des fins déterminées, explicites et légitimes (principe de limitation des finalités).

25. Le comité de sécurité de l'information note que les communications sont destinées à des finalités effectivement bien définies et explicitement décrites, à savoir mettre la carte ISI+ et les certificats COVID numériques de l'UE à la disposition de la personne concernée ou, dans le cas d'un mineur, des parents ou représentants légaux via le portefeuille numérique.

26. Compte tenu des missions légales des différentes instances concernées, telles que décrites ci-dessus, le Comité de sécurité de l'information considère également que les finalités sont justifiées.

B.3. MINIMISATION DE DONNEES ET LIMITATION DE CONSERVATION

27. L'article 5.1 c) du RGPD dispose que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées («minimisation de données»).

28. La communication ne concerne, d'une part, que les données de la carte ISI+ telles que décrites dans la loi du 29 janvier 2014 *portant dispositions sur la carte d'identité sociale et la carte ISI+* et l'arrêté d'exécution du 26 février 2014, et, d'autre part d'autre part, les certificats COVID numériques de l'UE tels que décrits dans l'accord de coopération du 14 juillet 2021.

29. L'identification de la personne concernée dans le cadre de la communication par les parties concernées via l'intégrateur de services fédéral pour divulguer la carte ISIS+ et les certificats COVID numériques de l'UE à la personne concernée ou, dans le cas d'un mineur, aux parents ou aux représentant via le portefeuille numérique, est basé sur le numéro d'identification de sécurité sociale, qui se compose soit du numéro de registre national, soit du numéro d'identification attribué par la Banque Carrefour de la sécurité sociale (appelé numéro bisregister). Cependant, l'utilisation du numéro de registre national n'est pas libre et nécessite une autorisation explicite. A cet égard, le comité de sécurité de l'information constate que l'intégrateur de services fédéral est effectivement autorisé à utiliser le numéro du Registre national tel que prévu à l'article art. 5, § 1er de la loi du 15 août 2012 *instituant et organisant un service fédéral intégrateur*.

30. Pour accéder à ces données spécifiques (carte ISI+ et Certificates COVID numériques de l'UE) dans le portefeuille numérique de la personne concernée ou, dans le cas d'un mineur, des parents ou du représentant légal, le SPF Stratégie et Appui utilisera également le numéro de registre national (plus précisément une forme pseudonymisée du numéro de registre national, cf. marginal numéro 6) de la personne concernée et, dans le cas d'un mineur, des

parents ou du représentant légal. Conformément à l'article 15, §3, de la loi du 15 janvier 1990 *portant création et organisation d'une Banque-Carrefour de la Sécurité Sociale* et conformément à l'art. 35/1, §2, de la loi du 15 août 2012 *relative à la création et à l'organisation d' un intégrateur de services fédéral*, respectivement la chambre sécurité sociale et santé et la chambre autorité fédérale sont autorisées à accorder une délibération sur l'utilisation du numéro d'identification du Registre national des personnes physiques par les autorités compétentes si cela est nécessaire dans le cadre de la communication envisagée. Les deux chambres accordent donc une délibération au service public fédéral Stratégie et Appui pour utiliser le numéro du Registre national aux fins décrites dans la présente délibération. La durée de conservation des données pseudonymisées par le SPF BOSA est limitée à ce qui est nécessaire, notamment la durée de l'activation de l'application par la personne concernée. En plus, le Comité de sécurité de l'information estime nécessaire que le SPF BOSA prévoit un life cycle management des comptes afin d'assurer les actions nécessaires en cas de décès.

31. En ce qui concerne la durée de conservation, le comité de sécurité de l'information rappelle que les données à caractère personnel ne doivent pas être conservées sous une forme permettant d'identifier les personnes concernées plus longtemps que nécessaire aux fins pour lesquelles les données à caractère personnel sont traitées.

32. Le Comité de sécurité de l'information prend acte du fait que l'intégrateur de services fédéral ne conserve les données concernant la carte ISI+ et les Certificats COVID numériques de l'UE que pendant la durée nécessaire au transfert vers le portefeuille numérique de la personne concernée elle-même ou, en cas de un mineur, les parents ou le représentant légal. Le stockage des documents et certificats reçus dans le portefeuille numérique est exclusivement déterminé par le titulaire du portefeuille numérique, y compris la durée de conservation des données pertinentes.

B.4. SECURITE

33. Les données à caractère personnel doivent être traitées en prenant des mesures techniques ou organisationnelles appropriées de manière à assurer une sécurité adéquate, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle («intégrité et confidentialité»).[12]

34. Compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des différents risques pour les droits et libertés des personnes physiques en termes de probabilité et de gravité, le responsable du traitement doit prendre les mesures techniques et organisationnelles appropriées pour garantir et démontrer que le traitement est effectué conformément au règlement général sur la protection des données. Ces mesures sont réexaminées et mises à jour si nécessaire.

35. Le Comité de sécurité de l'information prend acte du fait que le Service public fédéral Politique et Appui a nommé à la fois un délégué à la protection des données et un conseiller en sécurité de l'information (CISO).

36. Le comité de la sécurité de l'information prend note du fait que le principe de confidentialité dès la conception a été appliqué dans le développement du portefeuille numérique.

---

[12] Art. 5.1 f) RGDP.

- Les composants data center du portefeuille numérique ne contiennent que des références techniques pour faire fonctionner l'écosystème. En dehors des numéros d'identification pseudonymisés, aucune donnée à caractère personnel de l'utilisateur n'est stockée dans les composants data center et aucune référence croisée n'est possible.
- L'application mobile ne s'adresse pas directement aux sources authentiques. L'échange de données s'effectue via les composants data center du portefeuille numérique de manière sécurisée.
- Les données destinées à l'application mobile peuvent être cryptées à la source (c'est-à-dire en dehors du portefeuille numérique), après quoi la garantie est offerte qu'elles ne peuvent être lues que par la bonne *instance* d'application[13], sur le bon appareil et par le bon utilisateur.
- Les données stockées dans le portefeuille numérique peuvent être stockées de manière encryptées sur le téléphone de la même manière.
- Le portefeuille numérique peut être utilisé pour authentifier et/ou identifier l'utilisateur, mais seule la source authentique dispose des données personnelles nécessaires pour faire le lien avec une personne physique. La source authentique peut le déverrouiller via le Federal Authentication System (FAS) ou directement à la partie qui souhaite déverrouiller les données via le portefeuille numérique.
- Les données peuvent être sécurisées de bout en bout (end-2-end). Dans ce cas, la partie qui souhaite déverrouiller les données via le portefeuille numérique peut crypter ces données sur la base des clés de cryptage générées par le portefeuille numérique sur l'appareil. Seul le bon utilisateur peut alors déchiffrer ces données sur le bon appareil avec le bon corps du portefeuille numérique.
- Les données stockées sur l'appareil mobile sont stockées cryptées, après quoi seul le bon utilisateur sur le bon appareil avec le bon corps du portefeuille numérique peut revoir ces données.

37. Le Comité de la sécurité de l'information prend acte du fait que le SPF Stratégie et Appui procède à une analyse d'impact sur la protection des données en application de l'article 35 du RGPD. Compte tenu de la nécessité de cette analyse d'impact sur la protection des données, le Comité de Sécurité de l'Information considère que cette délibération ne peut en tout état de cause être accordée que sous réserve de sa mise en œuvre. S'il ressort de cette évaluation que des mesures complémentaires doivent être prises, les parties concernées soumettront de leur propre initiative une demande de modification de la présente délibération. Le cas échéant, la communication des données à caractère personnel ne pourra avoir lieu qu'après l'obtention de l'autorisation requise du Comité de sécurité de l'information. Si l'analyse d'impact sur la protection des données montre qu'il existe un risque résiduel élevé, les demandeurs doivent soumettre le traitement de données envisagé à l'Autorité de protection des données, conformément à l'art. 36.1 RGPD.

[13] L'*instance* est une application installée. Sur Android, il est possible de créer plusieurs utilisateurs sur 1 appareil. S'il y a 2 utilisateurs sur un appareil, chacun ayant installé l'application, cela est considéré comme 2 instances.

Par ces motifs,

les chambres réunies du comité de sécurité de l'information et de la chambre sécurité sociale et santé, chacune pour ce qui concerne la communication relevant de leurs compétences respectives, décident

que la communication des données à caractère personnel concernant la carte ISI+ et les Certificats COVID numériques de l'UE à la personne concernée ou, s'il s'agit d'un mineur, à ses parents ou représentants légaux via le portefeuille numérique tel que proposé par le SPF Stratégie et Appui, est autorisée moyennant le respect des mesures de protection de la vie privée, et en particulier des données à caractère personnel, qui ont été définies dans cette délibération en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la durée de conservation des données et de sécurité de l'information.

Le Comité de sécurité de l'information prend note qu'une analyse d'impact sur la protection des données concernant le portefeuille numérique sera réalisée par le SPF Stratégie et Appui. Il en communiquera, pour information, une copie au Comité de sécurité de l'information. S'il ressort de cette analyse que des mesures supplémentaires doivent être prises pour sauvegarder les droits et libertés des personnes concernées, les parties sont tenues de soumettre les modalités modifiées de traitement des données au Comité pour délibération.

B. VIAENE
Chambre sécurité sociale et santé

D. HACHÉ
Chambre autorité fédérale