

Informatieveiligheidscomité Kamer sociale zekerheid en gezondheid

IVC/KSZG/26/032

BERAADSLAGING NR. 26/016 VAN 13 JANUARI 2026 MET BETREKKING TOT DE VERWERKING VAN GEPSEUDONIMISEERDE PERSOONSGEGEVENS DIE DE GEZONDHEID BETREFFEN DOOR DE VERZEKERINGSINSTELLINGEN, HET NATIONAAL INTERMUTUALISTISCH COLLEGE EN HET RIZIV IN HET KADER VAN DE WET TOT UITVOERING VAN EEN VERSTERKT TERUG NAAR WERKBELEID IN GEVAL VAN ARBEIDSONGESCHIKTHEID (GAOCIT-DATABANK)

De kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité (hierna “het Comité” genoemd);

Gelet op de Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (Algemene Verordening Gegevensbescherming of AVG);

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*;

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*, inzonderheid op artikel 15;

Gelet op de wet van 13 december 2006 *houdende diverse bepalingen betreffende gezondheid*, in het bijzonder artikel 42, § 2, 3°;

Gelet op de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen*;

Gelet op de wet van 19 december 2025 *tot uitvoering van een versterkt terug naar werkbeleid in geval van arbeidsongeschiktheid*;

Gelet op de aanvraag van het RIZIV;

Gelet op het auditoraatsrapport van het eHealth-platform van 2 januari 2026;

Gelet op het verslag van de heer Michel Deneyer;

Beslist op 13 januari 2026, na beraadslaging, als volgt:

I. ONDERWERP VAN DE AANVRAAG

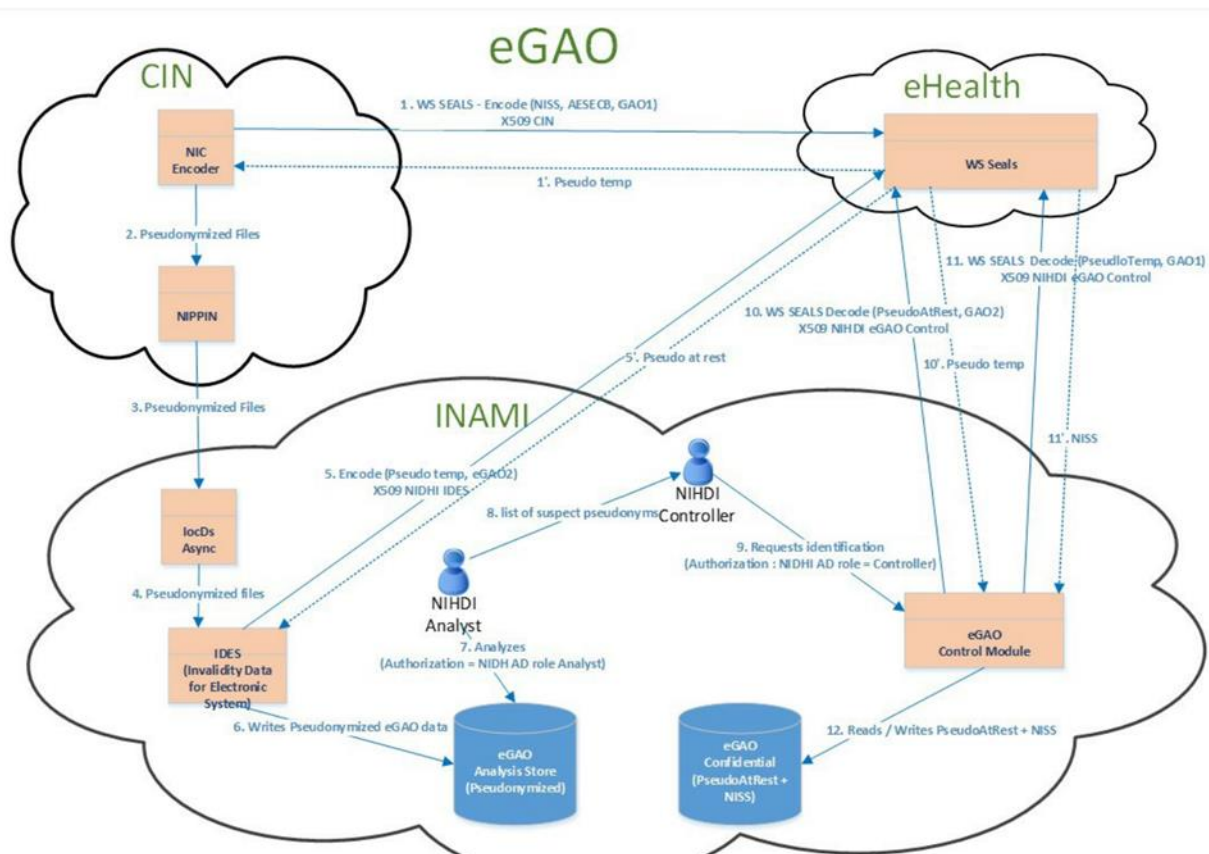
1. De regering wenst tijdens deze legislatuur een globaal plan voor de preventie en re-integratie van langdurig zieken uit te werken. De bedoeling van dat allesomvattend plan is om de betrokken actoren meer te responsabiliseren.
2. De betrokken personen zijn de gerechtigden op de uitkeringen vermeld in artikel 86, § 1, van de wet *betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen*, gecoördineerd op 14 juli 1994, en in artikel 3 van het koninklijk besluit van 20 juli 1971 *houdende instelling van een uitkeringsverzekering en een moederschapsverzekering ten voordele van de zelfstandigen en van de meewerkende echtgenoten* voor wie de behandelende artsen een elektronisch arbeidsongeschiktheidsattest opmaken ten behoeve van de medisch adviseur van het ziekenfonds. De arbeidsongeschiktheidsattesten worden elektronisch overgemaakt door de behandelende artsen via hun softwarepakket aan de medisch adviseur van het ziekenfonds voor de voormelde gerechtigden in het kader van het project Mult-eMediatt, iteratie 1.
3. In de artikelen 13 en 14 van de wet van 19 december 2025 *tot uitvoering van een versterkt terug naar werkbeleid in geval van arbeidsongeschiktheid* wordt bepaald dat er een “GAOCIT”-databank met gepseudonimiseerde gegevens wordt opgericht binnen het RIZIV op basis waarvan de analyses, opvolgingen, rapporteringen en datamining zullen worden uitgevoerd¹. De oprichting van deze databank vereist het gebruik van de dienst SEALS van het eHealth-platform.
4. Op termijn zal deze GAOCIT-databank de volgende gepseudonimiseerde gegevens omvatten:
 - de gepseudonimiseerde identificatiegegevens van de rechthebbende op uitkeringen (het INSZ - identificatienummer bedoeld in artikel 8 van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid*);
 - de identificatiegegevens van de betrokken behandelende arts (het INSZ of het RIZIV-nummer);
 - de begin- en einddatum van de arbeidsongeschiktheidsperiode;
 - een op eenvormige wijze gecodeerde pathologie of diagnose;
 - indien beschikbaar de vermelding dat het een eerste aangifte van arbeidsongeschiktheid of een verlenging van de arbeidsongeschiktheid betreft;
 - de datum van aanmaak van het elektronisch attest.
5. Het Nationaal Intermutualistisch College (NIC) zal deze beperkte gegevensset met het INSZ van de gepseudonimiseerde patiënt aan het RIZIV overmaken. Het RIZIV zal aldus over een GAOCIT-gegevensbank beschikken op basis waarvan de analyses, de opvolgingen, de rapporteringen en de datamining zullen kunnen worden verricht. Deze pseudonimisering kan echter worden opgeheven op verzoek van de service “SIDU-SECM CONTROL” (de

¹ Art. 13 van de wet van 19 december 2025 *tot uitvoering van een versterkt terug naar werkbeleid in geval van arbeidsongeschiktheid*.

zogenaamde NIHDI CONTROL) in het kader van de wettelijke opdrachten van het RIZIV inzake medische controle voor de individuele dossiers naargelang de verrichte vaststellingen.

Schematische beschrijving van de gegevensuitwisseling

6. Het INSZ zal door het Nationaal Intermutualistisch College (NIC) aan het eHealth-platform worden meegedeeld via de volgende procedure:



Step 1 : Pseudonymization WS SEALS at NIC side NIC Encoder contacts eHealth to encode SSIN into a temporary pseudonym Encode for project = eGAO1 Algorithm "AESECB": This algorithm realizes a no randomized encryption. This means that each time a user encrypts a same input with the same key, he receives the same output.

Steps 2–4 : File Transfert to NIHDI NIC Encoder sends the pseudonymized file to NIPPIN (NIC messaging system) NIPPIN forwards the file to IOCds IOCds delivers the pseudonymized data to IDES

Step 5 : Retrieve Pseudonym at rest (eGAO2) IDES calls eHealth to encode the temporary pseudonym WS SEALS ENCODE (pseudo temp, Algorithm "AESECB") -> returns pseudo at rest authentication = cert X509 NIHDI IDES

Steps 6 : IDES stores pseudonym at rest Tip : Right click on image(s) --> open in a new tab to view them in full screen Contact Person The pseudonym returned by eHealth is persisted in eGAO Analysis datastore {pseudonym at rest}

Steps 7 : Analysis of pseudonymized data NIHDI Analyst accesses eGAO pseudonymized datastore in order to find suspect records

Step 8 : Communication of lists of suspect records to NIHDI Controller This action occurs outside the application {Excel file}

Steps 9–12 : Suspicious Case Identification NIHDI Controller requests identification of pseudonyms related to a suspect record via the eGAO Control web application NIHDI Controller is authorized via NIHDI Active Directory group membership Two calls to eHealth ensue: a. WS SEALS DECODE {pseudo at rest, eGAO2} -> returns pseudo temp authentication = X509 cert NIHDI eGAO control b. WS SEALS DECODE {pseudo temp, eGAO1} -> returns NISS authentication = X509 cert "eGAO control" eGAO Control writes the SSIN with the corresponding pseudonym at rest to the Confidential Store eGAO Control reads nominative data from eGAO Confidential Store {contains SSIN} Access is authorized via NIHDI Active Director.

7. Bovendien moet de eindgebruiker de opheffing van de pseudonimisering van het INSZ van de rechthebbende op de uitkeringen in de volgende gevallen kunnen vragen:

In het kader van de doeleinden beschreven in voormelde wet zal het NIC een beperkte gegevensset overmaken aan het RIZIV met het INSZ van de gepseudonimiseerde patiënt. Het RIZIV zal aldus over een databank beschikken waarin de bovenvermelde analyses, opvolgingen, rapporteringen en datamining zullen worden verricht.

Deze pseudonimisering kan echter worden opgeheven op verzoek van de service "SIDU-SECM CONTROL" (de zogenaamde NIHDI CONTROL) in het kader van de wettelijke opdrachten van het RIZIV inzake medische controle voor de individuele dossiers naargelang de verrichte vaststellingen. Voor de uitvoering van hun controle-opdrachten in het kader van de verwerking van individuele dossiers door de Dienst uitkeringen en de Dienst voor geneeskundige evaluatie en controle van het RIZIV mogen de artsen van de Dienst uitkeringen die lid zijn van de Geneeskundige Raad voor Invaliditeit en de sociale inspecteurs van de Dienst voor geneeskundige evaluatie en controle toegang krijgen tot de gedepseudonimiseerde gegevens.

8. Hiertoe vragen ze aan het eHealth-platform om toegang te krijgen tot het identificatienummer bedoeld in artikel 8 van de wet van 15 januari 1990 dat werd gedepseudonimiseerd op basis van de vaststellingen verricht door:
 - de artsen van de Dienst uitkeringen, lid van de Geneeskundige Raad voor Invaliditeit, voor de opdrachten die hen zijn toegekend krachtens artikel 82, 2^{de} lid, van de wet betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen, gecoördineerd op 14 juli 1994 (de beslissingsmacht uitvoeren met betrekking tot de arbeidsongeschiktheid);

- de artsen-inspecteurs van de Dienst voor geneeskundige evaluatie en controle, voor de opdrachten die hen zijn toegekend krachtens 139, 4^{de} lid, van de gecoördineerde wet van 14 juli 1994 (die onder meer zijn belast met de controle van de verstrekkingen van de gezondheidszorgverzekering op het vlak van de realiteit en de conformiteit met de bepalingen van deze wet, de uitvoeringsbesluiten en verordeningen ervan en de overeenkomsten en akkoorden afgesloten krachtens diezelfde wet en met de medische controle van de uitkerings- en moederschapsverzekering).
9. Het Nationaal Intermutualistisch College (NIC) enerzijds en het RIZIV anderzijds verbinden zich ertoe om:
- ervoor te zorgen dat de depseudonimisering van het INSZ van de patiënt uitsluitend gebeurt via tussenkomst van het eHealth-platform dat een rol van vertrouwensderde vervult (TTP - Trusted Third-Party);
 - elke poging tot heridentificatie van een patiënt te verbieden op basis van het tijdelijk pseudoniem; bij een poging zullen de tussenkomende partijen (RIZIV, NIC, ziekenfondsen) de noodzakelijke maatregelen nemen zodat elke poging tot schending van hun verbintenis op voldoende afschrikkende wijze wordt gesanctioneerd en het Informatieveiligheidscomité op de hoogte brengen.
10. Volgens de contextdiagram gaat het NIC niet over tot depseudonimisering. Er zijn 2 verschillende sleutels. Een sleutel om het INSZ te pseudonimiseren (de pseudonimisering geschiedt door het eHealth-platform op verzoek van het NIC). Een sleutel voor het pseudonimiseren van de pseudonimisering verstuurd door het NIC en verricht door het eHealth-platform op verzoek van het RIZIV. Het RIZIV kent aldus het INSZ niet (pseudonimisering door het NIC) en het NIC weet niet op welke pseudonimiseringen de onderzoeken werden verricht (pseudonimisering door het RIZIV). Om te depseudonimiseren moet het RIZIV via het eHealth-platform passeren.

II. BEVOEGDHEID

11. Ingevolge artikel 42, § 2, 2° van de wet van 13 december 2006 *houdende diverse bepalingen betreffende gezondheid* is de kamer sociale zekerheid en gezondheid van het Informatieveiligheidscomité in beginsel bevoegd voor het verlenen van een principiële beraadslaging met betrekking tot elke mededeling van persoonsgegevens die de gezondheid betreffen.
12. Krachtens artikel 11 van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform* vereist elke mededeling van persoonsgegevens door of aan het eHealth-platform een principiële machtiging van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité.

III. BEHANDELING

A. TOELAARBAARHEID

13. Krachtens artikel 6 van de Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (AVG)* is de verwerking van persoonsgegevens enkel rechtmatig indien en voor zover minstens één van de vermelde voorwaarden vervuld is².
14. Krachtens artikel 5 van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform* is het eHealth-platform onder meer ermee belast een systeem voor pseudonimisering en anonimisering van informatie te ontwikkelen. Krachtens artikel 7 van voormelde wet heeft het eHealth-platform voor de uitvoering van zijn opdrachten het recht om het identificatienummer van het Rijksregister te gebruiken.
15. Het RIZIV werd bij het koninklijk besluit van 5 december 1986 gemachtigd om voor het vervullen van zijn opdrachten toegang te hebben tot het Rijksregister van de natuurlijke personen. De verzekeringsinstellingen verklaren dat ze gemachtigd zijn om het rijksregisternummer te gebruiken en om toegang te hebben tot het Rijksregister krachtens artikel 1 van het koninklijk besluit van 5 december 1986 *tot regeling van de toegang tot de informatiegegevens en van het gebruik van het identificatienummer van het Rijksregister van de natuurlijke personen in hoofde van instellingen die, in het kader van de wetgeving betreffende de ziekte- en invaliditeitsverzekering, opdrachten van algemeen belang vervullen*.
16. De verwerking van persoonsgegevens die de gezondheid betreffen is in principe verboden, overeenkomstig artikel 9, § 1, van de Verordening (EU) 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming), hierna de AVG genoemd.
17. Dit verbod geldt echter niet wanneer de verwerking noodzakelijk is voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnoses, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen (art. 9, §2, h) van de AVG.
18. Het Comité stelt vast dat de wet van 19 december 2025 *tot uitvoering van een versterkt terug naar werkbeleid in geval van arbeidsongeschiktheid* in het Belgisch Staatsblad van 30

² Artikel 6, § 1, c) van de AVG: de verwerking is noodzakelijk voor de naleving van een wettelijke verplichting waaraan de verwerkingsverantwoordelijke is onderworpen.

december 2025 werd bekendgemaakt. De betrokken bepalingen treden in werking op 1 januari 2026.

B. DOELBINDING

19. Overeenkomstig art. 5, b) van de AVG is de verwerking van persoonsgegevens enkel toegelaten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.
20. Zoals beschreven in artikel 13, § 3, van de wet van 19 december 2025 *tot uitvoering van een versterkt terug naar werkbeleid in geval van arbeidsongeschiktheid* heeft de GAOCIT-databank met gepseudonimiseerde gegevens als doel om:
 - 1) Over voldoende kennis te beschikken
 - over het aantal gevallen waarin een arbeidsongeschiktheid door een huisarts wordt vastgesteld waarbij rekening wordt gehouden met de grootte en de patiëntenpopulatie van zijn artspraktijk, de exacte duur van de arbeidsongeschiktheid gekoppeld aan de bij de patiënt vastgestelde diagnose of pathologie die door die arts wordt voorgeschreven;
 - over het aantal huisartsen dat door een sociaal verzekerde wordt geraadpleegd in het kader van de therapeutische relatie die de betrokken rechthebbende op uitkeringen in geval van een voorschrijven van een periode van arbeidsongeschiktheid met die artsen heeft.
 - 2) Deze kennis moet het mogelijk maken om zelfbeheertools te ontwikkelen voor de artsen aan de hand waarvan ze hun voorschrijfgedrag kunnen vergelijken en aanpassen aan wetenschappelijk onderbouwde “normen” en het voorschrijfgedrag van hun collega’s in eenzelfde regio.
 - 3) Financiële sensibilisering van voorschrijvende artsen met betrekking tot het voorschrijven van arbeidsongeschiktheid in het kader van de therapeutische relatie. Het RIZIV zal gebruikmaken van de nieuwe GAOCIT-databank die op 1 januari 2026 in werking treedt. Het RIZIV zal aldus dankzij die databank de betrokken artsen kunnen identificeren, contacteren, opvolgen en in voorkomend geval financieel sanctioneren. Het RIZIV zal ze bovendien aanmoedigen om hun gedrag met betrekking tot het voorschrijven van een arbeidsongeschiktheid bij te sturen via sensibiliseringscampagnes met als doel het aanpassen van hun voorschrijfgedrag met betrekking tot arbeidsongeschiktheid. Deze artsen zullen ook financieel verantwoordelijk kunnen worden gesteld voor hun voorschrijfgedrag volgens de modaliteiten die zullen worden vastgelegd in de RIZIV-reglementering.

C. PROPORTIONALITEIT

21. Overeenkomstig art. 5, b) en c), van de AVG dienen de persoonsgegevens toereikend, ter zake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt.
22. Elke betrokkene wordt geïdentificeerd met zijn identificatienummer van de sociale zekerheid, hetzij het rijksregisternummer (krachtens artikel 1 van het koninklijk besluit van 5 december 1986 *tot regeling van de toegang tot de informatiegegevens en van het gebruik van het identificatienummer van het Rijksregister van de natuurlijke personen* is het RIZIV gemachtigd om het rijksregisternummer te gebruiken), hetzij het kruispuntbanknummer (het gebruik van het kruispuntbanknummer is vrij, overeenkomstig artikel 8, § 2, van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*).
23. Het NIC zal een beperkte gegevensset met het INSZ van de gepseudonimiseerde patiënt aan het RIZIV overmaken. Het RIZIV zal aldus over een databank beschikken op basis waarvan de analyses, de opvolgingen, de rapporteringen en de datamining zullen kunnen worden verricht:
 - de identificatiegegevens van de gerechtigde op uitkeringen (identificatienummer bedoeld in artikel 8 van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid) en van de betrokken behandelende arts (identificatienummer bedoeld in artikel 8 van voormelde wet van 15 januari 1990 of het RIZIV-nummer);
 - de begin- en einddatum van de arbeidsongeschiktheidsperiode;
 - een op eenvormige wijze gecodeerde pathologie of diagnose;
 - indien beschikbaar de vermelding dat het een eerste aangifte van arbeidsongeschiktheid of een verlenging van de arbeidsongeschiktheid betreft;
 - de datum van aanmaak van het elektronisch attest.
24. Het RIZIV is de verwerkingsverantwoordelijke voor de gepseudonimiseerde gegevens³. Deze gegevens zullen worden verwerkt volgens de voorwaarden van artikel 13, § 4, van voormelde wet door de Dienst Uitkeringen van het RIZIV (artsen SIDU en data-analisten), de Dienst voor geneeskundige evaluatie en controle van het RIZIV (artsen-inspecteurs) en de Dienst DataOffice van het RIZIV voor het beheer van de gegevens.
25. Overeenkomstig artikel 5, 8°, van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform* komt het eHealth-platform tussen als intermediaire organisatie door middel van het gebruik van de dienst SEALS (*zie de punten 6 tot 10*). Het eHealth-platform mag de codeersleutel bewaren gedurende de duur die noodzakelijk is voor de uitvoering van die opdracht en de volledige duur waarin de pseudonimisering kan worden

³ Art. 13, § 5, van de wet van 19 december 2025 *tot uitvoering van een versterkt terug naar werkbeleid in geval van arbeidsongeschiktheid*.

gevraagd zoals voorzien in artikel 13, § 3, laatste lid, van de wet van 19 december 2025 tot uitvoering van een versterkt terug naar werkbeleid in geval van arbeidsongeschiktheid .

D. OPSLAGBEPERKING

26. Overeenkomstig artikel 5, § 1, e) , van de AVG mogen de persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verkregen. De persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, § 1, mits de bij de verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen ("opslagbeperking").
27. In artikel 13, § 6, van voormelde wet van 19 december 2025 wordt bepaald dat *“de gegevens in de GAOCIT-databank niet langer bewaard worden dan noodzakelijk voor de verwezenlijking van de doelstelling van de verwerking ervan, met een maximale bewaartermijn van vijf jaar te rekenen vanaf 1 januari van het jaar dat volgt op het jaar waarin het desbetreffende elektronische getuigschrift is opgesteld.”*

E. TRANSPARANTIE

28. Overeenkomstig artikel 12 van de AVG moet de verwerkingsverantwoordelijke passende maatregelen nemen opdat de betrokkene informatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt. De informatie wordt schriftelijk of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen, verstrekt.
29. Het RIZIV verklaart dat het krachtens artikel 14, § 5, van de AVG niet noodzakelijk is om de betrokkene te informeren omdat deze laatste reeds over deze informatie beschikt (het betreft de arbeidsongeschiktheidsattesten die door de huisartsen worden ingevuld). Het verkrijgen of verstrekken van de gegevens is bovendien uitdrukkelijk voorgeschreven bij Unie- of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen.

F. VEILIGHEIDSMATREGELEN

30. Overeenkomstig art. 5, f) van de AVG moet de aanvrager alle gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de persoonsgegevens. Deze maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend, enerzijds, met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's.

31. Om de vertrouwelijkheid en de veiligheid van de gegevensverwerking te garanderen, moet iedere instelling die persoonsgegevens bewaart, verwerkt of meedeelt maatregelen nemen in de volgende elf actiedomeinen die betrekking hebben op de informatieveiligheid: veiligheidsbeleid; aanstelling van een functionaris inzake gegevensbescherming; organisatorische en menselijke aspecten van de veiligheid (vertrouwelijkheidsverbintenis van het personeel, regelmatige informatieverstrekking en opleidingen ten behoeve van het personeel inzake bescherming van de privacy en veiligheidsregels); fysieke veiligheid en veiligheid van de omgeving; netwerkbeveiliging; logische toegangs- en netwerkbeveiliging; loggings, opsporing en analyse van de toegangen; toezicht, nazicht en onderhoud; systeem van beheer van de veiligheidsincidenten en de continuïteit (backup-systemen, fault tolerance-systemen, ...) en documentatie.
32. Het Comité stelt vast dat het RIZIV, het NIC en het eHealth-platform een functionaris voor gegevensbescherming hebben aangesteld en over een informatieveiligheidsbeleid beschikken.
33. Het Comité herinnert eraan dat de bepalingen van artikel 35 van de AVG met betrekking tot de gegevensbeschermingseffectbeoordeling moeten worden nageleefd.
34. Het RIZIV, het NIC en het eHealth-platform verklaren dat hun medewerkers gehouden zijn aan een vertrouwelijkheidsplicht. Dit geldt ook voor de behandelende artsen die aan het medisch geheim zijn onderworpen krachtens artikel 458 van het Strafwetboek.
35. Het Comité herinnert eraan dat krachtens artikel 9 van de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* de verwerkingsverantwoordelijke de volgende maatregelen neemt bij de verwerking van genetische, biometrische of gezondheidsgegevens:
 - 1° hij of, in voorkomend geval, de verwerker wijst de categorieën van personen die toegang hebben tot de persoonsgegevens aan, waarbij hun hoedanigheid ten opzichte van de verwerking van de betrokken gegevens nauwkeurig wordt omschreven;
 - 2° hij of, in voorkomend geval, de verwerker houdt de lijst van de aldus aangewezen categorieën van personen ter beschikking van de bevoegde toezichthoudende autoriteit;
 - 3° hij zorgt ervoor dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling ertoe gehouden zijn het vertrouwelijk karakter van de betrokken gegevens in acht te nemen.
36. Het Comité wijst op de bepalingen van Titel 6 van de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* waarin strenge administratieve sancties en strafsancities zijn voorzien in hoofde van de verwerkingsverantwoordelijke en van de verwerkers voor het niet-naleven van de voorwaarden voorzien in de AVG en de voormelde wet van 30 juli 2018.

Om deze redenen,

de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité

besluit dat de mededeling van de persoonsgegevens zoals beschreven in deze beraadslaging toegestaan is mits wordt voldaan aan de vastgestelde maatregelen ter waarborging van de gegevensbescherming, in het bijzonder de maatregelen op het vlak van doelbinding, minimale gegevensverwerking, opslagbeperking en informatieveiligheid;

verleent de machtiging voor het gebruik van de basisdienst SEALS van het eHealth-platform volgens de procedure voorzien in artikel 13 van de wet van 19 december 2025 *tot uitvoering van een versterkt terug naar werkbeleid in geval van arbeidsongeschiktheid*.

Deze beraadslaging treedt in werking op 14 januari 2026.

Michel DENEYER
Voorzitter

De zetel van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité is gevestigd in de kantoren van de Kruispuntbank van de Sociale Zekerheid, op het volgende adres: Willebroekkaai 38 - 1000 Brussel.
