

<p>Informatieveiligheidscomité Kamer sociale zekerheid en gezondheid</p>
--

IVC/KSZG/21/352

BERAADSLAGING NR. 21/174 VAN 15 SEPTEMBER 2021, GEWIJZIGD OP 21 SEPTEMBER 2021, MET BETREKKING TOT DE MEDEDELING VAN PERSOONSgegevens DOOR DE RIJKSDIENST VOOR SOCIALE ZEKERHEID EN VACCINNET+ AAN HET EHEALTH-PLATFORM VOOR HET BEPALEN VAN DE GRAAD VAN VACCINATIE TEGEN HET COVID-19-VIRUS VAN DE WERKNEMERS PER WERKGEVER EN VESTIGINGSEENHEID MET MINSTENS VIJFTIG WERKNEMERS, TEN BEHOEVE VAN DE BEVOEGDE DIENSTEN VOOR PREVENTIE EN BESCHERMING OP HET WERK

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*, in het bijzonder 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*, in het bijzonder artikel 5;

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*;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, in het bijzonder artikel 114;

Gelet op de wet van 5 september 2018 *tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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*, in het bijzonder artikel 97;

Gelet op de aanvraag van de Rijksdienst voor Sociale Zekerheid;

Gelet op het rapport van de Kruispuntbank van de Sociale Zekerheid;

Gelet op het verslag van de waarnemend voorzitter;

Beslist de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité, na beraadslaging, als volgt:

I. ONDERWERP VAN DE AANVRAAG

1. De diverse diensten voor preventie en bescherming op het werk – de externe diensten voor preventie en bescherming op het werk (onder de koepel van de vereniging zonder winstoogmerk CO-PREV), de interne diensten voor preventie en bescherming op het werk (onder de koepel van de vereniging voor interne bedrijfsartsen VVIB) en de gemeenschappelijke interne dienst voor preventie en bescherming op het werk van de Belgische federale overheid (EMPREVA) – willen bij het eHealth-platform, meer bepaald in de databank “contactgegevens van collectiviteiten” (zie de beraadslaging nr. 20/134 van 3 mei 2020, meermaals gewijzigd), de graad van vaccinatie tegen het COVID-19-virus kunnen nagaan van het personeel van de werkgevers aan wie zij hun diensten verstrekken (desgevallend ook op het niveau van de verschillende vestigingseenheden), op een (voor wat betreft de werknemers) anonieme wijze.
2. Aldus zouden de Rijksdienst voor Sociale Zekerheid (de openbare instelling van sociale zekerheid bevoegd voor het innen van de sociale bijdragen en het verwerken van de persoonsgegevens met betrekking tot de tewerkstelling, de lonen en de arbeidstijden) en Vaccinnet+ (het samenwerkingsverband tussen de deeltentiteiten aangaande de COVID-19-vaccinatie) enkele persoonsgegevens overmaken aan het eHealth-platform. Er zou in het bijzonder gebruik worden gemaakt van de volgende authentieke bronnen: de DMFA-databank (informatie uit de driemaandelijke multifunctionele werkgeversaangifte, nodig voor het identificeren van de werknemers per werkgever), het werkgeversrepertorium (informatie over de identiteit van de werkgevers) en de vaccinatiedatabank (informatie over de verstrekte vaccins). Die persoonsgegevens zouden door het eHealth-platform worden verwerkt tot louter anonieme gegevens (wat de werknemers betreft) en als dusdanig ter beschikking worden gesteld van de bevoegde diensten voor preventie en bescherming op het werk.
3. Elke dienst voor preventie en bescherming op het werk zou per werkgever voor wie hij bevoegd is en die minstens vijftig werknemers in dienst heeft van wie de vaccinatiestatus bekend is toegang krijgen tot het percentage werknemers die niet gevaccineerd zijn, het percentage werknemers die gedeeltelijk gevaccineerd zijn, het percentage werknemers die volledig gevaccineerd zijn en het percentage werknemers van wie de vaccinatiestatus bekend is. Voor zover een werkgever beschikt over vestigingseenheden met minstens vijftig werknemers van wie de vaccinatiestatus bekend is, zou diezelfde informatie ook op dat niveau ter beschikking worden gesteld (de vestigingseenheden met minder dan vijftig werknemers van wie de vaccinatiestatus bekend is, zouden daarbij weliswaar ook worden vermeld, maar enkel met de aanduiding dat er geen informatie over kan worden verschaft).
4. De COVID-19-vaccinatiestatistieken zouden per week worden berekend. Daartoe zouden de volgende stappen worden gezet: het selecteren van de werkgevers met minstens vijftig werknemers en de vestigingseenheden met minstens vijftig werknemers (in het werkgeversrepertorium), het achterhalen van het identificatienummer van de sociale zekerheid van elke werknemer van die geselecteerde werkgevers en vestigingseenheden (in de DMFA-databank), het raadplegen van de vaccinatiestatus van elke betrokken werknemer (in de vaccinatiedatabank), het uitvoeren van berekeningen (met eerbiediging van de gepaste maatregelen inzake de *small cells*) en het opslaan van de resultaten in de databank “contactgegevens van collectiviteiten” van het eHealth-platform.

5. De graad van vaccinatie tegen het COVID-19-virus zou worden aangeboden aan de hand van de webtoepassing “*Corona Test Prescription and Consultation*”. De informatie, op het niveau van de werkgevers en eventueel de vestigingseenheden, zou enkel toegankelijk zijn voor artsen die geauthenticeerd zijn door het eHealth-platform. Er zou daarbij gebruik worden gemaakt van de IAM-basisdienst (“*identity and access management*”) van diezelfde organisatie. De toegang zou in elk geval per arts beperkt worden tot de informatie van de werkgevers die een geregistreerde relatie hebben met de dienst voor preventie en bescherming op het werk waarvoor die arts werkt.
6. Er zouden enkel inlichtingen van werkgevers met minstens vijftig werknemers en inlichtingen van vestigingseenheden met minstens vijftig werknemers worden verwerkt. Indien een bepaalde graad (zie hoger, randnummer 3) kleiner of gelijk is aan 20% (5% voor het percentage niet-gevaccineerden) of groter of gelijk is aan 95% (80% voor het percentage niet-gevaccineerden) zou enkel de loutere vermelding daarvan worden opgenomen maar niet de exacte graad. Ten slotte geldt de toegang per werkgever enkel voor de bevoegde dienst voor preventie en bescherming op het werk.
7. De analyse van de vaccinatiegraad van de personeelsleden van een bepaalde werkgever (en desgevallend van diens vestigingseenheden) kunnen de bevoegde dienst voor preventie en bescherming op het werk in staat stellen om een inzicht te krijgen in hun houding ten aanzien van de vaccinatie en om eventuele lacunes in het vaccinatieprogramma op te sporen.
8. Aldus zou elke dienst voor preventie en bescherming op het werk per werkgever met minstens vijftig werknemers aan wie hij diensten verleent, geïdentificeerd met zijn ondernemingsnummer (desgevallend aangevuld met andere informatie ter identificatie, zoals de benaming en het adres), kunnen beschikken over het percentage niet-gevaccineerde werknemers, het percentage gedeeltelijk gevaccineerde werknemers, het percentage volledig gevaccineerde werknemers en het percentage werknemers van wie de vaccinatiestatus bekend is (onder voorbehoud van hetgeen vermeld is onder randnummer 6). Dezelfde inlichtingen zouden eveneens worden verstrekt per vestigingseenheid met minstens vijftig werknemers¹. Er zouden géén verdere onderverdelingen (in functie van andere criteria zoals leeftijd, geslacht en woonplaats van de werknemers) worden toegepast. Het eindresultaat behelst, wat de werknemers betreft, onverkort anonieme gegevens, dat wil zeggen gegevens die op geen enkele wijze kunnen worden herleid tot de natuurlijke personen op wie zij betrekking hebben. De betrokken werkgevers zullen – gelet op het feit dat ze minstens vijftig werknemers in dienst moeten hebben – voornamelijk rechtspersonen zijn (en bijgevolg als dusdanig zelf niet onder de geldende regelgeving met betrekking tot de bescherming van de persoonlijke levenssfeer vallen).

¹ Voorbeeld 1. Werkgever X heeft 400 werknemers, 200 in vestigingseenheid A, 160 in vestigingseenheid B en 40 in vestigingseenheid C. De vaccinatiegraad zou worden meegedeeld aangaande werkgever X en aangaande de vestigingseenheden A en B. Vestigingseenheid C zou enkel voor de volledigheid worden vermeld maar zonder bijkomende informatie.

Voorbeeld 2. Werkgever Y heeft 120 werknemers, 45 in vestigingseenheid D, 45 in vestigingseenheid E en 30 in vestigingseenheid F. De vaccinatiegraad zou enkel worden meegedeeld aangaande werkgever Y. De vestigingseenheden D, E en F zouden enkel voor de volledigheid worden vermeld maar zonder bijkomende informatie.

II. BEVOEGDHEID

9. De mededeling van de persoonsgegevens van de Rijksdienst voor Sociale Zekerheid aan het eHealth-platform, voor verdere verwerking, vergt een voorafgaande beraadslaging van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité, overeenkomstig artikel 15 van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*.
10. De mededeling van persoonsgegevens van Vaccinnet+ aan het eHealth-platform, voor verdere verwerking, vergt een voorafgaande beraadslaging van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité, overeenkomstig artikel 42, § 2, 3°, van de wet van 13 december 2006 *houdende diverse bepalingen betreffende gezondheid*.
11. Overeenkomstig artikel 5, 8°, van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen* is voor de tussenkomst van het eHealth-platform als intermediaire organisatie voor het koppelen en pseudonimiseren of anonimiseren van persoonsgegevens een beraadslaging van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité vereist.
12. Overeenkomstig artikel 5 van het samenwerkingsakkoord van 12 maart 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waals Gewest en de Franse Gemeenschapscommissie *betreffende de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19* mogen de in artikel 3 bedoelde gegevens uitsluitend voor de realisatie van de in artikel 4 opgesomde doeleinden en na beraadslaging van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité worden meegedeeld aan organisaties met een opdracht van algemeen belang voor de doeleinden waarmee ze door of krachtens een wet, decreet of ordonnantie zijn belast.
13. De kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité oordeelt bijgevolg dat zij bevoegd is om zich over de beschreven verwerking van persoonsgegevens uit te spreken.

III. TOELAATBAARHEID

14. De verwerking van persoonsgegevens is enkel rechtmatig indien en voor zover minstens één van de voorwaarden vermeld in 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* vervuld is.
15. De voormelde verwerking van persoonsgegevens is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijken rust, in de zin van artikel 6, 1, eerste lid, c), van de Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad van 27 april 2016.

16. De diverse diensten voor preventie en bescherming op het werk willen in het kader van de uitvoering van hun opdrachten per werkgever aan wie zij diensten verstrekken te weten komen wat de vaccinatiegraad van hun personeel is, met het oog op de aangepaste bescherming van dat personeel en de eventuele beëindiging van bepaalde strikte coronamaatregelen.
17. De arbeidsarts heeft een aantal algemene taken in het kader van het gezondheidstoezicht op werknemers, onder andere om te vermijden dat personen tot het werk worden toegelaten die getroffen zijn door ernstige besmettelijke aandoeningen of die een gevaar voor de veiligheid van andere werknemers inhouden (artikel I.4-2, f), en artikel II.1-5, 2°, van de Codex over het Welzijn op het Werk). Aanvullend hierbij en specifiek met het oog op het efficiënt bestrijden van de coronapandemie in de ondernemingen heeft de arbeidsarts de taak om hoogrisicocontacten in de onderneming op te sporen, rekening houdend met de richtlijnen van de bevoegde overheid, van zodra hij kennis krijgt van een COVID-19-positieve werknemer of van zodra hij over aanwijzingen beschikt dat er een risico op een uitbraak bestaat in de onderneming (artikel 3, 1°, van het koninklijk besluit van 5 januari 2021 *betreffende de rol van de preventieadviseur-arbeidsarts in het kader van het bestrijden van de coronapandemie in de ondernemingen*) en om quarantaineattesten te verstrekken (artikel 3, 2°, van hetzelfde koninklijk besluit van 5 januari 2021). Sciensano bepaalt als bevoegde overheid wie hoogrisicocontacten zijn en in welke gevallen quarantaine vereist is. De huidige regels inzake quarantaine zijn verschillend naargelang een persoon gevaccineerd is of niet (<https://covid-19.sciensano.be/nl/procedures/quarantaine>), zodat de arbeidsarts toegang moet hebben tot de vaccinatiestatus van de werknemers om desgevallend het quarantaineattest uit te schrijven. Kennis over een vaccinatiestatus is ook belangrijk om te weten of er in de onderneming al dan niet een cluster met doorbraakinfectie werd vastgesteld. Daarnaast dienen er voor gevaccineerde laagrisicocontacten geen extra maatregelen te worden genomen.
18. Het gezondheidsdossier van de werknemer moet bovendien alle relevante informatie bevatten over de werknemer om de arbeidsarts in staat te stellen het gezondheidstoezicht uit te voeren (en bijvoorbeeld na te gaan of een werknemer bepaalde inentingen heeft gehad ofwel deze inenting alsnog te geven als dat vereist is) maar ook om de doeltreffendheid te meten van de preventie- en beschermingsmaatregelen die in de onderneming zowel op individueel als op collectief niveau worden toegepast (artikel I.4-83, § 1, van de Codex over het Welzijn op het Werk). In de huidige context van COVID-19 omvatten deze preventie- en beschermingsmaatregelen in elk geval ook de passende preventiemaatregelen die in het kader van het ministerieel besluit van 28 oktober 2020 *houdende dringende maatregelen om de verspreiding van het coronavirus COVID-19 te beperken* en de Generieke Gids Veilig aan het Werk (artikel 2, § 2, van het ministerieel besluit) worden bepaald. Daartoe bevat het gezondheidsdossier een aantal objectieve medische persoonsgegevens (artikel I.4-85, § 1, b), van de Codex over het Welzijn op het Werk), zoals onder meer de datum en de aard van de inentingen en de hernieuwde inentingen (artikel I.4-86, 8°, van de Codex over het Welzijn op het Werk).
19. Wat bepaalde werknemers betreft die blootgesteld zijn aan een biologisch agens tijdens het werk (zoals werknemers in de zorgsector, met betrekking tot COVID-19) en voor wie een doeltreffend vaccin beschikbaar is, moet de werkgever die werknemers de mogelijkheid bieden om zich te laten inenten (artikel VII.1-51 van de Codex over het Welzijn op het Werk). Deze inentingen kunnen dan door de arbeidsarts worden verricht

maar hij moet daarvoor uiteraard kunnen nagaan dat zij de nodige inentingën nog niet hebben gekregen, om het gezondheidstoezicht uit te voeren (artikel VII.1-59 van de Codex over het Welzijn op het Werk).

20. De verwerking van persoonsgegevens die de gezondheid betreffen is in principe verboden. Het verbod is echter overeenkomstig artikel 9, 2, i), van de Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad van 27 april 2016 niet van toepassing (onder andere) wanneer de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim. Bij de hogerbeschreven verwerking van persoonsgegevens is dat effectief het geval. De doelstelling ervan komt overeen met het verwerkingsdoeleinde bepaald in artikel 4, § 2, punt 6°, van het samenwerkingsakkoord van 12 maart 2021, namelijk het bepalen van de anonieme vaccinatiegraad tegen COVID-19 van de bevolking.
21. Het informatieveiligheidscomité is bijgevolg van oordeel dat er een grondslag bestaat voor de beoogde verwerking van persoonsgegevens die de gezondheid betreffen.

III. PRINCIPES INZAKE DE VERWERKING VAN PERSOONSgegevens

Algemeen

22. Volgens artikel 5 van de Verordening (EU) 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* moeten persoonsgegevens worden verzameld voor bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen ze vervolgens niet verder worden verwerkt op een wijze die met die doeleinden onverenigbaar is (beginsel van de doelbinding), moeten ze toereikend en ter zake dienend zijn en beperkt worden tot wat noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt (beginsel van de minimale gegevensverwerking), moeten ze worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de geldende doeleinden noodzakelijk is (beginsel van de opslagbeperking) en moeten ze zodanig worden verwerkt, met passende technische of organisatorische maatregelen, dat een passende beveiliging gewaarborgd is en dat ze onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (beginsel van de integriteit en de vertrouwelijkheid).

Doelbinding

23. De mededeling van persoonsgegevens door de Rijksdienst voor Sociale Zekerheid en Vaccinnet+ aan het eHealth-platform beoogt een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde, namelijk het bepalen van de graad van vaccinatie tegen het COVID-19-virus van de werknemers, per Belgische werkgever met minstens vijftig

werknemers en per vestigingseenheid met minstens vijftig werknemers, ten behoeve van de bevoegde diensten voor preventie en bescherming op het werk.

24. Met de anonieme vaccinatiegraad per werkgever waarvoor zij bevoegd zijn, kunnen de diensten voor preventie en bescherming op het werk specifieke (aan de situatie van de werkgever aangepaste) maatregelen treffen. Afhankelijk van de resultaten kunnen zij bijvoorbeeld de werknemers sensibiliseren om zich alsnog te laten vaccineren tegen het coronavirus of bepaalde eerder getroffen strenge maatregelen laten stopzetten of versoepelen.
25. De verwerking kadert voorts in de toepassing van de regelgeving vermeld in de randnummers 17, 18 en 19.
26. Volgens artikel 5, 1, b), van de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 wordt de verdere verwerking voor wetenschappelijke onderzoeken of statistische doeleinden, overeenkomstig artikel 89, eerste lid, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd. Het gebruik van DMFA-persoonsgegevens en vaccinatiepersoonsgegevens vormt bijgevolg een toegelaten en verenigbaar gebruik.

Minimale gegevensverwerking

27. De diensten voor preventie en bescherming op het werk ontvangen van het eHealth-platform enkel geaggregeerde informatie ten aanzien van de werknemers, met name het percentage werknemers die niet gevaccineerd zijn, het percentage werknemers die gedeeltelijk gevaccineerd zijn, het percentage werknemers die volledig gevaccineerd zijn en het percentage werknemers van wie de vaccinatiestatus bekend is.
28. Indien een hogervermeld type percentage kleiner of gelijk is aan 20% (5% voor het percentage niet-gevaccineerden) of groter of gelijk is aan 95% (80% voor het percentage niet-gevaccineerden) vermeldt het eHealth-platform enkel die vaststelling, zonder verdere details (dus zonder het exacte percentage), om aldus elke heridentificatie van de betrokkenen te vermijden.
29. Voorts wordt enkel informatie van werkgevers met minstens vijftig werknemers (en eventueel van hun respectieve vestigingseenheden met minstens vijftig werknemers) verwerkt. Bij werkgevers met een relatief klein aantal werknemers stelt zich immers een reëel risico op heridentificatie van de werknemers.
30. De toegang per werkgever geldt daarenboven enkel voor de bevoegde dienst voor preventie en bescherming op het werk, dat wil zeggen de organisatie die uitdrukkelijk werd aangesteld om voor die werkgever taken inzake preventie en bescherming uit te voeren. Het is aldus cruciaal dat op elk ogenblik precies en juist geweten is *welke dienst* bevoegd is voor *welke werkgever*. Die informatie moet ter beschikking gesteld worden door de voormelde overkoepelende organisaties (CO-PREV, VVIB en EMPREVA). Die organisaties zijn onverkort verantwoordelijk om de informatie dienaangaande volledig, juist en actueel ter beschikking te stellen en te houden.
31. De voormelde bevoegde overkoepelende organisaties van de diensten voor preventie en bescherming op het werk zijn er aldus voor verantwoordelijk:

- om vooraf na te gaan of de informatie inzake de bevoegdheid van een dienst voor preventie en bescherming op het werk ten aanzien van een werkgever wel degelijk correct is en alle fouten vóór de verzending door het eHealth-platform te verbeteren, zodanig dat het bestand nauwkeurig is en geen onjuiste dubbele aansluitingen bevat;
- om bij de periodieke mededeling van informatie over de bevoegdheid van een dienst voor preventie en bescherming op het werk ten aanzien van een werkgever steeds ook de nieuwe aansluitingen bij een dienst voor preventie en bescherming op het werk sinds de vorige periode ter beschikking te stellen;
- om te waarborgen dat de overgang van een bepaalde werkgever van de ene dienst naar de andere dienst onmiddellijk ingaat en dat daarover ook tijdig, dat wil zeggen minstens één week vooraf, juiste informatie wordt verstrekt aan de organisaties die deze informatie nodig hebben voor het vervullen van hun opdrachten.

32. De voormelde informatie over de vaccinatiegraad van de werknemers kan maar ter beschikking worden gesteld voor zover de bevoegde koepelorganisaties (CO-PREV, VVIB en EMPREVA) elk uitdrukkelijk hebben verklaard akkoord te gaan met de inhoud van deze beraadslaging, door middel van een tegentekening ervan.

Opslagbeperking

33. Het eHealth-platform vernietigt de lijsten met identificatienummers van de sociale zekerheid van de betrokken werknemers, aangevuld met de hogervermelde informatie van de Rijksdienst voor Sociale Zekerheid en Vaccinnet+, onverwijld na de verwerking ervan tot loutere anonieme gegevens. Voor zover het eHealth-platform er later alsnog opnieuw nood aan heeft, voor een bijkomende gerechtvaardigde verwerking, richt het zich – mits voorafgaande beraadslaging van het informatieveiligheidscomité – tot de vermelde authentieke bronnen.

Integriteit en vertrouwelijkheid

34. Bij de verwerking van de persoonsgegevens worden alle gepaste technische en organisatorische maatregelen getroffen die nodig zijn voor de bescherming van de persoonsgegevens. Deze maatregelen verzekeren een passend beveiligingsniveau, 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.

35. Om de vertrouwelijkheid en de veiligheid van de persoonsgegevensverwerking te garanderen, neemt elke organisatie die persoonsgegevens bewaart, verwerkt of meedeelt maatregelen in de volgende actiedomeinen met betrekking tot de informatieveiligheid: het veiligheidsbeleid, de aanstelling van een functionaris voor gegevensbescherming, de organisatorische en persoonlijke aspecten (vertrouwelijkheidsverbintenis, regelmatige informatieverstrekking en opleidingen aangaande de bescherming van de persoonlijke levenssfeer en de veiligheidsregels), de fysieke veiligheid, de omgevingsveiligheid, de netwerkbeveiliging, de toegangsbeveiliging, de loggings, opsporing en analyse van de toegangen, het toezicht, nazicht en onderhoud, het systeem van beheer van de veiligheidsincidenten, de continuïteit en de documentatie.

36. Het informatieveiligheidscomité wijst expliciet op de bepalingen van titel 6 (sancties) van de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*, waarbij voorzien wordt in administratieve sancties en strafsancties in hoofde van de verwerkingsverantwoordelijken en de verwerkers in geval van overtreding van de voorwaarden die bepaald zijn in de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 en in de voormelde wet van 30 juli 2018.
37. Het informatieveiligheidscomité benadrukt vervolgens dat persoonsgegevens betreffende de gezondheid enkel mogen worden verwerkt onder het toezicht en de verantwoordelijkheid van een beroepsbeoefenaar in de gezondheidszorg en dat die, samen met zijn aangestelden of gemachtigden, bij de verwerking van persoonsgegevens tot geheimhouding verplicht is.
38. Vóór de mededeling van de output aan de respectieve diensten voor preventie en bescherming op het werk neemt het eHealth-platform de gepaste maatregelen om het anonieme karakter ervan in alle omstandigheden te waarborgen. Het voert vooraf een *small cell* risicoanalyse uit. Indien blijkt dat de COVID-19-vaccinatiegraad van het personeel van een bepaalde werkgever of vestigingseenheid een hoog risico op heridentificatie van de betrokken werknemers met zich brengt, wordt die niet als dusdanig ter beschikking gesteld maar worden geschikte acties ondernomen.
39. Overeenkomstig artikel 12 van de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 moet de verwerkingsverantwoordelijke passende maatregelen nemen opdat de betrokkene informatie over de verwerking van zijn persoonsgegevens in een beknopte, transparante, begrijpelijke en makkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zou ontvangen. De eindbestemmingen (de diverse diensten voor preventie en bescherming op het werk) kennen de identiteit van de betrokken werknemers niet vermits er slechts anonieme gegevens worden meegedeeld. Het medelen van informatie aan de betrokkenen is bijgevolg niet mogelijk. Het informatieveiligheidscomité oordeelt bijgevolg dat de aanvraag aan de eisen van transparantie voldoet.
40. De partijen houden bij de verwerking van de persoonsgegevens rekening met de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid* en elke andere regelgeving tot bescherming van de persoonlijke levenssfeer, in het bijzonder de Verordening (EU) 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* en de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*.

Om deze redenen, besluit

de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité

dat de mededeling van persoonsgegevens door de Rijksdienst voor Sociale Zekerheid en Vaccinnet+ aan het eHealth-platform, voor het bepalen van de graad van vaccinatie tegen het COVID-19-virus van de werknemers, per Belgische werkgever en vestigingseenheid met minstens vijftig werknemers, ten behoeve van de bevoegde diensten voor preventie en bescherming op het werk, zoals beschreven in deze beraadslaging, is toegestaan 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.

Michel DENEYER
Waarnemend 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.