Inhoud

Let op: De nummering van de bijlages wijkt af van het totale aantal pagina's door het invoegen van externe documenten

Verwerkersovereenkomst ARVODI-2018

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag, te dezen vertegenwoordigd door de Minister van Volksgezondheid, Welzijn en Sport, namens deze, de Directeur-generaal van het **Rijksinstituut voor Volksgezondheid en Milieu (RIVM)**, de heer Prof. dr. ir. 5.1.2e namens deze, mevrouw Prof. Dr. 5.1.2e 5.1.2e, Hoofd van het Centrum Landelijke Coördinatie Infectieziektebestrijding (LCI) van het RIVM, gevestigd aan de Antonie van Leeuwenhoeklaan 9 te (3721 MA) Bilthoven
hierna te noemen: Opdrachtgever,

en

2. I&O Research bv gevestigd te Enschede, KVK-nummer 5.1.2e te dezen vertegenwoordigd de heer G. 5.1.2e directeur.
hierna te noemen: Opdrachtnemer,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- voor zover Opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen
In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in artikel 1 van de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van Diensten 2018 (ARVODI-2018). In afwijking daarvan of in aanvulling daarop wordt onder de volgende begrippen in deze Verwerkersovereenkomst verstaan:

1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.2 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

1.3 Overeenkomst: de overeenkomst tussen Opdrachtgever en Opdrachtnemer met betrekking tot het uitvoeren van een vragenlijstonderzoek naar de coronavaccinatie. (De offerte 'Dataverzameling vragenlijst coronavaccinatie' van Opdrachtnemer getekend door Opdrachtgever op 10 maart 2021, Bijlage 4).

1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

1.5 Verordening: 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 de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.7 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Opdrachtnemer in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven.

2.3 Opdrachtnemer garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Opdrachtnemer garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat en voor zover Opdrachtnemer alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Opdrachtnemer van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Opdrachtnemer in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Opdrachtnemer op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking

5.1 In aanvulling op artikel 15 van de ARVODI-2018 en onverminderd artikel 2.3 treft Opdrachtnemer de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.

5.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid.

5.6 Opdrachtnemer verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 6. Geheimhouding door Personeel van Opdrachtnemer

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 13.1 van de ARVODI-2018.

6.2 Opdrachtnemer toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 13.2 van de ARVODI-2018.

Artikel 7. Subverwerker

Wanneer Opdrachtnemer, met inachtneming van het bepaalde in artikel 8 van de ARVODI-2018, een andere verwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene

Opdrachtnemer verleent Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Opdrachtnemer informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Overeenkomst draagt Opdrachtnemer, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Opdrachtnemer verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.

10.2 Opdrachtnemer wist de ruwe onderzoekdata binnen 24 maanden na afloop van de Overeenkomst. Steekproefgegevens worden gewist na afronding van het project.

10.3 Persoonsgegevens worden in de door Opdrachtgever aangegeven vorm en op de door Opdrachtgever aangegeven wijze terugbezorgd.

Artikel 11. Informatieverplichting

Opdrachtnemer stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Bilthoven, [datum] Enschede, [datum]

De minister van Volksgezondheid, Welzijn en Sport, namens deze, de Directeur-generaal, de heer Prof. dr. ir. J. 5.1.2e van het Rijksinstituut voor Volksgezondheid en Milieu, namens deze mevrouw Prof. Dr. 5.1.2e 5.1.2e.

[Handtekening 5.1.2e]

De heer drs. 5.1.2e 5.1.2e
[Handtekening 5.1.2e]

Bijlage 1. De Verwerking van Persoonsgegevens

Opdrachtnemer zet een vragenlijst van Opdrachtgever uit bij ~3000 van haar panelleden. Deze vragenlijst test de Opdrachtnemer ook in een interview met 10 panelleden. Na de dataverzameling levert Opdrachtnemer een databestand met de data op basis van de vragenlijst en met bij Opdrachtnemer bekende achtergrondgegevens (bijv. leeftijd, opleidingsniveau in categorieën en migratieachtergrond in categorieën) van de panelleden die deelnamen aan de vragenlijst. Het vragenlijstonderzoek heeft als doel inzicht te krijgen in publieke percepties van corona en de coronavaccinatie, corona vaccinatiekeuzes, en vertrouwen in de medemens en instanties. Voor dit onderzoek worden ook enkele (bijzondere) persoonsgegevens uitgevraagd. Deze gegevens worden door Opdrachtgever gebruikt om verschillen te onderzoeken tussen personen in (o.a.) corona vaccinatiekeuzes. De verwerking in deze overeenkomst heeft betrekking op de in de vragenlijst uitgevraagde persoonsgegevens, welke in deze bijlage zijn gespecificeerd aan de hand van de betreffende vragenlijstvragen.

De betreffende vragenlijstvragen die resulteren in (bijzondere) persoonsgegevens:

- Bent u al gevaccineerd tegen het coronavirus? *(Vraag 5 in vragenlijst, versie 25-02-2021)*
  - O Nee
  - O Ja, ik heb één prik gehad tegen het coronavirus
  - O Ja, ik heb twee prikken gehad tegen het coronavirus
- Er volgt een aantal uitspraken over de keuze van vaccineren tegen het coronavirus. Geef voor elke uitspraak aan in hoeverre deze bij u past. *(Vraag 20e in vragenlijst, versie 25-02-2021)*

  Bij de keuze van vaccinatie tegen het coronavirus ...

  Speelt mijn geloof of levensovertuiging een belangrijke rol

  Helemaal niet O O O O O *Helemaal wel*
- Zijn uw kinderen gevaccineerd volgens het Rijksvaccinatieprogramma? *(Vraag 28 in vragenlijst, versie 25-02-2021)*
  - O Ja, mijn kind/kinderen hebben alle vaccinaties gehad die werden aangeraden voor zijn/haar leeftijd
  - O Ja gedeeltelijk, mijn kind/kinderen hebben niet alle vaccinaties gehad die werden aangeraden voor zijn/haar leeftijd)
  - O Nee, mijn kinderen zijn niet gevaccineerd volgens het Rijksvaccinatieprogramma
- Bent u op dit moment zwanger? *(Vraag 30 in vragenlijst, versie 25-02-2021)*
  - O Ja
  - O Nee
  - O Weet ik niet
  - O Zeg ik liever niet
- Bent u besmet geweest met het coronavirus? *(Vraag 31 in vragenlijst, versie 25-02-2021)*
  - O Nee, waarschijnlijk niet

O Ja, waarschijnlijk wel

O Ja, zeker wel (ik ben positief getest met het coronavirus)

O Weet ik niet

- Hoe is over het algemeen uw gezondheid? *(Vraag 32 in vragenlijst, versie 25-02-2021)*

O Zeer goed

O Goed

O Gaat wel

O Slecht

O Zeer slecht

- Heeft u één of meer van de volgende gezondheidsproblemen? *(Vraag 33 in vragenlijst, versie 25-02-2021)*

- chronische luchtweg- of longproblemen
- chronische hartaandoeningen
- suikerziekte (diabetes mellitus)
- ernstige nieraandoeningen die leiden tot dialyse of niertransplantatie
- een Hiv-infectie
- een ernstige leverziekte
- zeer ernstig overgewicht (BMI van boven de 40)
- lagere weerstand tegen infecties:
    - door medicijnen voor auto-immuunziekten
    - na orgaan- of stamceltransplantatie
    - door een niet-functionerende of ontbrekende milt
    - door bloedziekten
    - door ernstige afweerstoornissen waarvoor behandeling nodig is
    - door chemotherapie en/of bestraling bij kanker
    - door medicijnen die uw weerstand verlagen

O Nee

O Ja

- Bent u allergisch voor vaccinaties? *(Vraag 34 in vragenlijst, versie 25-02-2021)*

O Nee, zeker niet

O Nee, waarschijnlijk niet

O Weet ik niet

O Ja, waarschijnlijk wel

O Ja, zeker wel

- Werkt u in de gezondheidszorg? *(Vraag 35 in vragenlijst, versie 25-02-2021)*

O Nee, ik werk niet in de gezondheidszorg

O Ja, ik werk in de gezondheidszorg als verzorgende

O Ja, ik werk in de gezondheidszorg als verpleegkundige

O Ja, ik werk in de gezondheidszorg ik werk als arts

O Ja, ik werk in de gezondheidszorg in een ander beroep dan hierboven genoemd

Bijlage 2. Passende technische en organisatorische maatregelen

De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk: ISO 27001. De toereikendheid van de informatiebeveiliging blijkt uit certificering en de verklaring van toepasselijkheid.

1233919

Lloyd's Register

Huidige uitgiftedatum:	31 mei 2020	Originele uitgiftedatum:
Vervaldatum:	30 mei 2023	ISO/IEC 27001 - 31 mei 2017
Certificaatnummer:	10269953	

Certificaat

Hiermede wordt verklaard dat het managementsysteem van:

I & O Research B.V.

Zuiderval 70, 7543 EZ Enschede, Nederland

door Lloyd's Register is goedgekeurd voor de volgende norm(en):

ISO/IEC 27001:2013
BS EN ISO/IEC 27001: 2017

Goedkeuringsnummer: ISO/IEC 27001 – 0025778

Dit certificaat is alleen geldig in samenhang met het certificaataanhangsel met hetzelfde nummer, waarop de van toepassing zijnde locaties met betrekking tot deze goedkeuring vermeld zijn.

Dit certificaat is geldig voor de volgende scope:
Het uitvoeren van dataverzameling, beleidsonderzoek en het geven van advies en het detacheren van onderzoekers en dataspecialisten voor overheid en de publieke sector volgens de verklaring van toepasselijkheid versie 1.6 van 8 mei 2020.

5.1.2e

5.1.2e

Area 5.1.2e 5.1.2e North Europe

Afgegeven door: Lloyd's Register Nederland B.V.

voor en namens: Lloyd's Register Quality Assurance Limited

UKAS MANAGEMENT SYSTEMS
001

Lloyd's Register

Certificaatnummer: 10269953

Certificaataanhangsel

Locatie	Activiteiten
I & O Research B.V. Zuiderval 70, 7543 EZ Enschede, Nederland	**ISO/IEC 27001:2013** Het uitvoeren van dataverzameling, beleidsonderzoek en het geven van advies en het detacheren van onderzoekers en dataspecialisten voor overheid en de publieke sector volgens de verklaring van toepasselijkheid versie 1.6 van 8 mei 2020.
I & O Research B.V. Piet Heinkade 55, 1019 GM Amsterdam, Nederland	**ISO/IEC 27001:2013** Het uitvoeren van dataverzameling, beleidsonderzoek en het geven van advies en het detacheren van onderzoekers en dataspecialisten voor overheid en de publieke sector volgens de verklaring van toepasselijkheid versie 1.6 van 8 mei 2020.

UKAS MANAGEMENT SYSTEMS
001

Verklaring van toepasselijkheid ISO27001:2013 en ISO27001:2017

Versie: 1.6
Datum: 8 mei 2020

I&O Research, Amsterdam en Enschede

Scope ISO27001:2013 en ISO 27001:2017 certificaat
Nederlands:
Engels:

				STATUS			TRIGGER			
Nummer	Niet van toepassing	Van toepassing	Beheersmaatregel	Nog niet ingevoerd	Volledig ingevoerd	Verantwoordelijke	Beleid	Wet- en regelgeving	Contractuele eis	Risico-analyse
IB Beleid										
A.5.1.1		√	Het IB beleid moet worden gedefinieerd, door het management goedgekeurd, gepubliceerd en gecommuniceerd naar alle betrokken partijen.		x	Algemeen directeur	x			x
A.5.1.2		√	Het IB beleid moet periodiek worden beoordeeld of in geval van significante wijzigingen om zeker te stellen dat het geschikt, adequaat en effectief is.		x	Algemeen directeur	x			x
IB Organisatie										
A.6.1.1		√	IB verantwoordelijkheden moeten worden gedefinieerd en toegewezen.		x	Algemeen directeur	x			x
A.6.1.2		√	Conflicterende rechten en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld misbruik van bedrijfsmiddelen te beperken.		x	Hoofd ICT	x			x

A.6.1.3		√	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.		x	Algemeen directeur	x			x
A.6.1.4		√	Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.		x	Security Officer	x			x
A.6.1.5		√	IB moet aan de orde komen in projectbeheer, ongeacht het soort project.		x	Hoofd ICT	x	x		x
A.6.2.1		√	Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.		x	Hoofd ICT	x	x		x
A.6.2.2		√	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.		x	Hoofd ICT	x	x		x
HRM										
A.7.1.1		√	Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.		x	HR-adviseur	x			x
A.7.1.2		√	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor IB en die van de organisatie vermelden		x	HR-adviseur	x			x

A.7.2.1		√	De directie moet van alle medewerkers en contractanten eisen dat ze IB toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.		x	Algemeen directeur	x			x
A.7.2.2		√	Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijnsopleiding en -training krijgen en regelmatig bijscholing van beleidsregels en procedures van de organisatie voor zover relevant voor hun functie.		x	HR-adviseur	x			x
A.7.2.3		√	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de IB.		x	HR-adviseur	x			x
A.7.3.1		√	Verantwoordelijkheden en taken met betrekking tot IB die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht.	x		HR-adviseur	x			x
Middelen										
A.8.1.1		√	Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.		x	Hoofd ICT	x			x
A.8.1.2		√	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.		x	Hoofd ICT	x			x
A.8.1.3		√	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.		x	Hoofd ICT	x			x
A.8.1.4		√	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die zij in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.		x	HR-adviseur	x			x

A.8.2.1		√	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.		x	Algemeen directeur	x	x		x
A.8.2.2		√	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.		x	Algemeen directeur	x			x
A.8.2.3		√	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.		x	Hoofd ICT	x			x
A.8.3.1		√	Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met de classificatie die door de organisatie is vastgesteld.		x	Hoofd ICT	x			x
A.8.3.2		√	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.		x	Hoofd ICT	x			x
A.8.3.3		√	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.		x	Hoofd ICT	x			x
Toegang										
A.9.1.1		√	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en IB eisen.		x	Algemeen directeur	x			x
A.9.1.2		√	Gebruikers mogen alleen toegang hebben tot het netwerk en de netwerkdiensten waartoe zij specifiek bevoegd zijn.		x	Algemeen directeur	x			x
A.9.2.1		√	Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.		x	HR-adviseur	x			x

A.9.2.2		√	Een formele gebruikerstoegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.		x	Algemeen directeur	x			x
A.9.2.3		√	Het toewijzen en gebruik van bevoorrechte toegangsrechten moet worden beperkt en gecontroleerd.		x	Algemeen directeur	x			x
A.9.2.4		√	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.		x	Hoofd ICT	x			x
A.9.2.5		√	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.		x	Hoofd ICT	x			x
A.9.2.6		√	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.		x	Hoofd ICT	x			x
A.9.3.1		√	Gebruikers moeten de regels naleven aangaande het gebruik van geheime authenticatie informatie.		x	Algemeen directeur	x			x
A.9.4.1		√	Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.		x	Hoofd ICT	x			x
A.9.4.2		√	Indien het beleid van toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.		x	Hoofd ICT	x			x
A.9.4.3		√	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.		x	Hoofd ICT	x			x

A.9.4.4		√	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moeten worden beperkt en nauwkeurig worden gecontroleerd.		x	Hoofd ICT	x			x
A.9.4.5		√	Toegang tot programmabroncode moet worden beperkt.		x	Hoofd ICT	x			x
Cryptografie										
A.10.1.1		√	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.		x	Hoofd ICT	x	x		x
A.10.1.2		√	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.		x	Hoofd ICT	x			x
Fysiek										
A.11.1.1		√	Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.		x	Algemeen directeur	x			x
A.11.1.2		√	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.		x	Algemeen directeur	x			x
A.11.1.3		√	Voor kantoren, ruimten en faciliteit moet fysieke beveiliging worden ontworpen en toegepast.		x	Algemeen directeur	x			x
A.11.1.4		√	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.		x	Security Officer	x	x		x

A.11.1.5		√	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.		x	Algemeen directeur	x			x
A.11.1.6		√	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.		x	Algemeen directeur	x			x
A.11.2.1		√	Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.		x	Algemeen directeur	x			x
A.11.2.2		√	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.		x	Hoofd ICT	x			x
A.11.2.3		√	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.		x	Hoofd ICT	x			x
A.11.2.4		√	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.		x	Hoofd ICT	x			x
A.11.2.5		√	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.		x	Algemeen directeur	x			x
A.11.2.6		√	Bedrijfsmiddelen die zich buiten het werkterrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.		x	Algemeen directeur	x			x

A.11.2.7		√	Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven.		x	Hoofd ICT	x			x
A.11.2.8		√	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.		x	Algemeen directeur	x			x
A.11.2.9		√	Er moet een clean desk beleid voor papieren documenten en verwijderbare opslagmedia en een clean screen beleid voor informatieverwerkende faciliteiten worden ingesteld.		x	Security Officer	x			x
Operations											
A.12.1.1		√	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.		x	Hoofd ICT	x			x
A.12.1.2		√	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de IB moeten worden beheerst.		x	Security Officer	x			x
A.12.1.3		√	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.		x	Hoofd ICT	x			x
A.12.1.4		√	Ontwikkel, test en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.		x	Hoofd ICT	x			x
A.12.2.1		√	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.		x	Hoofd ICT	x			x
A.12.3.1		√	Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.		x	Hoofd ICT	x			x

A.12.4.1		√	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en IB gebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.		x	Hoofd ICT	x			x
A.12.4.2		√	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.		x	Hoofd ICT	x			x
A.12.4.3		√	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.		x	Hoofd ICT	x			x
A.12.4.4		√	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met een referentiebron.		x	Hoofd ICT	x			x
A.12.5.1		√	Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.		x	Hoofd ICT	x			x
A.12.6.1		√	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.		x	Security Officer	x			x
A.12.6.2		√	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.		x	Hoofd ICT	x			x
A.12.7.1		√	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.		x	Security Officer	x			x
Communicatie											
A.13.1.1		√	Netwerken moeten worden beheerd en beheerst om informatie in de systemen en toepassingen te beschermen.		x	Hoofd ICT	x			x

A.13.1.2		√	Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.		x	Hoofd ICT	x			x
A.13.1.3		√	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.		x	Hoofd ICT	x			x
A.13.2.1		√	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.		x	Hoofd ICT	x			x
A.13.2.2		√	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.		x	Security Officer	x			x
A.13.2.3		√	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.		x	Hoofd ICT	x			x
A.13.2.4		√	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.		x	Security Officer	x			x
Systeemontwikkeling en -onderhoud											
A.14.1.1		√	De eisen die verband houden met IB moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.		x	Hoofd ICT	x			x
A.14.1.2		√	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken worden uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.		x	Security Officer	x			x

A.14.1.3		√	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.		x	Hoofd ICT	x			x
A.14.2.1		√	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.		x	Hoofd ICT	x			x
A.14.2.2		√	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.		x	Hoofd ICT	x			x
A.14.2.3		√	Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.		x	Hoofd ICT	x			x
A.14.2.4		√	Wijzigingen aan softwarepakketten moet worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.		x	Hoofd ICT	x			x
A.14.2.5		√	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.		x	Hoofd ICT				x
A.14.2.6		√	Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.		x	Hoofd ICT				x

A.14.2.7		√	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.		x	Hoofd ICT				x
A.14.2.8		√	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.		x	Hoofd ICT				x
A.14.2.9		√	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.		x	Hoofd ICT	x			x
A.14.3.1		√	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.		x	Hoofd ICT	x			x
Leveranciers											
A.15.1.1		√	Met de leverancier moeten de IB eisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.		x	Hoofd ICT	x			x
A.15.1.2		√	Alle relevante IB eisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.		x	Hoofd ICT	x			x
A.15.1.3		√	Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de IB risico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.		x	Security Officer	x			x

A.15.2.1		√	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.		x	Security Officer	x			x
A.15.2.2		√	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor IB, moeten worden beheerd, rekening houdend met kritikaliteit van bedrijfsinformatie, betrokken systeem en processen en herbeoordeling van risico's.		x	Security Officer	x			x
Incidentmanagement											
A.16.1.1		√	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op IB incidenten te bewerkstelligen.		x	Security Officer	x			x
A.16.1.2		√	IB gebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.		x	Security Officer	x			x
A.16.1.3		√	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de IB registreren en rapporteren.		x	Algemeen directeur	x			x
A.16.1.4		√	IB gebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als IB incidenten.		x	Security Officer	x			x
A.16.1.5		√	Op IB incidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.		x	Security Officer	x			x
A.16.1.6		√	Kennis die is verkregen door IB incidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.		x	Security Officer	x			x

A.16.1.7		√	De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.		x	Security Officer	x			x
Continuïteit										
A.17.1.1		√	De organisatie moet haar eisen voor IB en voor de continuïteit van het IB beheer in ongunstige situaties, bv. Een crisis of ramp, vaststellen.		x	Security Officer	x			x
A.17.1.2		√	De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor IB tijdens een ongunstige situatie te waarborgen.		x	Security Officer	x			x
A.17.1.3		√	De organisatie moet ten behoeve van IB continuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.		x	Security Officer	x			x
A.17.2.1		√	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.		x	Hoofd ICT	x			x
Compliance										
A.18.1.1		√	Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.		x	Algemeen directeur	x	x		x
A.18.1.2		√	Om de naleving van wettelijke, regelgevende, contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.		x	Hoofd ICT	x	x		x

A.18.1.3		√	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.		x	Hoofd ICT	x	x		x
A.18.1.4		√	Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.		x	Security Officer	x	x		x
A.18.1.5		√	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.		x	Hoofd ICT	x			x
A.18.2.1		√	De aanpak van de organisatie ten aanzien van het beheer van IB en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor IB) moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld.		x	Security Officer	x			x
A.18.2.2		√	De directie moet regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.		x	Security Officer	x			x
A.18.2.3		√	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor IB.		x	Security Officer	x			x

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

Bij een Datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van Persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een Datalek valt dus niet alleen het vrijkomen (lekken) van Persoonsgegevens, maar ook onrechtmatige verwerking van Persoonsgegevens.

De Opdrachtgever spreekt van een Datalek als er een inbreuk is op de beveiliging van persoonsgegevens. Bij een Datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking, dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging
De Opdrachtgever dient als verwerkingsverantwoordelijke een Datalek te melden bij de Autoriteit Persoonsgegevens. Om aan deze plicht te kunnen voldoen dient de Opdrachtnemer binnen 24 uur, rekenend vanaf het moment dat de Opdrachtnemer een Datalek heeft vastgesteld, dit te melden bij 5.1.2e @rivm.nl en 5.1.2e @rivm.nl, of per telefoon op 030 - 2742747 (telefoon alleen tijdens kantoortijden).

De Opdrachtnemer dient bij een melding expliciet aan te geven dat de melding een Datalek Persoonsgegevens betreft. De opdrachtnemer ontvangt een datalek formulier die digitaal wordt aangeleverd bij 5.1.2e @rivm.nl.

Bijlage 4: Offerte 'Dataverzameling vragenlijst coronavaccinatie' d.d. 10 maart 2021

Pagina's zijn verwijderd 1233919

28 - 54

dubbel

dubbel