# Gemeente Amsterdam - Data Protection Impact Assessment (DPIA)

Gemeente Amsterdam

Cluster: Corona
Directie:
Procesnaam (bedrijfsproces): Corona testen
Datum: 1 april 2022
Proceseigenaar: x
Opdrachtgever: x
Versie: 1.0
Auteur: x
Functie: Privacy Officer

| | Vraag | | Risico scoring | Juridische toelichting |
|---|---|---|---|---|
| | **Deel 1 - Algemeen** | | | |
| **1** | Is dit een nieuw proces, of een nieuwe versie van een bestaand proces? | Nieuw proces. | | |
| **2** | Is er een DPIA gedaan voor eerdere versies van dit proces? | Nee. | | |
| **3** | Is iets veranderd sinds de laatste DPIA is uitgevoerd? | N.v.t. | Indien voor dit proces reeds een DPIA is gedaan en ten opzichte van de laatste DPIA is er niets veranderd | |
| **4** | Beschrijf het proces en de (voorgenomen) verwerkingsactiviteiten en/of het voorgenomen beleid/regelgeving waarvoor deze DPIA wordt uitgevoerd. | Het proces begint bij het maken van een afspraak. Daar zijn 4 mogelijkheden voor.<br><br>**Optie 1**: een burger maakt zelf digitaal een afspraak via coronatest.nl. Hier wordt de burger gevraagd om in te loggen met zijn Digid en vervolgens een aantal vragen te beantwoorden. Vervolgens worden er een aantal mogelijke tijdstippen/data/locaties gegeven waar de burger een test kan laten afnemen. Tijdens dit proces wordt tevens toestemming aan de burger gevraagd voor het delen van de testuitslag met zijn/haar huisarts. Met behulp van het BSN nummer kan de huisarts van de burger worden achterhaald. De afspraak wordt geregistreerd in CoronIT.<br><br>**Optie 2**: de burger maakt telefonisch een afspraak via 0800-1202 of 0800-8101 (PRIO). De burger doorloopt hier een keuzemenu. Er wordt door een automatisch bandje verteld dat om een afspraak te maken persoonsgegevens worden verwerkt. Vervolgens wordt er verwezen naar de site van de GGD GHOR mocht je hier meer vragen over hebben. Nadat je het keuze menu hebt doorlopen krijgt de burger een telefonist aan de lijn die een aantal vragen stelt mbt zijn/haar klachten en naar de burger zijn BSN nummer, op basis van de woonplaats wordt dan de dichtsbijzijnde locatie en het eerste mogelijke tijdstip voorgedragen aan de burger. Afspraken worden gemaakt in Coronit. Het telefoongesprek kan worden opgenomen voor trainingsdoeleinden. Hierover wordt de burger geinformeerd.<br><br>Na het maken van een afspraak ontvangt de burger een sms of e-mail met een afspraakbevestiging. Vervolgens komt de burger op de afgesproken tijd naar de testlocatie. Op de testlocatie wordt de burger allereerst geidentificeerd en moet zijn testafspraak laten zien. Dit wordt door de medewerker gecontroleerd in CoronIT. Vervolgens wordt de test afgenomen en door middel van een barcode, initialen en geboortedatum wordt de test gekoppeld aan de betreffende burger. De burger kan zijn uitslag bekijken door het inloggen bij coronatest.nl met zijn DigID.<br>**Optie 3**: Er wordt een aanvraag ingediend bij de bellijn 105 voor een testafname door een zorginstelling. De aanvraag komt binnen bij secretariaat Corona Rai en wordt uitgezet. De testafname vindt dan ook op locatie plaats. Een medewerker van de GGD gaat naar de instelling met het aanvraagformulier en het afnamemateriaal. De uitslag komt via de arts (SOG) van de zorginstelling binnen. Burgers die bij de landelijke bellijn aangeven niet naar een testlocatie te kunnen komen, worden ook doorverbonden naar de GGD bellijn, middels triage wordt bepaald of we thuisbemonstering doen, dit gaat wel via CoronIT.<br><br>**Optie 4**: een burger kan met afspraak getest bij de één van de 3 testbussen die rond rijden (verplaatsen zich elke 2 weken) in de Regio Amsterdam-Amstelland. Bij een testafname in de testbus worden de gegevens wel gelogd in Coronit. Let op: het testen zonder afspraak is niet altijd mogelijk.<br>**Testen zonder afspraa**k: burger meldt zich bij de locatie. De burger identificeert zich met zijn ID. Indien de burger al een dossier heeft wordt ter plekke een afspraak gemaakt om de burger te testen. Indien een burger geen dossier heeft, dan worden de gegevens ingevoerd in CoronIT. | | Een DPIA moet een systematische beschrijving bevatten van de beoogde verwerkingen (art. 35 lid 7, onder a AVG). |

| | | | | |
|---|---|---|---|---|
| **5** | Beschrijf eventuele (nieuwe) technologieën voor zover daarvan gebruik wordt gemaakt bij dit proces? Bijvoorbeeld internet of things, wifi tracking of behavioral advertising. | Binnen het testproces worden twee verschillende technologien ingezet (PCR, Antigeen, LAMP en E-NOSE). Ten eerste is er een PCR-test (polymerase chain reaction test) deze test toont aan of een betrokkene op het moment van testen besmet is met het coronavirus. Dit wordt gedaan door een arts of teststraatmedewerker afgenomen keel- en neusswab. Ten derde is er de LAMP-test (loop-mediated isothermal amplification test). Dit is een variatie op de PCR-test die sneller is dan de meeste PCR-testen. Het testproces is hetzelfde bij de PCR-test alleen worden hier andere apparaten en stoffen ingezet.<br><br>Ter afsluiting is er de E-NOSE- test (Electronic Nose test). Dit is een apparaat dat deeltjes detecteerd in lucht die mensen uitademen. De samenstelling van de lucht van besmette individuen is anders dan gezonde individuen, hierdoor kan besmetting vastgesteld worden. Deze laatste optie wordt echter tot op heden niet meer uitgevoerd. | Bij deze technologieën loopt u een verhoogd risico voor de impact van uw proces op de betrokkenen. De manier waarop betrokkenen gaan reageren is moeilijk in te schatten. Dit kan leiden tot verhoogde kans op imagoschade, verstoring van de bedrijfscontinuïteit, en acties door handhavers en toezichthouders. | |
| **6** | Betreft deze DPIA een enkele verwerking, of een reeks verwerkingen met een vergelijkbaar risico? | Reeks verwerkingen met een vergelijkbaar risico. | | |
| **7** | Wat zijn de doelen van de verwerkingen van persoonsgegevens binnen het proces? | Vaststellen positieve of negatieve test, informeren geteste personen, clusters detecteren, monitoring van ziekte. Het doel van het verwerken van persoonsgegevens binnen het testproces is om zo een zo compleet mogelijk beeld te krijgen van waar, hoeveel en hoe de infectie zich verspreiden. Het is een belangrijk middel om regionaal vast te stellen hoe de infectie zich verhoudt tot het landelijk gemiddelde, vanuit hier worden de eerste (regionale) maatregelen getroffen om het virus te bestrijden. Hierdoor kan de pandemie doeltreffender worden bestreden. | Als weet niet/niet omschreven: Een SMART omschreven doelstelling is essentieel voor het maken van keuzes voor het inrichten van een kwalitatief goede gegevensverwerking.<br>Bovendien loop uw organisatie compliance risico's als het doel niet voldoende precies is omschreven. | Een DPIA moet een systematische beschrijving bevatten van de verwerkingsdoeleinden (art.35 lid 7, onder a AVG). |
| **8** | Beschrijf de (categorieën van) betrokkenen waarvan persoonsgegevens worden verwerkt. Benoem of er sprake is van kwetsbare groepen. | In dit geval kunnen dit alle mensen zijn die zich in de regio van de GGD Amsterdam, regio Amstelland: Driemond, Amstelveen, Aalsmeer, Uihoorn, Weesp, Diemen en Ouder Amstel laten testen. Mensen met milde klachten die gerelateerd zijn aan het coronavirus en mensen die voort zijn gekomen uit bron- en contact onderzoek. Er wordt hierbij geen onderscheid gemaakt tussen groepen dus hier kan ook sprake zijn van kwetsbare groepen (zoals kinderen en/of ouderen). | Bij kwetsbare groepen: U loopt een verhoogd risico. Indien deze gegevens worden misbruikt heeft dit negatieve beeldvorming in de publieke opinie over de organisatie tot gevolg. U wordt geadviseerd maatregelen te treffen op een hoger beveiligingsniveau en betrokkenen de mogelijkheid te bieden zich aan de verwerking te onttrekken | |
| **9** | Geef aan welke (categorieën van) persoonsgegevens worden verwerkt? | Voornaam & achternaam<br>Adres (woonplaats, postcode, huisnummer, straatnaam, gemeente, land)<br>Geboortedatum<br>Geslacht<br>BSN<br>Telefoonnummer<br>E-mailadres<br>Geboorteland<br>Patiëntnummer<br>Klachten<br>Streepjescode testbuisje (hierop staan ook de naam en postcode van gestest persoon, om fouten te voorkomen bij het lab)<br>Uitslag van de coronatest<br>Datum van test<br>Orderformulier laboratoriumonderzoek<br>Datum eerste ziektedag<br>Testlocatie<br>Eventueel: naam van de arts die de test aanvraagt<br>Of je direct contact hebt gehad met anderen<br>Of je gewerkt hebt, en zo ja in welke beroepsgroep je werkt. Aanvullend voor prioriteit ABG-nummer of BRIN-nummer<br><br>Van cliënten zonder vaste verblijfsplaats of woonachtig in een ander land (zonder BSN-nummer worden andere persoonsgegevens vastgelegd. Bij deze burgers wordt bij BSN 9x9 ingevuld. Daarnaast krijgen zij het adres van de Nieuwe Achtergracht. Op de stickers van de barcodes staat de naam en geboortedatum van de geteste persoon, soms ook alleen patiëntnummer, afhankelijk van laboratorium en aanvullend doel, bijvoorbeeld sequencen. | | Persoonsgegevens zijn alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Bijvoorbeeld: NAW gegevens, geboortedatum, e-mail adres, telefoonnummer, gegevens over iemands financiële situatie, IP adres, bankrekeningnummer, salaris etc. |
| **10** | Worden er ook bijzondere persoonsgegevens, strafrechtelijke persoonsgegevens en/of BSN verwerkt? Zo ja geef aan welke gegevens. | De bijzondere gegevens die worden verwerkt zijn het BSN nummer en medische gegevens, waaronder:<br>- Testuitslag<br>- Klachten<br>- Datum eerste ziektedag | Het werken met dit type gegevens brengt een verhoogd risico van misbruik met zich mee die (potentieel grote) impact op de betrokkene heeft en vraagt daarmee o.a. om betere beveiliging. Het verwerken van deze gegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden. | Bijzondere persoonsgegevens zijn gegevens waaruit ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond blijkt en verwerkingen van genetische gegevens, biometrische gegevens met het oog op unieke identificatie van een persoon, of gegevens over gezondheid, gegevens met betrekking tot iemands seksuele gedrag of seksuele gerichtheid. Daarnaast ziet deze vraag ook op gegevens met betrekking tot strafrechtelijke veroordeling of strafbare feiten en de verwerking van het BSN |
| **11** | Geef aan op welke gegevensdrager de persoonsgegevens worden opgeslagen (hardware, software, netwerken). | Wordt alleen opgeslagen in CoronIT en het systeem dat wordt gebruikt door het Streeklab(GLIMS). Het aanvragen van onderzoeken vindt plaats door middel van de officiële aanvraagformulieren van het Streeklaboratorium of via digitale import (zoals zorgdomein of cyberlab). | | De WP29 vereist dat een systematische beschrijving van de gegevens ook omvat dat: "*de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen) worden geïdentificeerd*;" toelichting WP29 over gegevensbeschermingseffectbeoordeling) |
| **12** | Zijn de bewaartermijnen in kaart gebracht? Zo ja, geef aan wat de bewaartermijnen zijn. | Op grond van de WGBO is bij een positieve test de bewaartermijn maximaal 20 jaar nadat de pandemie is verholpen. Lab bewaart 3 maanden enkel positief. Het laboratorium laat in het administratiesysteem weten welke uitslag hoort bij welke streepjescode. Dit systeem koppelt de streepjescode weer aan jouw persoonsgegevens. In Amsterdam wordt ook de naam van de betrokkene op de testbuis genoteerd. | Als nee/weet niet: Het risico bestaat dat de gegevens langer worden verwerkt dan noodzakelijk. Hierdoor loopt u een compliance risico. Stel daarom bewaartermijnen vast. | "*Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is, dient de verwerkingsverantwoordelijke termijnen vast te stellen voor het wissen van gegevens of voor het periodiek toetsen ervan"* (overweging 39 AVG).<br>Let op: bewaartermijnen zijn iets anders dan archief termijnen. |
| **13** | Van hoeveel individuen worden er (ongeveer) persoonsgegevens verwerkt in het kader van dit proces? | Tot op heden zijn er 660.000 testen afgenomen. Voor de toekomst is dit aantal niet te voorspellen. | De kans op misbruik van de gegevens wordt groter naarmate u meer gegevens verwerkt. U wordt bij grootschalige verwerkingen geadviseerd maatregelen te treffen op een hoger beveiligingsniveau | |

| | | | | |
|---|---|---|---|---|
| | **Deel 2 - Betrokken actoren** | | | |
| **14** | Zijn alle partijen die in contact komen met de persoonsgegevens in kaart gebracht? | De partijen betrokken bij het test-proces zijn in kaart gebracht. Hieronder zullen deze partijen worden uitgelicht. | Als nee/weet niet: U loopt een verhoogd risico. Het risico bestaat dat niet duidelijk is wie de maatregelen die getroffen moeten worden om risico's af te dekken moet nemen en dat daardoor de risico's niet worden | |
| **15** | Welke interne en externe verantwoordelijken zijn betrokken bij dit proces? | Intern: Streeklab. Extern: GGD GHOR, alle GGD's in Nederland en externe labs (RIVM heeft toegang tot geanonimiseerde data). | | Bijvoorbeeld: College B&W, externe partijen etc. Dit kunnen gezamenlijke verantwoordelijken zijn, maar ook keten partners. |
| **16** | Zijn er afspraken gemaakt met andere verantwoordelijken over de verwerking van persoonsgegevens? | GGD Amsterdam, GHOR, VWS: GGD Amsterdam en GGD GHOR zijn een convenant overeengekomen waarin de samenverwerking wordt uitgewerkt, waarbij een verdeling wordt gemaakt in de verschillende verantwoordelijkheden. Deze verdeling van verantwoordelijkheden ziet ook op de verantwoordelijkheden afkomstig uit de AVG. | In de samenwerking met externe verantwoordelijkheden loopt u een verhoogd risico. Het risico bestaat dat niet alle partijen zorgvuldig met gegevens omgaan die tijdens het proces worden verzameld. Ook bestaat het risico dat de partijen de | |
| **17** | Zijn er verwerkers betrokken bij het proces? Zo ja, noem de verwerkers. | Verwerkers zijn:<br>- Atal Medial (Lab)<br>- Inbiome (Lab)<br>- Topicus (CoronIT)<br>- OLVG (Lab)<br>- LAMP Labs (nog beperkt in gebruik)<br>- CoMicro (Lab) | | |
| **18** | Is er een verwerkersovereenkomst afgesloten met de verwerkers? | Met Topicus is een verwerkersovereenkomst gesloten. Met Atal Medial, Pure Medical Dot World, OLVG, Inbiome is er geen verwerkersovereenkomst gesloten. | In de samenwerking met verwerkers loopt u een verhoogd risico. Het risico bestaat dat niet alle partijen zorgvuldig met gegevens omgaan die tijdens het proces worden verzameld. Ook bestaat het risico dat de partijen de risico's en de inspanning die nodig is om deze te verminderen anders inschatten. U wordt | Art. 28 AVG stelt het verplicht om met verwerkers een verwerkingsovereenkomst af te sluiten. De gemeente Amsterdam heeft een model verwerkersovereenkomst ontwikkeld. |
| **19** | Zijn er ontvangers betrokken bij dit proces? Zo ja, is er een overeenkomst met de ontvanger? | Huisartsen (met toestemming). RIVM (geanonimiseerd): hoeveel testen per locatie en hoeveel positieve testuitslagen. | Indien gegevens verstrekt worden aan andere partijen zonder dat deze gegevens daarvoor verzameld zijn bestaat het risico dat deze gegevens niet geschikt zijn voor het doel en dat betrokkenen worden geschaad door de verdere verspreiding van de gegevens | |
| **20** | Worden persoonsgegevens doorgegeven naar landen buiten de Europese Unie? Zo ja, geef aan om welke partijen het gaan en welke waarborgen hiervoor zijn genomen. | Nee. | U wordt geadviseerd na te gaan in hoeverre een adequaat beschermingsniveau wordt geboden door het betreffende land of de betreffende organisatie. Maak schriftelijke afspraken over hoe dit beschermingsniveau gehandhaafd kan worden. | Persoonsgegevens mogen niet zomaar worden doorgegeven naar buiten de Europese Unie. Hiervoor moeten passende waarborgen zijn genomen. Deze waarborgen staan genoemd in art. 45 en 46 AVG. |
| | **Deel 3 - Rechtmatigheid** | | | |
| | **Rechtsgrond** | | | |
| **21** | Is van alle verwerkingen in kaart gebracht of een rechtmatige grondslag van toepassing is? Zo ja, geef aan elke rechtmatige grondslag van toepassing is, of welke grondslagen van toepassing zijn. Motiveer waarom die grondslag van toepassing is. | De verwerkingen zijn in kaart gebracht. De grondslag voor de verwerkingen met betrekking tot het testen is een wettelijke plicht. Op de GGD's rust de plicht om infectieziektes te bestrijden en hiervan is testen een belangrijk onderdeel. Daarnaast stuurt GGD Amsterdam mogelijk ook de uitslag door naar de huisarts van de persoon die is gestest, dit gebeurt op basis van toestemming. De grondslag is zowel de WPG als WGBO voor het testen. | Voor het verwerken van persoonsgegevens is een grondslag noodzakelijk. Indien deze ontbreekt, loopt u compliance risico. Breng daarom de rechtmatige grondslag in kaart. | Je mag persoonsgegevens pas verwerken als er een rechtmatige grondslag voor aanwezig is (art. 5 en 6 AVG).<br><br>De AVG kent de volgende grondslagen:<br>a. ondubbelzinnige toestemming van de betrokkene,<br>b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;<br>c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;<br>d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;<br>e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen |
| **22** | Indien de verwerkingsactiviteiten zijn gebaseerd op het uitvoeren van een overeenkomst, geef aan om welke overeenkomst dit gaat en neem zo mogelijk een verwijzing naar de overeenkomst op. | De behandelingsovereenkomst op grond van de WGBO is de grondslag voor de verwerking van persoonsgegevens. | Om deze grondslag aan te kunnen tonen moet de overeenkomst aantoonbaar zijn. | "*Een verwerking die noodzakelijk is in het kader van een overeenkomst of een voorgenomen overeenkomst, dient rechtmatig te zijn*" overweging 44 AVG. |
| **23** | Indien de verwerkingsactiviteiten zijn gebaseerd op een wettelijke plicht, geef aan om welke wettelijke plicht dit gaat. Vermeld hierbij het wetsartikel. | N.v.t. | | "*Wanneer in deze verordening naar een rechtsgrond of een wetgevingsmaatregel wordt verwezen, vereist dit niet noodzakelijkerwijs dat een door een parlement vastgestelde wetgevingshandeling nodig is (...) Deze rechtsgrond of wetgevingsmaatregel moet evenwel duidelijk en nauwkeurig zijn, en de toepassing daarvan moet voorspelbaar zijn voor degenen op wie deze van toepassing is (....)*" overweging 41 AVG. |
| **24** | Indien de verwerkingsactiviteiten zijn gebaseerd op de vitale belangen van de betrokkene, geef aan om welke belangen dit gaat. | N.v.t. | Deze grondslag is slechts in uitzonderlijke gevallen van toepassing. Overleg daarom bij twijfel met de Privacy Officer van uw cluster of stadsdeel. | "*Verwerking van persoonsgegevens op grond van het vitale belang voor een andere natuurlijke persoon is in beginsel alleen toegestaan indien de verwerking kennelijk niet op een andere rechtsgrond kan worden gebaseerd.*" overweging 46 AVG. |

| | | | | |
|---|---|---|---|---|
| **25** | Indien de verwerkingsactiviteiten zijn gebaseerd op een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen, geef aan om welke taak dit gaat en noem het wetsartikel. | De Wet Publieke Gezondheid als uitgangspunt:<br>Art. 1 sub c WPG<br>"publieke gezondheidszorg: de gezondheidsbeschermende en gezondheidsbevorderende maatregelen voor de bevolking of specifieke groepen daaruit, waaronder begrepen het voorkómen en het vroegtijdig opsporen van ziekten."<br><br>Art. 2 lid 1 j.o. lid 2 sub a WPG<br><br>B&W bevordert de totstandkoming en de continuïteit van de publieke gezondheidszorg. Ter uitvoering van deze taak dragen zij zorg voor: "het verwerven van, op epidemiologische analyse gebaseerd, inzicht in de gezondheidssituatie van de bevolking".<br><br>En daarbij ook specifiek:<br><br>Art. 6 lid 1 sub a j.o. lid 2 WPG<br><br>B&W draagt zorg voor algemene infectieziekte bestrijding heeft onder andere de taak om preventieve maatregelen te nemen.<br><br>GGD Amsterdam-Amstelland:<br><br>Art. 14 lid 1 j.o. lid 2 WPG<br><br>Colleges van B&W van een veiligheidsregio treffen een gemeenschappelijke regeling, waarin er een openbaar lichaam wordt ingesteld, namelijk de Gemeentelijke Gezondheidsdienst.<br><br>Het mandaat van de GGD Amsterdam is op basis van art. 2 j.o. art 3 j.o. art. 4 lid 1 sub b van de Gemeenschappelijke regeling Gemeentelijke Gezondheidsdienst Amsterdam-Amstelland 2016, nr. 323/1432. | | "*Deze verordening schrijft niet voor dat voor elke afzonderlijke verwerking specifieke wetgeving vereist is. Er kan worden volstaan met wetgeving die als basis fungeert voor verscheidene verwerkingen op grond van een wettelijke verplichting die op de verwerkingsverantwoordelijke rust, of voor verwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang dan wel voor een taak in het kader van de uitoefening van het openbaar gezag. Het moet ook het Unierecht of het lidstatelijke recht zijn die het doel van de verwerking bepaalt. Voorts zou dat recht een nadere omschrijving kunnen geven van de algemene voorwaarden van deze verordening waaraan de persoonsgegevensverwerking moet voldoen om rechtmatig te zijn, en specificaties kunnen vaststellen voor het bepalen van de verwerkingsverantwoordelijke, het type verwerkte persoonsgegevens, de betrokkenen, de entiteiten waaraan de persoonsgegevens mogen worden vrijgegeven, de doelbinding, de opslagperiode en andere maatregelen om te zorgen voor rechtmatige en behoorlijke verwerking.*" Overweging 45 AVG. |
| **26** | Indien de verwerkingsactiviteiten zijn gebaseerd op een gerechtvaardigd belang, geef aan om welk belang dit gaat en beschrijf de afweging die hierbij is gemaakt. | N.v.t. | | De gemeente kan geen persoonsgegevens verwerken op basis van deze grondslag in het kader van de uitvoering van haar taken. Deze grondslag kan alleen gebruikt worden als het om een niet publieke taak gaat. "*In elk geval is een zorgvuldige beoordeling geboden om te bepalen of sprake is van een gerechtvaardigd belang, alsook om te bepalen of een betrokkene op het tijdstip en in het kader van de verzameling van de persoonsgegevens redelijkerwijs mag verwachten dat verwerking met dat doel kan plaatsvinden. De belangen en de grondrechten van de* |
| **27** | Is de verwerking van bijzondere persoonsgegevens, strafrechtelijke persoonsgegevens en/of het BSN toegestaan? Geef aan waarom. | De WGBO de grondslag voor de verwerking van bijzondere persoonsgegevens. Doorgifte huisarts en RIVM op basis van uitdrukkelijke toestemming. | | Bijzondere en strafrechtelijke persoonsgegevens mogen in principe niet verwerkt worden, tenzij een uitzondering van toepassing is (art. 9 en 10 AVG). Overheidsorganen kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun taak gebruik maken van het Burgerservicenummer (art. 10 Wet algemene bepalingen burger service nummer). Voor het overige mag het BSN alleen worden verwerkt als dat bij wet of AMvB is bepaald. |
| | **Toestemming** | | | |
| **28** | Indien de verwerkingsactiviteiten zijn gebaseerd op toestemming: is de toestemming vrij, specifiek, op informatie gebaseerd en ondubbelzinnig gegeven door de betrokkene? | Er is een verwerking die gebasseerd is op de grondslag toestemming en dat is de vraag over doorgifte uitslag naar huisarts bij positieve test. De betrokkene kan zelf een keuze maken. Deze keuze is vrij, specifiek en gebaseerd op ondubbelzinnige toestemming. Zoals ook vastgelegd in de privacyverklaring van de GGD GHOR (https://ggdghor.nl/privacyverklaring-coronit/). | | "*Wanneer de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegeven*." (Art. 7, lid 1 AVG) "' *Toestemming' van de betrokkene is elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwekring van persoonsgegevens aanvaardt*." (Art. 4, lid 11 AVG) |
| **29** | Is de toestemming gegeven door middel van een duidelijke actieve handeling? | Ja, het plaatsen van een vinkje. | | "*Toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring, ook met elektronische middelen, of een mondelinge verklaring waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van persoonsgegevens instemt*" (overweging 32 AVG) |
| **30** | Is of wordt bijgehouden hoe en wanneer de betrokkene toestemming heeft gegeven? | Ja. Dit wordt telefonisch of online expliciet gevraagd en geregistreerd in CoronIT. | | Toestemming moet aantoonbaar zijn gegeven (art. 7 AVG). |
| **31** | Heeft de betrokkene de mogelijkheid om toestemming op ieder moment in te trekken en zonder negatieve gevolgen? | De verwerking die berust op de toestemming is het doorsturen van de gegevens naar de huisarts. De betrokkene heeft de mogelijkheid om toestemming in te trekken. Dit heeft geen negatieve gevolgen. Enkel het gevolg dat de gegevens niet meer doorgestuurd worden naar de huisarts.<br><br>De betrokkene kan toestemming intrekken door middel van een schriftelijk verzoek aan de desbetreffende GGD. | Als nee/weet niet: U loopt een verhoogd risico. Indien u niet kunt voldoen aan verzoeken van betrokkenen om verwerking van gegevens te stoppen of omdat u deze mogelijkheid niet aanbiedt kan dit leiden tot irritatie of kostbare aanpassingen in systemen. U wordt geadviseerd betrokkenen de mogelijkheid te bieden de toestemming in te trekken en dit systeem technisch mogelijk te maken. Indien de impact van het intrekken van de toestemming groot is, is er waarschijnlijk geen sprake van een vrije wilsuiting. U loopt daarmee een compliance risico | " *De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet. Alvorens de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld. Het intrekken van de toestemming is even eenvoudig als het geven daarvan*." (Art. 7, lid 3 AVG) |

| | | | | |
|---|---|---|---|---|
| **32** | Omvatten de verwerkingsactiviteiten websites, apps of andere online diensten van de informatie maatschappij gericht op/aangeboden aan kinderen onder de leeftijd van 16 jaar? | Kinderen tot 7 jaar<br>Voor kinderen tot 7 jaar kan de ouder een testafspraak inplannen via 0800 - 1202. De GGD plant dan meer tijd in voor de testafname.<br><br>Kinderen vanaf 7 jaar<br>De ouder of verzorger maakt een afspraak via 0800-1202. Voor kinderen vanaf 7 jaar met eigen DigiD, kan ook online een afspraak ingepland worden. Maar als het kind de test spannend vindt kan beter telefonisch een afspraak maken. De GGD plant dan meer tijd in voor de testafname.<br><br>Kinderen vanaf 12 jaar<br>Voor kinderen vanaf 12 jaar kan zowel telefonisch als online een afspraak worden gemaakt. Kinderen vanaf 12 jaar moeten zelf ook aan de telefoon komen om toestemming te geven.<br><br>Kinderen vanaf 12 jaar die een DigiD hebben, kunnen ook zelf online een testafspraak maken. Ouders mogen hun kinderen tot 14 jaar helpen met het inloggen met DigiD. Kinderen van 14 jaar en ouder mogen zelf een testafspraak maken door in te loggen met hun eigen DigiD. U mag namelijk niet een DigiD van iemand anders gebruiken.<br><br>Kinderen vanaf 16 jaar<br>Kinderen van 16 of 17 kunnen zelf bellen voor een testafspraak. U mag als ouder ook bellen maar uw kind moet dan wel aan de telefoon komen om toestemming te geven. Vanaf 18 jaar moet uw kind, in de meeste gevallen, zelf bellen. | | "[bij het vragen van toestemming] *in verband met een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind, is de verwerking van persoonsgegevens rechtmatig wanneer het kind ten minsten 16 jaar is. Wanneer het kind jonger is dan 16 jaar is zulke verweking slechts rechtmatig indien en voor zover de toestemming of machtiging tot toestemming in dit verband wordt verleend door de persoon die ouderlijke verantwoordelijkheid voor het kind draagt*." (Art. 8, lid 1 AVG). |
| **33** | Wordt toestemming bij de situatie in de vorige vraag gevraagd door de persoon die ouderlijke verantwoordelijkheid voor het kind draagt? | Zie vorige vraag. | | |
| | **Transparantie** | | | |
| **34** | Indien de persoonsgegevens direct bij de betrokkene worden verzameld; welke informatie wordt ten tijde van de verzameling gecommuniceerd? | Op het moment dat de gegevens worden verzameld is op het moment dat de betrokkene een verzoek indient om een corona test te laten doen. De identiteit van de GGD is duidelijk, want daar maakt de betrokkene een afspraak. De grondslag van de verwerking, verwerkingsdoeleinden, bewaartermijnen en rechten van betrokkenen worden benoemd in de privacyverklaring op de website van de GGD GHOR.<br><br>Privacy verklaring: https://ggdghor.nl/privacyverklaring-testenopcoronavirus/ | Indien geen of niet voldoende informatie aan de betrokkenen wordt verstrekt dan is er een verhoogd risico. Transparantie is een belangrijk beginsel onder de AVG. Neem maatregelen om ervoor te zorgen dat betrokkenen goed geïnformeerd zijn. | Hier kan bijvoorbeeld naar het privacy statement worden verwezen, maar ook naar aanvullende informatie die beschikbaar is gesteld. Art. 13 AVG geeft een volledig overzicht van de informatie die aan een betrokkene moet worden verstrekt ten tijde van de verzameling van de persoonsgegeven. Het betreft ten minste: 1. identiteit van de verantwoordelijke, 2. Gegevens van de FG, 3. De verwerkingsdoeleinden, 4. Welk gerechtvaardigd belang wordt behartigd (indien als grondslag gebruikt), 5. (Categorieën van) ontvangers, 6. Of gegevens worden doorgegeven aan landen buiten de EU, 7. De bewaartermijn, 8. Rechten van de betrokkenen, 9. Het recht om toestemming in te trekken, 10. Het recht een klacht in te mogen dienen bij de toezichthouder, 11. Of de betrokkene verplicht is om de gegevens te verstrekken, 12. Of er sprake is van geautomatiseerde besluitvorming. |
| **35** | Indien de persoonsgegevens niet direct bij de betrokkene worden verzameld; welke informatie wordt ten tijde van de verzameling (of ten minste binnen een maand na verkrijging) gecommuniceerd? | Het 'Meldportaal Testuitslagen' is beschikbaar voor iedere arts die werkt op een coronatestlocatie buiten de GGD. Iedere organisatie die een (snel)test op corona aanbiedt en uitvoert, is verplicht de positieve testuitslagen te melden bij de GGD. | Indien geen of niet voldoende informatie aan de betrokkenen wordt verstrekt dan is er een verhoogd risico. Transparantie is een belangrijk beginsel onder de AVG. Neem maatregelen om ervoor te zorgen dat betrokkenen goed geïnformeerd zijn. | Art. 14 AVG geeft een volledig overzicht van de informatie die aan een betrokkene moet worden verstrekt wanneer de persoonsgegevens niet direct bij de betrokkene zijn verzameld. Het betreft ten minste: 1. identiteit van de verantwoordelijke, 2. Gegevens van de FG, 3. De verwerkingsdoeleinden, 4. Categorieën van persoonsgegevens, 5. (Categorieën van) ontvangers, 6. Of gegevens worden doorgegeven aan landen buiten de EU, 7. De bewaartermijn, 8. Welk gerechtvaardigd belang wordt behartigd (indien als grondslag gebruikt), 9. Rechten van de betrokkenen, 10. Het recht om toestemming in te trekken, 11. Het recht een klacht in te mogen dienen bij de toezichthouder, 12. De bron van de persoonsgegevens, 12. Of er sprake is van geautomatiseerde besluitvorming. |
| **36** | Is het privacy statement geschreven in duidelijke bewoordingen en makkelijk vindbaar voor de betrokkenen? | Ja, zie website GGD GHOR (https://ggdghor.nl/privacyverklaring-coronit/). De betrokkene ziet dit ook op het moment een afspraak wordt gemaakt voor een corona test. | | "*Overeenkomstig het transparantiebeginsel moet informatie die bestemd is voor het publiek of voor de betrokkene beknopt, eenvoudig toegankelijk en begrijpelijk zijn en moet duidelijke en eenvoudige taal en, in voorkomen geval, aanvullende visualisatie worden gebruikt*." (Overweging 58 AVG) |
| **37** | Indien de verwerking betrekking heeft op een samenwerkingsverband waarbij meerdere verwerkingsverantwoordelijken betrokken zijn, worden de relevante afspraken dan duidelijk gecommuniceerd aan de betrokkenen? | GGD Amsterdam en GGD GHOR zijn een convenant overeengekomen waarin duidelijk afspraken staan over hoe gecommuniceerd wordt aan de betrokkenen. | | "*Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze verordening vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene...*" (Art. 26, lid 1 AVG) " *De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld.*" (Art. 26, lid 2 AVG) |
| | **Deel 4 - Rechten van betrokkenen** | | | |
| **38** | Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op inzage? | De betrokkene kan zijn rechten uitoefenen bij het Loket Persoonsgegevens. Vervolgens wordt het verzoek opgepakt door de privacy contactpersoon. | Als nee/weet niet: U loopt een verhoogd risico. Betrokkenen hebben het recht om hun gegevens in te zien. Hierbij is het van belang dat u zelf ook een helder overzicht heeft van de gegevens die worden verwerkt en waar deze zich binnen de organisatie bevinden. U loopt ook een compliance risico aangezien het verplicht is betrokkenen (op verzoek, eventueel tegen een redelijke vergoeding) inzage te geven. | "*De betrokkene heeft het recht om de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens ….*" (Art. 15, lid 1 AVG)<br><br>Voor de rechten van betrokkenen is een stedelijk proces ingericht. Deze vraag ziet erop dat technisch en praktisch rekening wordt gehouden met deze rechten van betrokkenen. Bijvoorbeeld door de rechten duidelijk te vermelden. |
| **39** | Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op rectificatie? | Ja | Als nee/weet niet: U loopt een verhoogd risico. Het bieden van een mogelijkheid tot correctie verbetert de gegevenskwaliteit. Als correcties niet doorgevoerd (kunnen) worden, verslechterd de gegevenskwaliteit en zijn de gegevens uiteindelijk (mogelijk) niet meer geschikt. U loopt hiermee ook een compliance risico. | "*De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen*" (Art. 16 AVG).<br><br>Voor de rechten van betrokkenen is een stedelijk proces ingericht. Deze vraag ziet erop dat technisch en praktisch rekening wordt gehouden met deze rechten van betrokkenen. Bijvoorbeeld door de rechten duidelijk te vermelden. |
| **40** | Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op wissing/verwijdering van persoonsgegevens? | Ja | Als nee/weet niet: U loopt een verhoogd risico. Betrokkenen hebben het recht om te verzoeken om verwijdering van gegevens. Als er geen zwaarwegende redenen zijn om dit niet te doen, dient dit ook uitgevoerd te worden. In andere gevallen heeft de betrokkene het recht meegedeeld te worden om welke reden (deels) niet aan het verzoek wordt voldaan. U loopt hiermee een compliance risico. | "*De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen*" in een aantal gevallen (art. 17 AVG).<br><br>Voor de rechten van betrokkenen is een stedelijk proces ingericht. Deze vraag ziet erop dat technisch en praktisch rekening wordt gehouden met deze rechten van betrokkenen. Bijvoorbeeld door de rechten duidelijk te vermelden. |

| | | | | |
|---|---|---|---|---|
| **41** | Kan worden voldaan aan een verzoek om dataportabiliteit? | Ja | | Indien de grondslag van de verwerking toestemming of uitvoering van de overeenkomst is, dan kan de betrokkene een beroep doen op het recht van dataportabiliteit (art. 20 AVG). |
| **42** | Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op bezwaar? | Ja | | "*De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens op basis van* [de grondslag algemeen belang en gerechtvaardigd belang]*, met inbegrip van profilering op basis van die bepalingen*" (art. 21, lid 1 AVG).<br><br>Voor de rechten van betrokkenen is een stedelijk proces ingericht. Deze vraag ziet erop dat technisch en praktisch rekening wordt gehouden met deze rechten van betrokkenen. Bijvoorbeeld door de rechten duidelijk te vermelden. |
| **43** | Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op beperking? | Ja | | Betrokkenen hebben het recht om de verwerking van hun gegevens te laten beperken indien, kortweg, **a)** de juistheid van de persoonsgegevens wordt betwist door de betrokkene, **b)** de verwerking onrechtmatig is, **c)** de persoonsgegevens niet meer nodig zijn om het doel uit te oefenen, **d)** de betrokkene heeft bezwaar gemaakt en is in afwachting van antwoord (art. 18 AVG).<br><br>Voor de rechten van betrokkenen is een stedelijk proces ingericht. Deze vraag ziet erop dat technisch en praktisch rekening wordt gehouden met deze rechten van betrokkenen. Bijvoorbeeld door de rechten duidelijk te vermelden. |
| **44** | Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig | De kwalitieit van de gegevens wordt gewaarborgd doordat in principe alle gegevens worden aangeleverd door de betrokkenen zelf. Soms gebeurt het dat een betrokkene een verkeerde huisarts doorgeeft. Er wordt bij het maken van een afspraak gevraagd aan de betrokkene of de testuitkomst gedeeld kan worden met zijn/haar huisarts. Hierbij kan een datalek ontstaan aangezien de gegevens van welke huisarts een betrokkene onder valt niet up-to-date zijn. Ook kan het zijn dat een betrokkene niet weet onder welke huisarts hij/zij valt, vaak staat een betrokkene ingeschreven in een praktijk waar bij een bezoek steeds een andere huisarts wordt gezien. Hierdoor vult een betrokkene mogelijk de verkeerde huisarts in waar zij dus officieel niet onder vallen. | Als nee/weet niet: U loopt een verhoogd risico. Het is van belang dat de verwerkte gegevens juist zijn om ervoor te zorgen dat geen verkeerde conclusies worden getrokken of verkeerde acties worden ondernomen. U loopt hiermee ook een compliance risico. | "*Persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd (...)*" (art. 5, lid 1 onder d AVG). |
| | **Profilering en geautomatiseerde besluitvorming** | | | |
| **45** | Worden er profielen opgesteld van de betrokkenen, al dan niet geanonimiseerd? | Nee. | Als ja/weet niet: U loopt een verhoogd risico. Het risico bestaat dat de betrokkenen of de algemene opinie dit als een potentiële bedreiging voor hun privacy zien. | |
| **46** | Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden? | Nee. | Als ja/weet niet: U loopt een verhoogd risico. Het nemen van beslissingen op basis van profilering kan uitgelegd worden als discriminatie van bepaalde groepen. Zorg ervoor dat indien u toch gebruik maakt van profileringen duidelijk is:<br>- Op basis waarvan deze profielen worden opgesteld.<br>- Welke beslissingen op welke wijze worden genomen op basis van de profielen.<br>- Of uit profielen gevoelige informatie is af te leiden.<br>Zorg er ook voor dat indien nodig betrokkenen geïnformeerd worden over deze profilering en mogelijke beslissingen. | |
| **47** | Is er sprake van geautomatiseerde besluitvorming? Zo ja, op basis van welke grondslag? | Nee. | Als ja/weet niet: U loopt een verhoogd risico. Het nemen van beslissingen op basis van een bepaalde profilering kan uitgelegd worden als discriminatie van bepaalde groepen. Zorg ervoor dat indien u toch gebruik maakt van profileringen duidelijk is:<br>- Op basis waarvan deze profielen worden opgesteld.<br>- Welke beslissingen op welke wijze worden genomen op basis van de profielen.<br>- Of uit profielen gevoelige informatie is af te leiden.<br>Zorg er ook voor dat indien nodig betrokkenen geïnformeerd worden over deze profilering en mogelijke beslissingen. | "*De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.* [Dit] *geldt niet indien het besluit: a)noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke; b) is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of c) berust op de uitdrukkelijke toestemming van de betrokkene*." (art. 22, lid 1 & 2 AVG) |
| | **Deel 5 - Doelbinding & proportionaliteit** | | | |
| **48** | Worden de persoonsgegevens gebruikt voor een ander doel dan waarvoor zij verzameld zijn? | Ja, het is mogelijk dat op grond van wetenschappelijk onderzoek de gegevens die verzameld worden, gebruikt kunnen worden voor onderzoeken. Dit valt onder de grondslag WPG (art. 2 lid 1 j.o. lid 2 sub a WPG). Over alle onderzoeken wordt een aparte DPIA gedaan. In deze DPIA's worden de grondslagen uitvoerig bekeken. | U loopt een verhoogd risico. Indien betrokkenen worden verrast door de gegevens verwerking bijvoorbeeld omdat meer gegevens worden verzameld dan op het eerste gezicht noodzakelijk is, of omdat het verdere gebruik niet in lijn is met het doel van verzamelen bestaat het risico dat de betrokkene de gegevens niet wil verstrekken of bezwaar maakt tegen het gebruik.<br><br>U wordt geadviseerd na te gaan of het doel op andere | Persoonsgegevens mogen alleen worden verzameld voor een welbepaald uitdrukkelijk omschreven en gerechtvaardigd doel (art. 5, lid 1 onder b AVG). |
| **49** | Indien de vorige vraag met 'ja' is beantwoord: is het doel waarvoor de persoonsgegevens verwerkt gaan worden verenigbaar met het oorspronkelijke doel? | Onderzoeken o.g.v. andere grondslagen corona gerelateerd. | | Een verwerking voor een ander doel is slechts toegestaan als de verdere verwerking is gebaseerd op toestemming van de betrokkene of op een specifiek wettelijk voorschrift, dat een noodzakelijke en evenredige maatregel is in een democratische samenleving ter waarborging van een belangrijke doelstelling van algemeen belang. Dit kan bijvoorbeeld zijn de openbare veiligheid, budgettaire of fiscale aangelegenheden. (art. 6, lid 4 en art. 23 , lid 1 AVG). Daarnaast zijn verdere verwerkingen ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of voor statistische doeleinden verenigbaar met de oorspronkelijke doeleinden. Daarbij geldt dat passende maatregelen moeten worden getroffen om de betrokkene te beschermen (art. 89 |

| | | | | |
|---|---|---|---|---|
| **50** | Worden de persoonsgegevens gebruikt voor een ander doel dat niet specifiek is omschreven? | Nee, alle doelen zijn vooraf specifiek bepaald in wetgeving. | Als nee/weet niet: Het gebruik van de gegevens moet in overeenstemming met het doel van de verwerking zijn. Indien dit niet het geval is bestaat het risico dat de gegevens niet geschikt zijn voor het doel omdat bijvoorbeeld de kwaliteit niet goed is. U loopt een compliance risico indien u hier niet aan voldoet. | Persoonsgegevens mogen alleen worden verzameld voor een welbepaald uitdrukkelijk omschreven en gerechtvaardigd doel (art. 5, lid 1 onder b AVG). |
| **51** | Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen? | Ja, Hpzone & Coronit en GLIMS (Global Laboratory Information System) | Bij ja: U loopt een verhoogd risico dat de gegevens gebruikt worden of in de toekomst gebruikt gaan worden voor andere doeleinden dan oorspronkelijk voor verzameld (function creep). U wordt geadviseerd maatregelen te treffen om deze zogenaamde function creep te voorkomen of onmogelijk te maken, bijvoorbeeld door het hanteren van strikte bewaar termijnen en toegangsrestricties. | |
| **52** | Is de (voorgenomen) verwerking effectief om het beoogde doel te bereiken? Geef aan waarom. | Ja, pandemie wordt op deze manier zo effectief mogelijk bestreden. | Indien de verwerking niet effectief is om het doel te bereiken dat is er waarschijnlijk geen sprake van een goede dataminimalisatie en/of doelbinding. Uw organisatie loopt daarmee een compliance risico. | Dit kan bijvoorbeeld worden aangetoond met empirisch onderzoek of op basis van ervaringen uit het verleden. |
| **53** | Staat de impact voor de persoonlijke levenssfeer van de betrokkene van de voorgenomen verwerking van persoonsgegevens in redelijke verhouding tot het doel? Geef aan waarom. | Ja, pandemie wordt op deze manier zo effectief mogelijk bestreden. | | *"De beoordeling bevat ten minste… een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden*" (art. 35, lid 7 onder b AVG). |
| | **Deel 6 - Data minimalisatie & subsidiariteit** | | | |
| **54** | Kan het proces ook worden gerealiseerd op een manier die minder ingrijpend is voor de impact op de privacy van betrokkenen? Geef aan waarom wel/niet.<br><br>Geef aan welke alternatieven zijn overwogen om het proces te realiseren op een manier die minder ingrijpend is voor de impact op de privacy van de betrokkenen? | Het is niet mogelijk om dit proces op een minder ingrijpende manier te laten verlopen. In verband met de grote maatschappelijke gevolgen. Er zijn een aantal gegevens die niet direct nodig zijn voor het uitvoeren van het proces. Zoals het uitvragen van gezondheidsklachten, beroep etc. Deze gegevens zijn niet nodig voor het uitvoeren van een test. Wel bijvoorbeeld bij het uitvoeren van bron- en contactonderzoek. | Het verwerken van zo min mogelijk gegevens heeft een aantal voordelen:<br>- De benodigde opslag en rekencapaciteit van uw computer systemen is lager, waardoor prestaties, hersteltijden en service niveaus kunnen worden verhoogd.<br>- U zult minder gegevens te hoeven onderhouden en | *"De beoordeling bevat ten minste… een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden"* (art. 35, lid 7 onder b AVG). Kunnen er bijvoorbeeld minder gegevens worden verwerkt, minder bijzondere of gevoelige gegevens worden gebruikt, zijn privacy by default en privacy by design goed toegepast? etc. |
| **55** | Zijn alle persoonsgegevens noodzakelijk om het beoogde doel te bereiken? | Ja, landelijk bepaald. | Als nee/weet niet: U loopt een verhoogd risico. Het risico bestaat dat betrokkenen minder snel willen meewerken, of het vertrouwen in de organisatie vermindert. U wordt geadviseerd enkel gegevens te gebruiken die noodzakelijk zijn. Bovendien loopt uw organisatie compliance risico's als dit niet het geval is. | |
| **56** | Hoe is geborgd dat de standaardinstellingen van de betrokken apparatuur of applicaties zodanig zijn dat alleen de persoonsgegevens worden verzameld die noodzakelijk zijn voor het specifieke doel? Geef aan welke maatregelen zijn getroffen. | De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking.<br>In CoronIT is met behulp van sterretjes minimaal bepaald welke informatie noodzakelijk is. | | "*De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking*" (art. 25, lid 2 AVG) |
| | **Deel 7 - Opslagbeperkingen** | | | |
| **57** | Worden de persoonsgegevens verwijderd op het moment dat zij niet meer noodzakelijk voor het bereiken van het doel? | Ja, de persoonsgegevens worden bewaard o.g.v. de wettelijke termijnen. | Als nee/ weet niet: U loopt een verhoogd risico. Indien gegevens oneindig bewaard worden, wordt het risico dat deze gebruikt worden door ongeautoriseerde personen hoger. Eveneens brengt het kosten met zich mee om de gegevens te bewaren (en onderhouden). U loopt hiermee een compliance risico. U dient gegevens slechts zo lang te bewaren als nodig is voor het voldoen aan de doelstellingen. U wordt geadviseerd de gegevens nadat ze niet meer nodig zijn te vernietigen (als een wettelijke verplichting om ze te bewaren dit niet in de weg staat) of indien dit niet mogelijk is te anonimiseren. | "*Dit vereist met name dat ervoor wordt gezorgd dat de opslagperiode van de persoonsgegevens tot een strikt minimum wordt beperkt. Persoonsgegevens mogen alleen worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt*" (overweging 39 AVG).<br><br>Er kan in het kader van archivering voor bepaalde gegevens een andere bewaartermijn bestaan. Ga na welke persoonsgegevens noodzakelijk zijn om te bewaren voor archiveringsdoeleinden en welke verwijderd kunnen worden. |
| **58** | Op welke manier wordt gerealiseerd dat de data daadwerkelijk worden verwijderd/geanonimiseerd? | Wettelijke termijnen zijn vastgesteld en over vijf jaar vindt de uitvoering plaatst. | | |
| **59** | Indien geen bewaartermijnen zijn gedefinieerd, zijn er maatregelen genomen om de persoonsgegevens desalniettemin te verwijderen? | N.v.t. | | |
| | **Deel 8 - Bevelliging, integriteit en vertrouwelijkheid** | | | |
| **60** | Zijn er op basis van de VRA extra maatregelen nodig, naast de BIG maatregelen? | Inventarisatiesheet, tabblad 3. BIA, ingevuld (werkwijze binnen GGD Amsterdam). De BIA vragen komen overeen met de BIV-vragen uit de VRA/Baselinetoets. Naast de NEN 7510, extra maatregelen nodig. Deze maatregelen zijn opgenomen in de inventarisatiesheet. | | "*Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen (...)*" (art. 32, lid 1 AVG) |
| **61** | Is voor dit proces aangesloten bij een goedgekeurde gedragscode? Zo ja, vermeld de gedragscode. | Geen gedragscode van toepassing. Wel een ambseed en een geheimhouding. | Let op: Op dit moment is een dergelijke gedragscode nog niet afgesloten, dus hierbij kan niet worden aangesloten. | "*Bij het beoordelen van het effect van de door een verwerkingsverantwoordelijke of verwerker verrichte verwerkingen, en met name ter wille van een gegevensbeschermingseffectbeoordeling, wordt de naleving van de in artikel 40 bedoelde goedgekeurde gedragscodes naar behoren in aanmerking genomen*" (art. 35, lid 8 AVG). |
| **62** | Zijn de persoonsgegevens gepseudonimiseerd waar mogelijk? | Nee. | Door het pseudonimiseren van persoonsgegevens wordt de impact voor de betrokkenen verkleind aangezien minder informatie over de betrokkene wordt prijsgegeven. Let op: gepseudonimiseerde persoonsgegevens zijn nog steeds onderhevig aan de AVG. | |
| **63** | Zijn de persoonsgegevens versleuteld waar mogelijk? | Nee. | Door het versleutelen (encryptie) van persoonsgegevens wordt de impact voor de betrokkenen verkleind aangezien minder informatie over de betrokkene wordt prijsgegeven. | |

| | | | | |
|---|---|---|---|---|
| **64** | Zijn toegangsmaatregelen genomen waardoor alleen personen toegang hebben tot persoonsgegevens voor zover dat noodzakelijk is voor de uitoefening van hun taak? | Ja, landelijke maatregelen op het autorisatiebeheer. Hiervoor is er op rol niveau een autorisatiematrix opgesteld. | Indien nee/weet niet: u loopt een verhoogd risico. Door dat persoonsgegevens toegankelijk zijn voor personen die ze niet nodig hebben (binnen of buiten de gemeente Amsterdam) is het waarschijnlijk dat zij worden verwerkt voor andere doeleinden. Bovendien levert dit vanuit beveiligingsperspectief risico's op. | |
| | **Deel 9 - Beschrijving en beoordeling risico's betrokkenen** | | | |
| **65** | Omschrijf welke negatieve privacy gevolgen voor betrokkenen mogelijk kunnen optreden bij de uitvoering van dit proces. | Fraude, diefstal van gegevens en identiteitsfraude (zie volgende tabblad). | | Ga hierbij in op eventuele immateriële, materiele en/of lichamelijke schade voor de betrokkenen. Let daarbij op de aard, de omvang en het gevolg van de verwerkingen zoals die naar voren is gekomen bij het invullen van deze vragenlijst. Is er bijvoorbeeld kans op: discriminatie, stigmatisering en uitsluiting; (blootstelling aan) identiteitsdiefstal of fraude; financiële verliezen; reputatie- of anderszins relationele schade; verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens; |
| **66** | Hoe groot is de kans dat de omschreven risico's zich voordoen? | Aanzienlijk groot risico (zie volgende tabblad). | De kans dat een bepaald risico zich in de praktijk zal voordoen hangt in grote mate af van de genomen (beveiligings)maatregelen. Geef aan of de kans per risico klein/middel/groot is. | |
| **67** | Omschrijf het restrisico voor de betrokkenen. Geef aan of dit restrisico hoog is. | Restriciso blijft BCO. Grote flexibele schil van starters. Controle is lastig (zie volgende tabblad). | Als na de genomen maatregelen een risico resteert voor de betrokkenen dan moeten er aanvullende maatregelen worden getroffen om dit risico zo goed mogelijk te mitigeren. Het is ook mogelijk dat extra advies ingewonnen moet worden. | |
| **68** | Omschrijf de voorgestelde maatregelen om het restrisico te mitigeren. | Er zijn hier nog geen maatregelen voor. | | |
| | **Deel 10 - Ingewonnen advies** | | | |
| **69** | Is er advies ingewonnen van de Functionaris Gegevensbescherming (FG) bij het uitvoeren van deze DPIA? | Ja, controle achteraf. | | De gemeente Amsterdam heeft een FG [invoegen contactdetails]. Het advies van de FG moet worden ingewonnen bij het uitvoeren van een DPIA. (art. 35 lid 2 AVG) Neem het advies van de FG op bij de DPIA rapportage, bijvoorbeeld in tab 3. |
| **70** | Is er advies ingewonnen van de Autoriteit Persoonsgegevens bij het uitvoeren van deze DPIA? Geef aan waarom wel of geen advies is ingewonnen. | Nee. | | Art. 36 AVG schrijft voor dat de toezichthouder voorafgaand moet worden geraadpleegd indien (i) de DPIA uitwijst dat er, ondanks eventuele maatregelen, een hoog risico verbonden blijft aan de (voorgenomen) verwerking en, (ii) indien dat nationaal is bepaald.<br><br>Van optie (ii) kan gebruik worden gemaakt door nationale lidstaten indien het gaat om verwerkingen ter vervulling van een taak van algemeen belang, onder meer sociale bescherming en volksgezondheid. Uit de toelichting bij de UAVG blijkt dat op dit moment geen gebruik is gemaakt van de mogelijkheid om nationaal toestemming van de Autoriteit Persoonsgegevens verplicht te stellen voor bepaalde verwerkingen. Er wordt verwezen naar de oude artikelen 31 en 32 Wbp. |
| **71** | Indien advies is ingewonnen van de Autoriteit Persoonsgegevens, geef aan op welke manier invulling is gegeven aan dit advies. | N.v.t. | | |
| **72** | Is de betrokkenen (of hun vertegenwoordigers) gevraagd om hun visie te geven over de verwerkingsactiviteiten? Geef aan waarom wel/niet. | N.v.t. | | "*De verwerkingsverantwoordelijke vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van de bescherming van commerciële belangen of de beveiliging van verwerkingen*." (Art. 35 lid 9 AVG)<br><br>Op dit moment zijn nog geen concrete voorbeelden bekend van een voorkomend geval waarbij betrokkenen om hun mening moet worden gevraagd.<br><br>NB: ook indien hiervoor persoonsgegevens worden verwerkt dient daarvoor een rechtmatige grondslag aanwezig te zijn. De WP29 geeft aan dat dit niet toestemming kan zijn. |
| **73** | Geef aan op welke manier opvolging is gegeven aan de visie van betrokkenen. Indien geen opvolging is gegeven aan deze visie, motiveer waarom dat niet is gedaan. | n.v.t. | | |