Beschrijving en beoordeling risico's betrokkenen en mitigerende maatregelen		
Welke negatieve privacy gevolgen voor betrokkenen kunnen mogelijk optreden?	**Voorgestelde maatregelen?**	**Opgenomen in PvE?**
ongeautoriseerde wijzigingen in de informatie/data	Voor de applicatie zijn functioneel en technisch beheerders aangewen. Een overzicht van beheerders is beschikbaar.	ja
	Het voeren van wijzigingen in de applicatie wordt door de gerbruikersgoep via FBEI door de leverancier aangebracht. De keyusers worden door de leverancier geïnformeerd. De wijziging wort eerst in een testomgeving voordat de implementatie plaatsvindt.	ja
	De leverancier levert periodieke updates en releases die door een specifiek team van gebruikers in de testomgeving worden getest.	ja
	Gegevens worden geanonimiseerd verzonden naar RIVM (via OSIRIS) en zijn niet herleidbaar naar persoonsgegevens.	ja
	Voor het verzenden van informatie naar het RIVM (via OSIRIS) wordt de informatie eerst gecontroleerd door een geautoriseerde medewerker. (Werkwijzen zijn vastgelegd in werkinstructies).	ja
	De leverancier van de software van de applicatie is gecertificeerd volgens ISO 27001.	
Informatie/data niet beschikbaar/verloren gegaan	Door KPN intened services (24/7) worden voortdurend back-ups gemaakt. Met deze leverancier en InFact zijn afspraken gemaakt over support en verhelpen van storingen.	ja
Vertrouwelijke informatie ongeautoriseerd verpsreiden	Toegang via persoonlijke code geregeld door ID manager. Controle op toegang zal periodiek plaatsvinden door Automatisering.	
	Een procedure voor autorisatie en logging is beschikbaar bij Automatisering. Controle op logging wordt uitgevoerd dooor Automatisering.	
	Controle op logging zal periodiek uitgevoerd worden (de frequentie en omgvang zal bepaald worden na verzameling van data/gegevens).	
Rapportage aan RIVM via OSIRIS is niet veilig	Data wordt na controle, autorisatie en anonimisatie beveiligd verzonden aan RIVM.	ja

Gemeente Amsterdam - Data Protection Impact Assessment (DPIA)

Gemeente Amsterdam

Cluster: GGD A'dam, afdeling Infectieziekten, cluster sociaal
Directie:
Procesnaam (bedrijfsproces): Bron- en contactopsporing t.b.v. COVID-19 m.b.v HPZone
Datum: 18-05-2020
Proceseigenaar: 5.1.2,e
Opdrachtgever: GGD Amsterdam
Versie: 1
Auteur: 5.1.2,e
Functie: Kwaliteitsadviseur

	Vraag		Risico scoring
	Deel 1 - Algemeen	**Beantwoordingsveld**	**Toelichting**
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 in het proces, dan hoeft niet opnieuw een DPIA te worden gedaan. U kunt stoppen.
4	Beschrijf het proces en de (voorgenomen) verwerkingsactiviteiten en/of het voorgenomen beleid/regelgeving waarvoor deze DPIA wordt uitgevoerd.	Het uitvoeren van bron- en contactonderzoek conform de Wet publieke gezondheid (Wpg); met behulp van HPZone; een applicatie specifiek ontworpen voor dit doel. De verwerking betreft patiëntadministratie voor het registreren en uitvoeren van bron- en contactopsporing bij een meldingsplichtige infectieziekte COVID-19, inclusief aanemen, vastleggen en opvolgen van een melding/aanvraag, testuitslagen en rapporteren van data aan het RIVM. (HPZone was al geïmplementeerd in alle GGD'en van Nederland).	Het Dashboard is een real-time weergave van alle infectieziektemeldingen, uitbraken en vragen bij de GGD'en in Zuid-Nederland.
5	Beschrijf eventuele (nieuwe) technologieën voor zover daarvan gebruik wordt gemaakt bij dit proces? Bijvoorbeeld internet of things, wifi tracking of behavioral advertising.	N.v.t.	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?	Een reeks van verwerkigen met een vergelijkbaar risico: het registreren van patiënten met (mogelijk) COVID-19, het uitvoeren van bron- en contactonderzoek en het rapporteren van de resultaten aan het RIVM.	
7	Wat zijn de doelen van de verwerkingen van persoonsgegevens binnen het proces?	Registreren en managen van een meldingsplichtige ziekte; uitvoeren van bron- en contactonderzoek.	Als weet niet/niet omschreven: Een SMART omschreven doelstelling is essentieel voor het maken van keuzes voor het inrichten van een kwalitatief goede gegevensverwerking. Bovendien loop uw organisatie compliance risico's als het doel niet voldoende precies is omschreven.
8	Beschrijf de (categorieën van) betrokkenen waarvan persoonsgegevens worden verwerkt. Benoem of er sprake is van kwetsbare groepen.	Cliënten (kunnen ook kwetsbare groepen zijn) mogelijk besmet (of verdacht van besmetting) met het coronavirus (COVID-19).	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?	NAW gegevens, geboortedatum, e-mail adres, telefoonnummer.	
10	Worden er ook bijzondere persoonsgegevens, strafrechtelijke persoonsgegevens en/of BSN verwerkt? Zo ja geef aan welke gegevens.	Bijzondere persoonsgegevens (etnische afkomst, gegevens over gezondheid) en BSN.	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.
11	Geef aan op welke gegevensdrager de persoonsgegevens worden opgeslagen (hardware, software, netwerken).	GGD hardware, software HPZone (InFact), OSIRIS (RIVM). De applicatie wordt gehost door de provider KPN B.V.	

12	Zijn de bewaartermijnen in kaart gebracht? Zo ja, geef aan wat de bewaartermijnen zijn.	Ja. Voor het registreren en managen van meldingesplichtige ziekten geldt een bewaartermijn van 20 jaar (Wgbo, art. 454). Voor bron- en contactopsporing geldt een termijn van 5 jaar (Wpg, art. 29).	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.
13	Van hoeveel individuen worden er (ongeveer) persoonsgegevens verwerkt in het kader van dit proces?	Meerdere personen, afhankelijk van omvang en verloop infectieziekte/uitbraak.	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?	Ja	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 afgedekt. Bovendien loopt u een compliance risico omdat er diverse wettelijke verplichtingen op de verantwoordelijke rusten en het risico bestaat dat niet alle wettelijke verplichtingen worden nagekomen.
15	Welke interne en externe verantwoordelijken zijn betrokken bij dit proces?	Interne verantwoordelijken: GGD Amsterdam/IZ, GGD Automatisering, Streeklab. Externe verantwoordelijken: RIVM, de provider van de applicatie (KPN B.V.) en InFact (de leverancier van de software voor de applicatie).	
16	Zijn er afspraken gemaakt met andere verantwoordelijken over de verwerking van persoonsgegevens?	Ja. GGD Amsterdam is lid van de Federatie Beheer en Exploitatie Infrastructuur Infectieziektenbestrijding NL (FBEI). FBEI is verantwoordelijk voor het opstellen van (verwerker)sovereenkomsten met de hosting provider KPN B.V. voor alle GGD'en in NL i.k.v. kostenreductie.	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 risico's en de inspanning die nodig is om deze te verminderen anders inschatten. U wordt geadviseerd heldere afspraken vast te leggen.
17	Zijn er verwerkers betrokken bij het proces? Zo ja, noem de verwerkers.	Ja. De applicatie wordt gehost door KPN B.V. Er wordt gewerkt aan verwerkersovereenkomsten (zie ook 16). KPN is gecertificeerd conform ISO 27001. Met de leverancier van de software InFact heeft GGD een contract en een SLA	
18	Is er een verwerkersovereenkomst afgesloten met de verwerkers?	De GGD heeft nog geen verwerkersovereenkomst met KPN B.V. (Zie ook 16 en 17). KPN B.V. werkt in opdracht van FBEI. Deze laatste moet een verwerkersovereenkomst met KPN aansluiten.	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 geadviseerd heldere afspraken vast te leggen.
19	Zijn er ontvangers betrokken bij dit proces? Zo ja, is er een overeenkomst met de ontvanger?	Ja. RIVM is ontvanger van de rapporten. Deze worden in geanonimiseerde vorm aangeleverd via OSIRIS/GLIMS (GGD heeft een verwerkersovereenkomst voor GLIMS).	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. U hebt mogelijk een compliance risico. Beoordeel of er een rechtmatige grondslag aanwezig is om de persoonsgegevens te verstrekken.
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.
	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.	Ja. De verwerking is noodzakelijk om te voldoen aan een wettelike verplichting; en voor de vervulling van een taak van algemeen belang; Wet publieke gezondheid Wpg (art. 21-29). Dus voorwaarden c en e van art. 5 en 6 AVG.	Voor het verwerken van persoonsgegevens is een grondslag noodzakelijk. Indien deze ontbreekt, loopt u compliance risico. Breng daarom de rechtmatige grondslag in kaart.
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.	N.v.t.	Om deze grondslag aan te kunnen tonen moet de overeenkomst aantoonbaar zijn.
23	Indien de verwerkingsactiviteiten zijn gebaseerd op een wettelijke plicht, geef aan om welke wettelijke plicht dit gaat. Vermeld hierbij het wetsartikel.	Meldingen t.b.v. meldingsplichtige infectieziekten volgens artikel 21-29 van de Wpg.	
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.
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.	Bestrijden en voorkomen van infectieziekten, specifiek COVID-19 (zie ook 23).	

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.	
27	Is de verwerking van bijzondere persoonsgegevens, strafrechtelijke persoonsgegevens en/of het BSN toegestaan? Geef aan waarom.	Ja, GGD is een overheidsorgaan en de taak wordt uitgevoerd o.a. in het kader van een wettelijke verplichting (zie ook 21). Voor de overheid is het gebruik van het BSN, geregeld in art. 10 Wet algemene bepalingen burgerservicenummer (Wabb) Overheidsorganen kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun publieke taak gebruikmaken van het BSN, zonder dat daarvoor nadere wetgeving is vereist. (zie ook bij art. 87 AVG)	
	Toestemming		
28	Indien de verwerkingsactiviteiten zijn gebaseerd op toestemming: is de toestemming vrij, specifiek, op informatie gebaseerd en ondubbelzinnig gegeven door de betrokkene?	N.v.t.	
29	Is de toestemming gegeven door middel van een duidelijke actieve handeling?	N.v.t.	
30	Is of wordt bijgehouden hoe en wanneer de betrokkene toestemming heeft gegeven?	N.v.t.	
31	Heeft de betrokkene de mogelijkheid om toestemming op ieder moment in te trekken en zonder negatieve gevolgen?	N.v.t.	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
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?	N.v.t.	
33	Wordt toestemming bij de situatie in de vorige vraag gevraagd door de persoon die ouderlijke verantwoordelijkheid voor het kind draagt?	N.v.t.	
	Transparantie		
34	Indien de persoonsgegevens direct bij de betrokkene worden verzameld; welke informatie wordt ten tijde van de verzameling gecommuniceerd?	Tijdens de aanmelding van de betrokkene worden persoonsgegevens en bijzondere persoonsgegevens gevraagd en geregistreerd. Tevens wordt de procedure (inc. werkwijze) en doel van de verwerking uitgelegd.	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.
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?	In het kader van contactopsporing wroden persoonsgegevens (naam, telnr en emailadres) van de contacten van de indexpatiënt verkregen van deze laatste. Bij het contacteren van de contacten wordt het doel van de verwerking (het hele traject) uitgelegd en hun gegevens nog eens gecontroleerd.	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.
36	Is het privacy statement geschreven in duidelijke bewoordingen en makkelijk vindbaar voor de betrokkenen?	Het privacy statement van de organisatie is te vinden op de website van de GGD. De privacy verklaring van de afdeling Infectieziekten wordt op dit moment door de privacy officer opgesteld.	
37	Indien de verwerking betrekking heeft op een samenwerkingsverband waarbij meerdere verwerkingsverantwoordelijken betrokken zijn, worden de relevante afspraken dan duidelijk gecommuniceerd aan de betrokkenen?	N.v.t.	
	Deel 4 - Rechten van betrokkenen		
38	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op inzage?	Ja	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.
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.

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.
41	Kan worden voldaan aan een verzoek om dataportabiliteit?	N.v.t.; de verwerking is gebaseerd op een wettelijke plicht.	
42	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op bezwaar?	Ja	
43	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op beperking?	Ja	
44	Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig	Ja	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.
	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?	N.v.t.	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: - Op basis waarvan deze profielen worden opgesteld. - Welke beslissingen op welke wijze worden genomen op basis van de profielen. - Of uit profielen gevoelige informatie is af te leiden. 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: - Op basis waarvan deze profielen worden opgesteld. - Welke beslissingen op welke wijze worden genomen op basis van de profielen. - Of uit profielen gevoelige informatie is af te leiden. Zorg er ook voor dat indien nodig betrokkenen geïnformeerd worden over deze profilering en
	Deel 5 - Doelbinding & proportionaliteit		
48	Worden de persoonsgegevens gebruikt voor een ander doel dan waarvoor zij verzameld zijn?	Nee	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. U wordt geadviseerd na te gaan of het doel op andere wijze kan worden gerealiseerd.
49	Indien de vorige vraag met 'ja' is beantwoord: is het doel waarvoor de persoonsgegevens verwerkt gaan worden verenigbaar met het oorspronkelijke doel?	N.v.t.	
50	Worden de persoonsgegevens gebruikt voor een ander doel dat niet specifiek is omschreven?	Nee	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.
51	Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?	Nee. Gegevens worden per patiënt verzameld en alszodanig doorgestuurd naar het RIVM.	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, de verwerking van persoonsgegevens wordt gebruikt voor (administratief) afhandeling van de melding; het terugkoppelen van testresultaten en eventueele follow-up (surveillance).	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.

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, het doel is bestrijden en voorkomen van infectieziekten (COVID-19 in dit geval). Dit staat in redelijke verhouding tot de impact voor de persoonlijke levenssfeer van de betrokkene.	
	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. 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?	Nee, het doel is bestrijden van infectieziekten (het uitvoeren van bron- en contactonderzoek; en bepalen van vervolg(behandel)stappen en monitoring; wat specifiek is voor iedere betrokkene.	Het verwerken van zo min mogelijk gegevens heeft een aantal voordelen: - De benodigde opslag en rekencapaciteit van uw computer systemen is lager, waardoor prestaties, hersteltijden en service niveaus kunnen worden verhoogd. - U zult minder gegevens te hoeven onderhouden en updaten en de kans op fouten wordt verkleind. Bovendien loop uw organisatie compliance risico's als u te veel gegevens voor het doel verzamelt.
55	Zijn alle persoonsgegevens noodzakelijk om het beoogde doel te bereiken?	Ja, zie ook 54.	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.	Ja. Alleen geautoriseerde personen hebben toegang tot het verzamelen van persoonsgegevens. De noodzakelijke persoonsgegevens zijn aangemerkt als verplichte velden. Autorisatie is geregeld via GGD GHOR ID-manager op basis van AD-groepen (Automatisering beheert de autorisatiematrix).	
	Deel 7 - Opslagbeperkingen		
57	Worden de persoonsgegevens verwijderd op het moment dat zij niet meer noodzakelijk voor het bereiken van het doel?	Voglens het wettelijke bewaartermijn. Zie 12.	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.
58	Op welke manier wordt gerealiseerd dat de data daadwerkelijk worden verwijderd/geanonimiseerd?	Procedure voor verwijdering opstellen.	
59	Indien geen bewaartermijnen zijn gedefinieerd, zijn er maatregelen genomen om de persoonsgegevens desalniettemin te verwijderen?	Bewaartermijnen conform Wpg (5 jaar, art. 29).	
	Deel 8 - Beveiliging, integriteit en vertrouwelijkheid		
60	Zijn er op basis van de VRA extra maatregelen nodig, naast de BIG maatregelen?	Nee. BIV-rating is ingevuld in de inventarisatiesheet van IZB; 3.BIA. (Zie ook risico's en maatregelen).	
61	Is voor dit proces aangesloten bij een goedgekeurde gedragscode? Zo ja, vermeld de gedragscode.	N.v.t.	Let op: Op dit moment is een dergelijke gedragscode nog niet afgesloten, dus hierbij kan niet worden aangesloten.
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, geautoriseerde toegang via persoonlijk inlogcode: er wordt een AD-account via ID-manager van GGD GHOR geregeld (Automatisering beheert de autorisatiematrix).	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. Neem daarom maatregelen om ervoor te zorgen dat mensen alleen toegang hebben tot de gegevens die zij
	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.	Verlies van vertrouwelijkheid.	
66	Hoe groot is de kans dat de omschreven risico's zich voordoen?	Minimaal, alleen geautoriseerden hebben toegang tot de data. Er is een lijst van medewerkers die toegang hebben tot de data. Tevens is in het systeem te traceren wie en wanneer is de data geraadpleegd/ingelogd.	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.	Laag	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.	Duidelijke procedures, werkinstructies en richtlijnen om risico's zoveel mogelijk uit te sluiten zijn vastgelegd en beschikbaar voor gebruikers.
	Deel 10 - Ingewonnen advies	
69	Is er advies ingewonnen van de Privacy Officer (PO) bij het uitvoeren van deze DPIA?	Ja
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, niet van toepassing.
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.	Nee, de verwerkingsactiviteit wordt uitgevoerd op basis van een wettelijke verplichting.
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.

Juridische toelichting

Een DPIA moet een systematische beschrijving bevatten van de beoogde verwerkingen (art. 35 lid 7, onder a AVG).

Een DPIA moet een systematische beschrijving bevatten van de verwerkingsdoeleinden (art.35 lid 7, onder a AVG).

Een DPIA moet een systematische beschrijving bevatten van de verwerkingsdoeleinden (art.35 lid 7, onder a AVG).

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.

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.

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)

"*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).
Let op: bewaartermijnen zijn iets anders dan archief termijnen.

Bijvoorbeeld: College B&W, externe partijen etc. Dit kunnen gezamenlijke verantwoordelijken zijn, maar ook keten partners.

Art. 28 AVG stelt het verplicht om met verwerkers een verwerkingsovereenkomst af te sluiten. De gemeente Amsterdam heeft een model verwerkersovereenkomst ontwikkeld.

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.

Je mag persoonsgegevens pas verwerken als er een rechtmatige grondslag voor aanwezig is (art. 5 en 6 AVG).

De AVG kent de volgende grondslagen:
a. ondubbelzinnige toestemming van de betrokkene,
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;
c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e. de verwerking is noodzakelijk voor de vervulling van 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;
f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die

"*Een verwerking die noodzakelijk is in het kader van een overeenkomst of een voorgenomen overeenkomst, dient rechtmatig te zijn*" overweging 44 AVG.

"*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.

"*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.

"*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*

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 betrokkene kunnen met name zwaarder wegen dan het belang van de verwerkingsverantwoordelijke wanneer persoonsgegevens worden verwerkt in omstandigheden waarin de betrokkenen redelijkerwijs geen verdere verwerking verwachten Aangezien het aan de wetgever staat om de rechtsgrond voor persoonsgegevensverwerking door overheidsinstanties te creëren, mag die rechtsgrond niet van toepassing zijn op de verwerking door overheidsinstanties in het kader van de uitvoering van hun taken* " Overweging 47 AVG.

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.

"*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)

"*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, geinformeerd en ondubbelzinnig met de verwerking van persoonsgegevens instemt"* (overweging 32 AVG).

Toestemming moet aantoonbaar zijn gegeven (art. 7 AVG).

" *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)

"[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).

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

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

"*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)

"*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)

"*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)

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.

"*De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen*" (Art. 16 AVG).

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.

"*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).

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.

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).

"*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).

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.

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).

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.

"*Persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd ( )*" (art. 5, lid 1 onder d AVG).

"*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)

Persoonsgegevens mogen alleen worden verzameld voor een welbepaald uitdrukkelijk omschreven en gerechtvaardigd doel (art. 5, lid 1 onder b AVG).

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 AVG)

Persoonsgegevens mogen alleen worden verzameld voor een welbepaald uitdrukkelijk omschreven en gerechtvaardigd doel (art. 5, lid 1 onder b AVG).

Dit kan bijvoorbeeld worden aangetoond met empirisch onderzoek of op basis van ervaringen uit het verleden.

"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).

"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.

"*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)

"*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).

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.

"*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)

"*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).

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;
ongeoorloofde ongedaan making van pseudonimisering; of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie.

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.

Voor GGD geldt dat eerst advies ingewonnen moet worden bij de Privacy Officer. De Privacy Officer wint advies in bij de FG als dat nodig mocht zijn. Neem het advies van de PO op bij de DPIA rapportage, in tab 4.

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.

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.

"*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)

Op dit moment zijn nog geen concrete voorbeelden bekend van een voorkomend geval waarbij betrokkenen om hun mening moet worden gevraagd.

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.

Nr.	Verwerking
1	[omschrijving van de verwerking]
2	Uitvoeren van bron- en contactonderzoek t.b.v. COVID-19, inclusief automatische rapportage aan het RIVM.
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	

Categorie persoonsgegeven	Type persoonsgegeven	Categorie betrokkenen
[welke persoonsgegevens worden er gebrukt voor deze verwerking? Bijv. Naam, adres, woonplaats, telefoonnummer, locatie, klantnummer etc.]	[Normaal, gevoelig, en/of bijzonder]	[van wie worden gegevens verwerkt? Bijvoorbeeld: inwoners, medewerkers, vergunninghouders etc]
identificerende persoonsgegevens: naam, geboortedatum, geslacht, adres woonplaats, telefoonnummer, e-mailares. Bijzondere persoonsgegevens: BSN nummer, testuitslagen (gezondheidsgegevens)	Normaal, gevoelig en bijzonder	Burgers, patiënten, zorgprofessionals

Doel	Applicatie	Bewaartermijn
[geef aan waarom de gegevens worden verwerkt]	[noem eventueel een gebruikt applicatie]	[Geef aan wat de bewaartermijn is, of hoe die wordt bepaald.]
infectieziektebestrijding conform de wet publieke gezondheid (Wpg).	HPZone	5 jaar conform Wpg

DPIA advies Privacy Officer

DPIA advies AP

DPIA visie betrokkenen