GGD Amsterdam Privacybeleid

Versie 1.2

Inhoudsopgave

1. Inleiding 3

1.1. Doelstelling GGD Amsterdam Privacybeleid 3
1.2. Reikwijdte GGD Amsterdam Privacybeleid 3
1.3. Juridisch kader 3

2. Begrippen 4

3. Verantwoordelijkheden 6

4. Algemeen beleid gebruik van persoonsgegevens 8

4.1. GGD Amsterdam heeft een grondslag nodig voor verwerking persoonsgegevens 8
4.2. GGD Amsterdam voldoet aan aanvullende voorwaarden bij vragen toestemming 8
4.3. GGD Amsterdam stelt vooraf doeleinden voor verwerking vast 9
4.4. Gebruik van bijzondere persoonsgegevens is aan strikte regels onderworpen 10
4.5. Data Protection Impact Assessment wordt uitgevoerd om privacy te verhogen 10
4.6. Dataminimalisatie 10
4.7. GGD Amsterdam controleert periodiek de kwaliteit van persoonsgegevens 11
4.8. Verwerkingen worden intern gedocumenteerd 11
4.9. Betrokkenen worden geïnformeerd 12
4.10. Rechten van betrokkenen worden gecommuniceerd en gefaciliteerd 13
4.11. Persoonsgegevens worden bewaard in aangewezen IT-systemen 13
4.12. Persoonsgegevens worden niet langer bewaard dan nodig 14
4.13. De Ondernemingsraad wordt betrokken bij privacy onderwerpen 14
4.14. Persoonsgegevens worden adequaat beveiligd 15
4.15. Datalekken worden gemeld 15
4.16. Medewerkers krijgen training over privacy 15
4.17. GGD Amsterdam communiceert over privacy naar en met haar stakeholders 16
4.18. Gebruik van cookies en andere tracking methodes wordt geregeld in Richtlijnen 16
4.19. Verwerkersovereenkomst wordt gesloten met de verwerker 16
4.20. Verwerving persoonsgegevens van derden 17
4.21. Persoonsgegevens worden nooit aan derden verkocht 17
4.22. Persoonsgegevens worden in beginsel binnen de Europese Economische Ruimte verwerkt 18
4.23. Binnen samenwerkingsverbanden wordt eenzelfde privacyniveau verlangd 18

Versiebeheer 20

Bijlage 1: Wet- en regelgeving 21

1. Inleiding

1.1. Doelstelling GGD Amsterdam Privacybeleid

De Geneeskundige Gezondheidsdienst Amsterdam (GGD) bewaakt en bevordert actief de gezondheid van de bevolking in het werkgebied Amsterdam, Aalsmeer, Amstelveen, Diemen, Ouder-Amstel en Uithoorn. Om als openbare gezondheidsdienst op een goede manier de zorg aan bewoners te kunnen verlenen wordt een enorme hoeveelheid persoonsgegevens verwerkt, in de meeste gevallen ook bijzondere persoonsgegevens. GGD Amsterdam belooft als professionele gezondheidsdienst zorgvuldig en verantwoord om te gaan met de persoonsgegevens van alle betrokkenen en de persoonsgegevens op een rechtmatige manier te verwerken. Niet alleen om aantoonbaar compliant te zijn[1], maar vooral omdat GGD Amsterdam het belangrijk vindt om zorgvuldig om te gaan met de gegevens van anderen.

Het GGD Amsterdam Privacybeleid dient als handvat voor alle GGD Amsterdam medewerkers die zich bezighouden met de verwerking van persoonsgegevens. Het beleid beschrijft de uitgangspunten met betrekking tot het gebruik van persoonsgegevens van alle betrokkenen.

1.2. Reikwijdte GGD Amsterdam Privacybeleid

Het GGD Amsterdam privacybeleid is van toepassing op alle persoonsgegevens die door GGD Amsterdam worden verwerkt, in geheel of gedeeltelijk geautomatiseerde verwerking en op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Hieronder vallen dus ook papieren dossiers, mits deze in een gestructureerd bestand zijn opgenomen.

Het privacybeleid heeft betrekking op de verwerking van alle persoonsgegevens van alle betrokkenen, dus zowel van alle cliënten, als van alle medewerkers en leveranciers.

1.3. Juridisch kader

De uitgangspunten in dit beleidsstuk zijn gebaseerd op wettelijke normen. De basis van de Nederlandse privacywetgeving ligt in Artikel 10 van de Grondwet en artikel 8 van het Europese Verdrag voor de Rechten van de Mens. De Algemene verordening gegevensbescherming (Avg) en de Uitvoeringswet Algemene verordening gegevensbescherming (Uavg) vormen de uitwerking hiervan. Per 1 juli 2020 is bovendien De Wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg van kracht.

GGD Amsterdam heeft daarnaast te maken met de een groot aantal andere wetten die van invloed is op de verwerking van persoonsgegevens. Zie Bijlage 1: Wet- en regelgeving.

[1] Zoals vereist op grond van Artikel 5 lid 2 AVG

2. Begrippen

In dit beleidsstuk worden specifieke begrippen gebruikt met betrekking tot de verwerking van persoonsgegevens. Sommige vloeien voort uit de wet, terwijl andere zijn opgesteld ten behoeve van dit GGD Amsterdam Privacybeleid. Hieronder staan de belangrijkste begripsbepalingen opgesomd.

Persoonsgegevens: Dit zijn alle gegevens die afzonderlijk of in combinatie direct of indirect herleidbaar zijn naar een natuurlijk persoon (dit beleid is dan ook niet van toepassing op rechtspersonen of overleden personen). Voorbeelden zijn: naam, adres, woonplaats, geboortedatum, emailadres, huwelijkse staat, maar ook bijvoorbeeld een ip-numer (een unieke code voor een computer).

Bijzondere persoonsgegevens: Dit zijn gegevens over etnische achtergrond, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, gegevens over het lidmaatschap van een vakbond, en verwerking van genetische en biometrische gegevens (met het oog op de unieke identificatie), gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele geaardheid. Verwerking van deze gegevens is verboden, behalve als er zich uitzonderingsgevallen voordoen.

Verwerking: Hiermee wordt bedoeld *"één of meerdere bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens"*. In principe is dus iedere handeling die uitgevoerd wordt met een persoonsgegeven een verwerking.

Betrokkenen: Degene op wie een persoonsgegeven betrekking heeft. Met andere woorden: van 'wie de persoonsgegevens zijn'.

Verwerkingsverantwoordelijke: De Verantwoordelijke is de natuurlijke persoon of rechtspersoon die het doel en de middelen van de verwerking van de persoonsgegevens vaststelt. De Verantwoordelijke geeft antwoord op de vraag of er gegevens worden verwerkt en zo ja, welke verwerking, van welke persoonsgegevens en voor welk doel. Daarnaast beslist de Verantwoordelijke op welke wijze deze gegevensverwerking zal plaatsvinden.

Verwerker: De Verwerker is een derde partij die voor de Verantwoordelijke persoonsgegevens verwerkt. Dit betekent dat de Verwerker volgens de instructies van de Verantwoordelijke en onder diens (uitdrukkelijke) verantwoordelijkheid persoonsgegevens verwerkt.

Data Privacty Impact Assessment (DPIA): Een instrument (een vragenlijst) dat wordt gebruikt om de privacy risico's van een voorgenomen verwerking van persoonsgegevens of een wijzing van een bestaande verwerking van persoonsgegevens in kaart te brengen, teneinde de eventueel naar voren gekomen risico's te adresseren.

Beschikbaarheid, Integriteit, Vertrouwelijkheid-classificatie (BIV-classificatie/ er BBN niveau's 1/m 3): Een instrument (een vragenlijst) dat wordt gebruikt om te bepalen welk beveiligingsniveau dient te worden gehanteerd, met betrekking tot een verwerking van persoonsgegevens, om de beschikbaarheid, integriteit en vertrouwelijkheid van de persoonsgegevens en de (IT) systemen waarmee de persoonsgegevens worden verwerkt, op passende wijze te waarborgen.

Bewaartermijn: De maximale termijn waarbinnen gegevens mogen worden bewaard. Dit kan zijn voorgeschreven door een wettelijke bepaling of worden afgebakend door een bedrijfsnoodzaak.

Inbreuk persoonsgegevens ('datalek'): Een inbreuk in verband met persoonsgegevens, beter bekend als een datalek, is een inbreuk die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Het is

voor de kwalificatie als inbreuk niet relevant dat er kwade opzet in het spel is. Hoewel een hack van systemen waarbij persoonsgegevens worden buitgemaakt een uitgesproken voorbeeld is van een datalek, kunnen ook gegevens die op een verloren laptop staan of een afgesloten website met persoonsgegevens die per ongeluk openstaat ook kwalificeren als een datalek. Voor meer informatie kan worden gekeken in het *GGD Amsterdam Datalek Protocol*. Inbreuken met een hoog risico voor de betrokkenen worden binnen 72 uur gemeld bij de Autoriteit Persoonsgegevens.

3. Verantwoordelijkheden

Om een zorgvuldige verwerking van persoonsgegevens te waarborgen heeft GGD Amsterdam een privacy organisatiestructuur ingericht. In hoofdlijnen zijn de verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens als volgt belegd:

1. Compliance aan privacywetgeving is de (gemandateerde) verantwoordelijkheid van de Directie van GGD Amsterdam. Zij belegt afgeleide verantwoordelijkheden bij afdelingshoofden middels het Onder mandaat GGD Amsterdam 2019..
2. Een team van verschillende functionarissen zoals de Programmamanager en assisitent, Privacy Officers, Information Security Officers, privacycontactpersonen, procesmanagers, adviseur informatiebeheer en informatiemanager werkt samen en is verantwoordelijk voor de borging van privacy en informatiebeveiliging, het omgaan met en beoordelen van eventuele datalekken, het (laten) uitvoeren van audits, het organiseren van bewustwordingsactiviteiten en het beheer van het GGD Amsterdam Privacybeleid. Dit beleid wordt ten minste jaarlijks gecontroleerd door de Privacy Officer op juistheid en actualiteit, zonodig aangepast en vastgesteld door het DPGA-team.
3. Het inbedden van beveiligingsmaatregelen in de ict systemen (privacy by design) is een verantwoordelijkheid van de lijnverantwoordelijken. Onder andere door het uitvoeren van Data Protection Impact Assessments (DPIA)
4. De primaire verantwoordelijkheid voor de omgang met persoonsgegevens ligt bij de medewerkers van GGD Amsterdam. Dit betekent dat iedere medewerker binnen GGD Amsterdam verantwoordelijk is voor het toepassen van de geldende privacyregels binnen hun werkzaamheden. Ook het voldoen aan verzoeken van betrokkenen is primair de verantwoordelijkheid van de bij het proces betrokken medewerker.
5. De Privacy Officer is verantwoordelijk voor het implementeren en bewaken van het privacybeleid binnen GGD Amsterdam. Daarnaast speelt de Privacy Officer ook een belangrijke rol op de werkvloer, zo heeft hij of zij net als de Information Security Officer een adviserende rol richting de afdelingen en kan hij of zij vragen beantwoorden. De Privacy Officer beoordeelt verwerkersovereenkomsten en is verantwoordelijk voor de behandeling en opvolging van onderzoek en informatieverzoeken door bevoegde overheidsinstanties.
6. De Information Security Officer is de spin in het web als het gaat om de beveiliging van informatie binnen GGD Amsterdam. Hij is verantwoordelijk voor het implementeren van en toezicht houden op het informatiebeveiligingsbeleid binnen GGD Amsterdam. De Information Security Officer heeft een centrale rol in het beheren van alle processen die daarmee te maken hebben en moet daarbij voldoen aan een set van organisatorische en technische beveiligingsmaatregelen die geïmplementeerd en beheerd dient te worden.
7. De verwerking van persoonsgegevens wordt pas gestart nadat door de Information Security Officer het beveiligingsniveau is vastgesteld op basis van BIV-classificatie en nadat op basis van een DPIA en een BIV-classificatie/BBN-niveau een passend beveiligingsniveau volgens de richtlijnen van de NEN7510 (norm voor informatiebeveiliging in de zorg) gerealiseerd is.
8. De Technical Security Officer beoordeelt samen met de Privacy Officer gemlede inbreuken op de informatiebeveiliging.
9. De privacycontactpersoon is het eerste aanspreekpunt binnen de afdeling op het gebied van privacybescherming, informatiebeveiliging en informatiebeheer en adviseert het afdelingshoofd over en draagt zorg voor het verspreiden van kennis over privacybescherming, informatiebeveiliging en informatiebeheer. Daarnaast adviseert de privacycontactpersoon collega's en afdelingshoofd over verwerkingsregister, verwerkersovereenkomst, DPIA, beveiliging (BIV-triade, datalekprotocol), privacy by design/default, rechten van betrokkenen, en privacy cultuur.
10. De Functionaris Gegevensbescherming van de gemeente Amsterdam houdt toezicht op GGD Amsterdam. De onafhankelijke Functionaris Gegevensbescherming heeft een adviserende rol m.b.t.

privacy gerelateerde onderwerpen, maar verricht ook controlerende of toezichthoudende werkzaamheden binnen GGD Amsterdam.

11. De Commissie Persoonsgegevens Amsterdam (CPA) adviseert over het privacybeleid van de gemeente en de uitvoering daarvan. Daarnaast adviseert de commissie de ambtelijke organisatie bij complexe en/of politiek gevoelige kwesties rondom persoonsgegevens. De CPA signaleert wat er binnen de gemeente speelt op het gebied van persoonsgegevens en brengt dit onder de aandacht van het gemeentebestuur en het management van de ambtelijke organisatie.

4. Algemeen beleid gebruik van persoonsgegevens

Het *GGD Amsterdam Privacybeleid* bestaat uit een aantal beleidsregels, die toelichting geeft op de wijze waarop bij GGD Amsterdam met persoonsgegevens wordt omgegaan. Per beleidsregel wordt toegelicht aan welke eisen voldaan moet worden en wie daarvoor verantwoordelijk is.

4.1. GGD Amsterdam heeft een grondslag nodig voor verwerking persoonsgegevens

Wanneer er met persoonsgegevens wordt gewerkt binnen GGD Amsterdam, dient volgens de wet altijd een zogeheten grondslag te bestaan.[2] Dit betekent dat GGD Amsterdam altijd een geldige reden moet hebben om persoonsgegevens te mogen gebruiken.

De Avg geeft de volgende zestal mogelijke redenen (ofwel: grondslagen) voor de verwerking van persoonsgegevens. Hieronder staat de limitatieve lijst. Er zit geen volgordelijkheid in deze lijst; per situatie moet bekeken worden welke van de onderstaande grondslagen van toepassing zijn.

> Tip! Er wordt vaak als eerste gedacht aan toestemming als men naar een grondslag zoekt. Dit terwijl er in veel gevallen betere alternatieve grondslagen voorhanden zijn, zoals de uitvoering van een overeenkomst. Kijk daarom altijd éérst in hoeverre een van de andere genoemde grondslagen op de verwerking van persoonsgegevens van toepassing zijn. Staat er niets tussen? Vraag dan toestemming en houdt rekening met de voorwaarden in artikel 4.2.

De verwerking door GGD Amsterdam is alleen rechtmatig als aan ten minste een van de onderstaande voorwaarden is voldaan:

1. De betrokkene heeft toestemming gegeven voor het gebruik van persoonsgegevens voor één of meer specifieke doelen. *Meer informatie hierover in paragraaf 4.2.*
2. De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst tussen GGD Amsterdam en de betrokkene. *Denk hierbij aan een zorgovereenkomst of een arbeidsovereenkomst.*
3. De gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan GGD Amsterdam moet voldoen. Denk bijvoorbeeld *aan verplichtingen op grond van de Wet publieke gezondheid.*
4. De gegevensverwerking is van levensbelang voor de betrokkene. *Denk hierbij aan een direct noodgeval voor de betrokkene, bijvoorbeeld wanneer deze zelf niet in staat is informatie of toestemming te geven.*
5. De gegevensverwerking is noodzakelijk voor de uitoefening van een publiekrechtelijke taak door het bestuursorgaan waaraan de gegevens worden verstrekt.
6. **Als overheidsorganisatie kan GGD Amsterdam zich niet baseren op de grondslag van een gerechtvaardigd belang.**

4.2. GGD Amsterdam voldoet aan aanvullende voorwaarden bij vragen toestemming

Indien er om toestemming moet worden gevraagd, omdat andere grondslagen niet mogelijk zijn, moet rekening worden gehouden met de volgende voorwaarden:

1. GGD Amsterdam zorgt ervoor dat de toestemming duidelijk en transparant is waardoor de betrokkene snapt dat hij accepteert dat persoonsgegevens van hem of haar worden verwerkt.

[2] Artikel 5 lid 1 sub 1 jo Artikel 6 lid 1 AVG.

Stilzwijgende toestemming, of toestemming door het gebruik van al aangevinkte vakjes laten onvoldoende zien dat de betrokkene op een actieve manier de toestemming heeft gegeven en mogen dus niet worden gebruikt.

2. Het schriftelijk vragen van toestemming is niet vereist. Maar omdat de bewijslast voor toestemming bij GGD Amsterdam ligt wordt de toestemming wél schriftelijk vastgelegd.
3. Toestemming moet ondubbelzinnig worden gegeven. Dit betekent dat deze toestemming niet gebundeld kan worden met toestemming voor andere zaken, d.w.z. andere zaken dan de verwerking van persoonsgegevens. Zorg er dus voor dat GGD Amsterdam expliciet kan aantonen dat de cliënt akkoord gaat met de verwerking van zijn persoonsgegevens.
4. Eenmaal gegeven toestemming mag altijd weer worden ingetrokken. GGD Amsterdam zorgt er daarom voor dat de betrokkene altijd zijn toestemming kan intrekken. Het intrekken van toestemming brengt niet met zich mee dat de eerdere verwerking onrechtmatig was.
5. GGD Amsterdam gebruikt toestemming niet als grondslag voor de verwerking van persoonsgegevens van haar werknemers, omdat er een gezagsverhouding bestaat tussen GGD Amsterdam en de medewerker.

4.3. GGD Amsterdam stelt vooraf doeleinden voor verwerking vast

Een belangrijk principe binnen privacywetgeving is doelbinding. Kort gezegd houdt dit in dat voor iedere verwerking van persoonsgegevens vooraf moet worden vastgesteld met welk doel de persoonsgegevens worden gebruikt. De doeleinden moeten heel concreet worden omschreven. De doeleinden bepalen welke persoonsgegevens je mag verwerken, hoe lang je gegevens mag gebruiken en waarvoor je de gegevens in de toekomst mag gebruiken. In de *GGD Amsterdam Privacystrategie* is dan ook het volgende uitgangspunt opgenomen over het gebruik van persoonsgegevens binnen GGD Amsterdam:

“GGD Amsterdam stelt vooraf de doeleinden voor de verwerking van persoonsgegevens vast, en gebruikt persoonsgegevens niet voor andere doeleinden dan is vastgesteld.”

Denk goed na waarvóór je de persoonsgegevens nodig hebt. Houd hierbij rekening met de volgende vereisten:

1. GGD Amsterdam mag slechts persoonsgegevens verzamelen voor duidelijk omschreven en gerechtvaardigde doeleinden. GGD Amsterdam stelt vooraf de doeleinden van de verwerking vast en legt deze vast in het verwerkingsregister. Dat betekent in de praktijk dat GGD Amsterdam voorafgaand aan de introductie van een nieuw(e) proces of applicatie moet vaststellen voor welke doeleinden zij de persoonsgegevens verzameld.
2. GGD Amsterdam informeert de betrokkene(n) vóór aanvang van de verwerking over de doeleinden van de verwerking.
3. GGD Amsterdam verwerkt persoonsgegevens niet voor andere doeleinden dan de doeleinden waarvoor de persoonsgegevens zijn verkregen. Dit betekent dat GGD Amsterdam zich houdt aan de doeleinden die zij heeft gecommuniceerd aan de betrokkene(n). Als GGD Amsterdam de persoonsgegevens die zijn verzameld voor doel X op een later tijdstip voor doel Y wil gebruiken, moet zij de betrokkene(n) opnieuw informeren, en indien van toepassing, opnieuw toestemming vragen. Tenzij het doel van de verdere verwerking verenigbaar is met het doel waarvoor de gegevens aanvankelijk zijn verzameld en de betrokkene dit redelijkerwijs kon verwachten. Bijvoorbeeld: Je sluit een arbeidsovereenkomst, daar spreek je een salaris in af en de werkgever is verplicht om loonheffing daarover af te dragen.

4.4. Gebruik van bijzondere persoonsgegevens is aan strikte regels onderworpen

Bijzondere persoonsgegevens worden als gevoelig beschouwd en zijn daarom door de wetgever extra beschermd. Het risico op misbruik en de impact bij dit soort gegevens is ook groter dan bij 'normale' persoonsgegevens. Het verwerken is verboden, tenzij er aan een wettelijke voorwaarde wordt voldaan, zoals het verstrekken van gezondheidszorg.

GGD Amsterdam verlangt dat bijzondere persoonsgegevens alleen worden verwerkt als dat noodzakelijk is en er voldoende waarborgen in acht zijn genomen:

1. Naast de (wettelijke) grondslag en vooraf bepaalde doeleinden voor de verwerking moet er een wettelijke uitzondering aanwezig zijn op het verbod van de verwerking van bijzondere persoonsgegevens, zoals neergelegd in artikel 9 van de Avg. GGD Amsterdam informeert betrokkenen hier tijdig over.
2. Medewerkers moeten ingelicht worden over het toegestane gebruik van bijzondere persoonsgegevens. De aandacht binnen GGD Amsterdam over het verwerken van bijzondere gegevens van medewerkers ligt vooral op het vastleggen van gezondheidsgegevens. Denk hierbij bijvoorbeeld aan de vraag of informatie over ziekte wel moet worden vastgelegd in notitievelden e.d.
3. GGD Amsterdam gebruikt geen Burgerservicenummers buiten de specifiek in de wet genoemde doeleinden.

4.5. Data Protection Impact Assessment wordt uitgevoerd om privacy te verhogen

Als GGD Amsterdam besluit om een nieuw systeem of proces te implementeren waardoor persoonsgegevens worden verwerkt moeten vooraf de privacyrisico's in kaart worden gebracht. Als al vroeg in het ontwikkelproces risico's worden geconstateerd, kunnen tijdig privacy verhogende maatregelen worden genomen. Het in kaart brengen van de risico's en het bedenken van privacy verhogende maatregelen is mogelijk met behulp van de *GGD Amsterdam Data Protection Impact Assessment* (hierna: DPIA). De betreffende afdeling is verantwoordelijk voor het uitvoeren van de DPIA, de privacycontactpersoon wint bij de Privacy Officer advies in.

Voordat een DPIA wordt gestart, wordt eerst met behulp van de *GGD Amsterdam DPIA Risico-inschatting* bepaald of een *Verkorte DPIA* of een *Volledige DPIA* moet worden uitgevoerd. Een *Verkorte DPIA* moet worden uitgevoerd voor applicaties of initiatieven waarbij op basis van de risico inschatting een laag risico is vastgesteld. Een *Volledige DPIA* moet worden uitgevoerd wanneer een hoog risico wordt vastgesteld. De beide DPIA's bestaan uit een vragenlijst die door ICT moet worden ingevuld.

Op basis van de antwoorden wordt vervolgens een analyse gemaakt van de (mogelijke) specifieke privacyrisico's voor betrokkene(n). Op basis van deze analyse worden privacy verhogende maatregelen voorgesteld, die door de verantwoordelijke van het betreffende proces binnen GGD Amsterdam worden doorgevoerd.

4.6. Dataminimalisatie

De wet zegt dat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, "toereikend, ter zake dienend en beperkt tot wat noodzakelijk is." Dit wordt ook wel het principe van dataminimalisatie genoemd. Dit betekent dat GGD Amsterdam bij het uitoefenen van haar werkzaamheden zo min mogelijk persoonsgegevens moet gebruiken. Dit principe zorgt ervoor dat het privacyrisico voor de betrokkene wordt verminderd, simpelweg omdat er minder gegevens van diegene aanwezig zijn. Bij een eventueel datalek is het risico van de betrokkene daarom kleiner.

Naast dataminimalisatie kan ook worden gekeken naar het anonimiseren of pseudonimiseren van gegevens, waardoor gegevens niet of bijna niet meer te herleiden zijn naar een individueel persoon. Hierdoor zijn de gegevens niet meer te kwalificeren als persoonsgegevens. Dit is met name van belang als er analyses worden uitgevoerd op data, of als gegevens worden gedeeld met derden.

Met betrekking tot dataminimalisatie gelden binnen GGD Amsterdam de volgende uitgangspunten:

1. GGD Amsterdam verwerkt niet meer persoonsgegevens dan noodzakelijk voor de doeleinden waarvoor zij zijn verzameld.
2. GGD Amsterdam bekijkt, voordat een systeem of proces operationeel is, of er minder persoonsgegevens kunnen worden gebruikt, en toch het zelfde doel kan worden bereikt.
3. GGD Amsterdam bekijkt voordat een systeem of proces operationeel is of de persoonsgegevens kunnen worden geanonimiseerd terwijl hetzelfde doel kan worden bereikt.
4. Punt 2 en 3 kunnen worden gecheckt tijdens het uitvoeren van de *GGD Amsterdam Data Protection Impact Assessment*.

4.7. GGD Amsterdam controleert periodiek de kwaliteit van persoonsgegevens

De wet stelt dat persoonsgegevens, gelet op doeleinden waarvoor zij worden verzameld en vervolgens worden verwerkt, juist zijn en zonodig worden geactualiseerd. Op GGD Amsterdam ligt geen absolute garantie om ervoor te zorgen dat de gegevens juist en nauwkeurig zijn, alle redelijke maatregelen moeten worden getroffen om ervoor te zorgen dat de gegevens juist zijn.

Het belang van het hebben van juiste persoonsgegevens voor GGD Amsterdam is ten eerste het verkleinen van het veiligheidsrisico, ten tweede het verkleinen van het privacyrisico voor betrokkenen. Denk bijvoorbeeld aan de gevolgen voor betrokkenen indien de adresgegevens niet meer juist zijn, en brieven verkeerd worden bezorgd.

Het controleren van de juistheid en nauwkeurigheid van persoonsgegevens kan een arbeidsintensieve en tijdrovende kwestie zijn. De verantwoordelijkheid voor de controle op juistheid van de persoonsgegevens ligt bij de verantwoordelijke van het proces waarbinnen de betreffende verwerking plaatsvindt.

Daarnaast zorgt GGD Amsterdam er bij de ontwikkeling van nieuwe systemen of diensten ervoor dat de nodige maatregelen worden doorgevoerd die de kwaliteit en betrouwbaarheid van de persoonsgegevens verhogen.

4.8. Verwerkingen worden intern gedocumenteerd

In het kader van optimale controle met betrekking tot de verwerking van persoonsgegevens en om te voldoen aan de documentatieplicht van de AVG documenteert GGD Amsterdam al haar verwerkingen in een overzicht, het verwerkingsregister.

Het overzicht draagt ertoe bij dat de Privacy Officer goed zicht heeft op alle verwerkingen en daarmee gepaard gaande risico's. Dit levert een betere controle op bijvoorbeeld in het kader van de doeleinden van een verwerking. Als gegevens oorspronkelijk zijn verzameld voor een specifiek doel, dan mogen deze gegevens niet zomaar voor een compleet ander doeleinde worden ingezet tenzij deze in het verlengde ligt van het oorspronkelijke doel. Het overzicht biedt deze verduidelijking. Het overzicht moet aan de toezichthouder worden aangeboden als daarom wordt gevraagd.

Met betrekking tot het overzicht gelden binnen GGD Amsterdam de volgende uitgangspunten:

1. Elke nieuwe of wijziging van een verwerking binnen GGD Amsterdam wordt gemeld aan de Privacy Officer.

2. De Privacycontactpersoon documenteert elke nieuwe of wijziging van een verwerking van persoonsgegevens centraal en in een daarvoor bestemd register. Dit register omvat in ieder geval de volgende informatie:
   a) De naam van GGD Amsterdam, gezamenlijk verantwoordelijke, verwerker, of vertegenwoordiger, indien aanwezig.
   b) De naam en contactgegevens van de Privacy Officer.
   c) Het doel of de doeleinden van de verwerking.
   d) Een beschrijving van de categorieën van betrokkenen en van de gegevens of categorieën van gegevens die daarop betrekking hebben.
   e) De ontvangers of categorieën van ontvangers aan wie de gegevens kunnen worden verstrekt.
   f) De voorgenomen doorgiften van gegevens naar landen buiten de Europees Economische Ruimte.
   g) De voorgenomen bewaartermijnen van de verschillende categorieën persoonsgegevens.
   h) Een algemene beschrijving van de technische en organisatorische maatregelen (zoals bedoeld als in paragraaf 4.16. van dit Beleid) die GGD Amsterdam heeft genomen om de persoonsgegevens te beveiligen te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
3. De Privacy Officer is verantwoordelijk voor het actueel houden van het register.
4. Op verzoek van de Autoriteit Persoonsgegevens stelt de Privacy Officer dit overzicht ter beschikking.

4.9. Betrokkenen worden geïnformeerd

Uit de wet volgt dat GGD Amsterdam verplicht is om betrokkenen te informeren over de persoonsgegevens die zij van hem of haar verwerkt. Als dit niet zorgvuldig gebeurt, heeft dit tot gevolg dat de verwerking onrechtmatig is. Betrokkenen moeten goed en duidelijk worden geïnformeerd over de verwerking zodat de betrokkene weet dat wat voor persoonsgegevens van hem of haar worden verwerkt, door wie, en wat er vervolgens met de gegevens gebeurt. Op deze wijze wordt het voor de betrokkene mogelijk gemaakt om controle te blijven houden op zijn of haar persoonsgegevens. Een belangrijk uitgangspunt uit de strategie is dat dan ook dat betrokkenen op begrijpelijke en transparante wijze over het gebruik van hun persoonsgegevens worden geïnformeerd:

“GGD Amsterdam communiceert transparant en op een begrijpelijke wijze over het gebruik van persoonsgegevens en de rechten van betrokkenen.”

Om ervoor te zorgen dat binnen GGD Amsterdam altijd op een juiste wijze aan deze informatievoorziening wordt voldaan, gelden de volgende uitgangspunten:

1. GGD Amsterdam zorgt voor duidelijke, transparante en toegankelijke informatievoorzieningen voor betrokkenen met betrekking tot de verwerking van hun persoonsgegevens. Een voorbeeld van een dergelijke informatievoorziening is de privacyverkaring op de GGD Amsterdam website.
2. GGD Amsterdam stelt betrokkenen op de hoogte van het gebruik van hun persoonsgegevens vóór aanvang van de verwerking van de persoonsgegevens.
3. Betrokkenen worden geïnformeerd over ten minste:
   a) Naam en contactgegevens van de Functionaris Gegevensbescherming van GGD Amsterdam.
   b) De doeleinden van de verwerking.
   c) De bewaartermijn(en) van de desbetreffende persoonsgegevens. Als dit niet mogelijk is worden de criteria uiteengezet die ten grondslag liggen aan de bepaling van de bewaartermijn(en).
   d) De rechten die de betrokkene jegens GGD Amsterdam kan uitoefenen (recht op inzage, correctie, verwijdering, afscherming en portabiliteit van zijn of haar persoonsgegevens). Zie hiervoor het *GGD Amsterdam Protocol Rechten van betrokkenen.*
   e) Het recht van de betrokkene om een klacht neer te leggen bij de AP (en de contactgegevens van de AP).
   f) De (categorieën van) ontvangers aan wie de persoonsgegevens worden verstrekt.

4. GGD Amsterdam informeert de betrokkene in uitzonderingssituaties met aanvullende informatie. GGD Amsterdam verstrekt alle verdere informatie die, met inachtneming van de bijzondere omstandigheden waaronder de gegevens worden verzameld, nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen. Om vast te stellen in hoeverre extra geïnformeerd moet worden, hanteert GGD Amsterdam de volgende richtlijnen:
   a) Als het gebruik van de persoonsgegevens anders is dan de betrokkene zou verwachten, kan dit aanleiding zijn beter hierover te informeren. Verwacht een betrokkene bijvoorbeeld niet dat GGD Amsterdam in bepaalde gevallen persoonsgegevens aan de politie verstrekt, dan moet GGD Amsterdam de betrokkene specifiek over deze mogelijkheid informeren.
   b) Als de omstandigheden waaronder GGD Amsterdam de gegevens krijgt rechtvaardigen om extra te informeren. Als GGD Amsterdam persoonsgegevens van een andere organisatie krijgt, kan de informatieplicht zwaarder uitvallen dan wanneer GGD Amsterdam de gegevens rechtstreeks van de betrokkene hebt gekregen. De betrokkene is er immers niet altijd van op de hoogte dat die andere organisatie gegevens aan GGD Amsterdam heeft verstrekt.
   c) Zodra GGD Amsterdam de persoonsgegevens op zodanige manier gaat gebruiken dat de betrokkene daar (negatieve) gevolgen aan kan ondervinden. Denk aan situaties als gedrags- of big data analyses. Afhankelijk van de gevolgen van het gebruik persoonsgegevens voor de betrokkene, kan meer informatie noodzakelijk zijn.
   d) Hoe 'gevoeliger' de persoonsgegevens, hoe transparanter GGD Amsterdam over het gebruik zal moeten zijn. Denk aan het gebruik van medische gegevens, in een dergelijk geval is het extra belangrijk om de cliënt goed te informeren.

4.10. Rechten van betrokkenen worden gecommuniceerd en gefaciliteerd

Uit de wet volgt dat GGD Amsterdam verplicht is om, naast het zorgvuldig informeren van betrokkenen over de verwerking van persoonsgegevens, ook toe te lichten welke rechten de betrokkene heeft en hoe zij deze kan uitoefenen. Het gaat hier over het recht op inzage, het recht op correctie en/of verwijdering, het recht van verzet en het recht om een klacht in te dienen.

Doordat betrokkenen weten dat zij specifieke rechten hebben kunnen zij controleren hoe gegevens over hen worden verwerkt en bepaalde verwerkingen aanpassen, blokkeren of zelfs verwijderen. Hierdoor blijven zij greep houden op hun eigen persoonsgegevens.

Om de rechten van de betrokkenen te kunnen waarborgen gelden daarom de volgende uitgangspunten:

1. GGD Amsterdam stelt procedures en mechanismes in werking die ervoor zorgen dat betrokkenen deze rechten daadwerkelijk kunnen inroepen.
2. *Het GGD Amsterdam Protocol Rechten van betrokkenen* beschrijft hoe deze rechten in de praktijk worden gebracht. Deze beschrijving bevat de werkwijze om te reageren op verzoeken binnen de wettelijke termijnen, en wanneer noodzakelijk deze te honoreren. De beschrijving bevat ook een beschrijving van de noodzakelijke communicatie van GGD Amsterdam met derden aan wie de gegevens mogelijkerwijs zijn verstrekt.

4.11. Persoonsgegevens worden bewaard in aangewezen IT-systemen

Binnen GGD Amsterdam worden persoonsgegevens van cliënten, medewerkers, vrijwilligers, mantelzorgers e.d. zoveel mogelijk opgeslagen in de daartoe bestemde IT-systemen. Door locaties te specificeren waar het is toegestaan om persoonsgegevens op te slaan, is het makkelijker om controle te houden over de kwaliteit van de gegevens. De privacy van de betrokkenen kan hierdoor beter gewaarborgd worden. Daarnaast zijn deze systemen goed beveiligd tegen onbevoegde toegang en kennisname.

Daarom gelden de volgende uitgangspunten:

1. Binnen GGD Amsterdam geldt het principe dat (bijzondere) persoonsgegevens worden bewaard in de daarvoor bestemde IT-systemen. Persoonsgegevens mogen dus niet worden opgeslagen op de publieke en/of persoonlijke schijf, Outlook, USB-sticks, etc.
2. Open tekstvelden binnen IT-systemen dienen zo min mogelijk te worden gebruikt. Op deze manier wordt het risico op overbodige invoer van (bijzondere) persoonsgegevens beperkt. Denk hierbij aan het vastleggen van gegevens over ziekte e.d.
3. Als IT-systemen ontoereikend zijn, wordt direct contact opgenomen met de verantwoordelijke van het IT-systeem. De verantwoordelijke van het systeem zorgt er dan voor dat de persoonsgegevens alsnog op dit systeem of op een andere veilige locatie kunnen worden opgeslagen.

4.12. Persoonsgegevens worden niet langer bewaard dan nodig

De wet zegt over het bewaren van persoonsgegevens dat zij niet langer mogen worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren dan noodzakelijk voor de doeleinden waarvoor zij zijn verzameld. Dit betekent dat GGD Amsterdam zich zal moeten afvragen hoe lang zij de persoonsgegevens nodig heeft (en zal hebben) voor het verwezenlijken van de doeleinden van de verwerking. Met andere woorden, GGD Amsterdam zal bewaartermijnen voor verwerkingen en/of persoonsgegevens moeten vaststellen, rekening houdend met de geldende wet- en regelgeving. Deze worden vastgelegd in het verwerkingsregister.

Met betrekking tot het bewaren en vernietigen van persoonsgegevens gelden daarom de volgende uitgangspunten:

1. Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.
2. GGD Amsterdam stelt bij ieder proces vooraf de bewaartermijn vast conform zorgspecifieke en archiefwet- en regelgeving.
3. Wanneer de gegevens niet langer noodzakelijk zijn, vernietigt GGD Amsterdam de gegevens conform de vestgestelde bewaartermijnen.

4.13. De Onderdeelcommissie wordt betrokken bij privacy onderwerpen

GGD Amsterdam wil graag in gesprek treden met haar medewerkers over de manier waarop privacy in haar organisatie moet worden benaderd, maar ook hoe privacy gerelateerde zaken beter kunnen. De Onderdeelscommissie spreekt namens de medewerkers van GGD Amsterdam. GGD Amsterdam betrekt daarom de Onderdeelscommissie bij privacy onderwerpen. Daarnaast geldt een wettelijke verplichting om de Ondernemingsraad/Onderdeelcommissie te betrekken als de persoonsgegevens van medewerkers worden verwerkt.
Bij vragen over de betrokkenheid van de Onderdeelcommissie gelden de volgende uitgangspunten:

1. GGD Amsterdam betrekt de Onderdeelscommissie bij privacy gerelateerde onderwerpen.
2. GGD Amsterdam informeert de Onderdeelscommissie in ieder geval over de invoering of wijziging van een belangrijke technologische voorziening.
3. GGD Amsterdam vraagt (als dit verplicht is volgens de Wet op de Ondernemingsraden)[3] toestemming aan de Ondernemingsraad gemeente Amsterdam in het geval GGD Amsterdam een regeling introduceert over het verwerken of de bescherming van persoonsgegevens van GGD Amsterdam-medewerkers waarbij sprake is van een hoog risico.
4. GGD Amsterdam vraagt (als dit verplicht is volgens de Wet op de Ondernemingsraden)[4] de toestemming aan de Ondernemingsraad gemeente Amsterdam in het geval GGD Amsterdam een voorziening introduceert die gericht is op of geschikt is voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de GGD Amsterdam-medewerkers.

3 Zie artikel 27 lid 1, sub k van de Wet op de Ondernemingsraden.
[4] Zie artikel 27 lid 1, sub l van de Wet op de Ondernemingsraden.

4.14. Persoonsgegevens worden adequaat beveiligd

GGD Amsterdam is wettelijk verplicht “passende technische en organisatorische maatregelen” te nemen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. GGD Amsterdam moet daarom beveiligingsmaatregelen instellen door haar hele organisatie heen. Dit heeft GGD Amsterdam geregeld in het *GGD Amsterdam Informatiebeveiligingsbeleid* die de uitgangspunten bevat met betrekking tot beveiliging van persoonsgegevens bij GGD Amsterdam. De beleidsuitgangspunten zijn in dit document uitgewerkt en er zijn beveiligingseisen en bijbehorende maatregelen opgenomen die binnen GGD Amsterdam gelden.

4.15. Datalekken worden gemeld

Op grond van de AVG kan GGD Amsterdam gehouden zijn tot het melden van datalekken aan de Autoriteit Persoonsgegevens en in sommige – meer ernstige – gevallen aan alle door het datalek getroffen betrokkenen. Het niet voldoen aan de meldplicht kan leiden tot boetes, maar bijvoorbeeld ook tot reputatieschade voor GGD Amsterdam. GGD Amsterdam vraagt aan haar medewerkers en leveranciers om uit te kijken naar eventuele datalekken, zodat zij snel kunnen worden gesignaleerd en kunnen worden gemeld via TOPdesk en het afdelingshoofd bij de Coördinator informatiebeveiliging en de Privacy Officer. GGD Amsterdam is verplicht alle inbreuken te documenteren, zodat de Autoriteit Persoonsgegevens naleving van de wet kan controleren.

Met betrekking tot de Meldplicht Datalekken gelden binnen GGD Amsterdam de volgende uitgangspunten:

1. Met het oog op een melding van een inbreuk in verband met persoonsgegeven bij de Autoriteit Persoonsgegevens is het *GGD Amsterdam Datalek Protocol* opgesteld met als doel het inrichten van een proces voor het signaleren, registreren en melden van datalekken. Zie het *GGD Amsterdam Datalek Protocol* voor een uitgebreide procesomschrijving.
2. GGD Amsterdam verplicht iedere medewerker (of leverancier) om een datalek met behulp van TOPdesk aan de Technical Security Officer en de Privacy Officer te melden en bij het afdelingshoofd.
3. De Technical Security Officer documenteert alle binnenkomende meldingen waarbij ten minste wordt bijgehouden de feiten omtrent de inbreuk, de gevolgen en de genomen maatregelen om de schade te beperken.
4. De Technical Security Officer en de Privacy Officer besluiten samen of een inbreuk door de FG gemeld dient te worden bij de Autoriteit Persoonsgegevens. Bovendien wordt de directie geinformeerd.

4.16. Medewerkers krijgen training over privacy

Bewustzijn van privacy (en de onderliggende principes) bij GGD Amsterdam medewerkers is ontzettend belangrijk. Medewerkers moeten op de hoogte zijn van de risico’s die zich voor kunnen doen tijdens het werken met persoonsgegevens, en moeten worden geïnformeerd over de beginselen van privacy (zoals doelbinding, dataminimalisatie, bewaartermijnen en datakwaliteit).

Daarom gelden binnen GGD Amsterdam de volgende uitgangspunten:

1. Alle medewerkers binnen GGD Amsterdam die te maken hebben met de verwerking van persoonsgegevens worden ingelicht over het gebruik en de risico’s van (bijzondere) persoonsgegevens (awareness) en de beginselen van privacy.
2. Dit moet onderdeel worden van onboarding / inwerkprogramma voor nieuwe medewerkers
3. Het DPGA-team is verantwoordelijk voor de coördinatie, ontwikkeling en uitvoer van het creëren van privacy bewustzijn binnen GGD Amsterdam.

4.17. GGD Amsterdam communiceert over privacy naar en met haar stakeholders

Het is belangrijk dat GGD Amsterdam op transparante en duidelijke wijze communiceert over het gebruik van persoonsgegevens, zowel intern als extern. GGD Amsterdam vindt privacy erg belangrijk, maar gebruikt haar benadering met betrekking tot privacy niet als onderscheidend vermogen in de markt. GGD Amsterdam legt de prioriteit bij het intern op orde hebben van privacy gerelateerde zaken.

Daarnaast zijn er meerdere interne en externe stakeholders die er belang bij hebben regelmatig over ontwikkelingen met betrekking tot privacy binnen GGD Amsterdam te worden geïnformeerd. Intern is dit goed mogelijk via het GGD Amsterdam Intranet en via verschillende protocollen. Extern informeert GGD Amsterdam via onder andere het *GGD Amsterdam Privacyverklaring, **de*** betrokkenen over het gebruik van persoonsgegevens door GGD Amsterdam.

4.18. Gebruik van cookies en andere tracking methodes wordt geregeld in Richtlijnen

Een cookie is een klein tekstbestandje dat een website op de harde schijf van je computer zet op het moment dat je de site bezoekt. De belangrijkste functie van cookies is om de ene websitebezoeker van de andere te onderscheiden. Met deze cookies kan GGD Amsterdam bijvoorbeeld het surfgedrag van mensen door de tijd heen volgen. Uit de informatie over bezochte websites kunnen persoonlijke interesses of voorkeuren worden afgeleid.

Er bestaan twee soorten cookies, technische cookies en tracking cookies. Tracking cookies maken het mogelijk om (gedrags-)profielen van mensen op te stellen en hen anders te behandelen. Met tracking cookies worden doorgaans persoonsgegevens verwerkt. De inzet van cookies of soortgelijke tracking methodes zijn daarom onderworpen aan bijzondere wettelijke regels.

Cookies of soortgelijke tracking methodes kunnen mogelijk worden ingezet voor de GGD Amsterdam website. Als GGD Amsterdam tracking cookies gebruikt wordt er volgens de wettelijke bepalingen een cookiesverklaring getoond aan de websitegebruiker en een keuze menu voorgesteld die niet vooraf is ingesteld.

4.19. Verwerkersovereenkomst wordt gesloten met de verwerker

GGD Amsterdam kan de verwerking van persoonsgegevens uitbesteden aan een gespecialiseerde partij: de zogenaamde ‘verwerker’. GGD Amsterdam schakelt alleen verwerkers in wanneer dat noodzakelijk is en waar deze derde partij de juiste waarborgen in acht neemt.

Om een zorgvuldige omgang met persoonsgegevens en de vertrouwelijkheid daarvan door verwerkers te waarborgen wordt door GGD Amsterdam een verwerkersovereenkomst met de verwerker afgesloten. GGD Amsterdam maakt gebruik van de modelovereenkomst van de Vereniging van Nederlandse Gemeenten (VNG). De afdeling inkoop zorgt ervoor dat als een contract gesloten wordt met een verwerker de verwerkersovereenkomst als bijlage toegevoegd wordt. Als er wijzigingen worden voorgesteld door de verwerker beoordelen de Privacy Officer en de Information Security Officer de impact en het gewijzigde risico met betrekking tot de bescherming van de persoonsgegevens of voor GGD Amsterdam en of tegen de voorgestelde voorwaarden de overeenkomst gesloten kan worden.

Als er sprake is van een samenwerkingsvorm waarbij persoonsgegevens worden uitgewisseld en er sprake is van een gezamenlijke verwerkersverantwoordelijkheid[5] wordt een overeenkomst gesloten waarin de

[5] Zoals bedoeld in Artikel 26 AVG

verantwoordelijkheden van de partijen, met name met betrekking tot het proces van verzoeken van betrokkenen en het recht op informatie van betrokkenen, wordt vastgelegd. De Privacy Officer wordt door degene die de hoofdovereenkomst sluit betrokken bij het contracteringsproces.

4.20. Verwerving persoonsgegevens van derden

Binnen GGD Amsterdam komt het voor dat persoonsgegevens worden uitgewisseld met of op andere wijze ter beschikking worden gesteld aan derde partijen voor de kwaliteit en de volledigheid van de aanwezige persoonsgegevens binnen GGD Amsterdam.

GGD Amsterdam verwerft alleen persoonsgegevens van verantwoorde partijen die privacy en security waarborgen (en dit ook kunnen aantonen).

De derde partij in kwestie moet voldoen aan door GGD Amsterdam opgestelde richtlijnen voordat persoonsgegevens van hem mogen worden verworven. In het kader van de verwerving van persoonsgegevens van derden partijen gelden de volgende uitgangspunten:

1. De afdeling die de persoonsgegevens verwerft is verantwoordelijk om zorg te dragen dat persoonsgegevens enkel worden verworven van verantwoorde partijen.
2. Afdeling Inkoop in samenwerking met de Privacy Officer spelen een adviserende rol in de verwerving van persoonsgegevens van derde partijen.
3. GGD Amsterdam beoordeelt de derde partij aan de hand van de volgende richtlijnen om een indicatie te krijgen in hoeverre de derde partij een verantwoorde partij betreft:
    a. De partij is niet op negatieve wijze in de media gekomen over de omgang met persoonsgegevens.
    b. De persoonsgegevens zijn direct van de betrokkene verkregen waardoor de partij kan instaan voor de rechtmatigheid van de eerdere verwerking.
    c. De derde partij kan aantonen dat de persoonsgegevens zijn verzameld op grond van een wettelijke grondslag.
    d. De derde partij heeft de persoonsgegevens van de betrokkene verkregen voor welbepaalde, gerechtvaardigde doeleinden die overeenkomen met de doeleinden waarvoor GGD Amsterdam de persoonsgegevens verkrijgt.
    e. De persoonsgegevens zijn juist en nauwkeurig.

4.21. Persoonsgegevens worden nooit aan derden verkocht

GGD Amsterdam verkoopt nooit persoonsgegevens aan derde partijenn, omdat de gegevens door onder andere cliënten, medewerkers en mantelzorgers in vertrouwen met GGD Amsterdam worden gedeeld. Dit vertrouwen staat voor GGD Amsterdam boven alles.

GGD Amsterdam hanteert de volgende uitgangspunten:

1. Persoonsgegevens worden niet aan derden verkocht.
2. Uitzondering: GGD Amsterdam kan wel gehouden zijn tot de doorgifte van persoonsgegevens op grond van een wettelijke bepaling, bijvoorbeeld in het kader van het opvragen van gegevens door strafrechtelijke autoriteiten of de Belastingdienst.

4.22. Persoonsgegevens worden in beginsel binnen de Europese Economische Ruimte verwerkt

Binnen GGD Amsterdam wordt het uitgangspunt gehanteerd dat persoonsgegevens in beginsel altijd binnen de Europese Economische Ruimte (hierna: EER) worden verwerkt.[6] Het kan echter voor komen dat persoonsgegevens (in de toekomst) door een verwerker worden verwerkt in een land buiten de EER. Denk bijvoorbeeld aan een Cloud provider. De AVG vereist voor verwerkingen van persoonsgegevens buiten de EER dat het land een passende waarborgen biedt, vooral voor de betrokkenen. Naast landen met een passend beschermingsniveau kan GGD Amsterdam ook een beroep op andere gronden waardoor doorgifte naar die landen is gerechtvaardigd. Dit betekent dat GGD Amsterdam altijd een geldige reden moet hebben voor een verwerking buiten de EER. Indien er geen uitzondering valt aan te wijzen mogen de persoonsgegevens niet worden verwerkt.

Voor GGD Amsterdam gelden de volgende uitgangspunten voor de verwerking van persoonsgegevens buiten de EU:

1. Persoonsgegevens worden in beginsel slechts doorgegeven naar een land dat een passend beschermingsniveau waarborgt.[7]
2. Persoonsgegevens mogen naar een land worden doorgegeven dat geen waarborgen biedt voor een passend beschermingsniveau, alleen als GGD Amsterdam aan één van de volgende vereisten voldoet:
    a. De betrokkene daarvoor zijn uitdrukkelijk toestemming heeft gegeven.
    b. De doorgifte noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst.
    c. De doorgifte noodzakelijk is voor de sluiting of uitvoering van een in het belang van de betrokkene tussen de verantwoordelijke en een derde gesloten of te sluiten overeenkomst.
    d. De doorgifte noodzakelijk is vanwege een gewichtige reden van algemeen belang, of voor de vaststelling, de uitvoering of de verdediging in rechte van enig recht.
    e. De doorgifte is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering.
    f. De doorgifte noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene.
    g. De doorgifte vindt plaats op grond van een door de Commissie goedgekeurde modelcontractsbepaling die bepaalde waarborgen biedt.[8]

4.23. Binnen samenwerkingsverbanden wordt eenzelfde privacyniveau verlangd

GGD Amsterdam werkt vaak samen met andere organisaties, zoals instellingen of ziekenhuizen (bijvoorbeeld huisartsen). Binnen deze samenwerkingsverbanden kan het zijn dat persoonsgegevens worden gedeeld in het kader van onderzoek en preventie. Wanneer GGD Amsterdam een samenwerkingsverband aangaat, is het van belang dat deze partijen minimaal hetzelfde privacyniveau in acht nemen wanneer het gaat om de bescherming van persoonsgegevens. Dit omdat GGD Amsterdam mede reputatieschade kan ondervinden als het bij de samenwerkende partij onverhoopt misgaat.

Het privacyniveau als beoogt in het *GGD Amsterdam Privacybeleid* is leidend.

[6] De EER bestaat uit de Europese Unie, aangevuld met Noorwegen, Liechtenstein en IJsland.
[7] Zie Doorgifte binnen en buiten de EU
[8] Artikel 46 jo Artikel 49 AVG

In het geval een partij afwijkt van deze standaard, kan bij wijze van uitzondering toch worden besloten om met deze partij de samenwerking aan te gaan. Over samenwerkingsverbanden gelden daarom binnen GGD Amsterdam de volgende uitgangspunten:

1. Binnen samenwerkingsverbanden wordt in beginsel eenzelfde privacyniveau verwacht als binnen GGD Amsterdam wordt gehanteerd. Het *GGD Amsterdam Privacybeleid* is daarbij leidend.
2. Het afdelingshoofd is verantwoordelijk voor het beoordelen van het privacyniveau van de partij(en) binnen het samenwerkingsverband.
3. Het afdelingshoofd vraagt voorafgaand aan het beoordelen van het privacyniveau van de partij(en) tijdig advies aan de Privacy Officer omtrent mogelijke consequenties van het besluit.

Versiebeheer

Versie	Datum	Gewijzigd door	Wijzigingen
0.1	11 mei 2020	5.1,2,e	Start eerste concept
0.2	12 mei 2020	5.1,2,e	Review eerste concept
1.2	1 juli 2020	5.1,2,e	Bijlage 1 Wet en regelgeving

Bijlage 1: Wet- en regelgeving

Wet & regelgeving GGD Amsterdam in relatie tot de AVG
Algemene verordening gegevensbescherming (Avg/GDPR)
Uitvoeringswet Algemene verordening gegevensbescherming (Uavg)
Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)
Wet maatschappelijke ondersteuning 2015 (Wmo 2015)
Wet op de geneeskundige behandelingsovereenkomst (WGBO)
Wet op de identificatieplicht (WID)
Wet op de loonbelasting 1964
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wbsn-z)
Wet publieke gezondheidszorg
Wet elektronische gegevensuitwisseling in de zorg
Wet Marktordening Gezondheidszorg (Wmg)
Wet op de ondernemingsraden (WOR)
Grondwet
Archiefwet
Wet op de medische keuringen
Wet langdurige zorg (WLZ)
Zorgverzekeringswet (Zvw)
Wet kwaliteit, klachten en geschillen zorg (Wkkgz)
Wet medisch-wetenschappelijk onderzoek met mensen (WMO)
Geneesmiddelenwet
Jeugdwet
Besluit Basisregistratie Personen
Wet op de Arbeidsongeschiktheidsverzekering
Ziektewet
Pensioenwet
Arbeidsomstandighedenwet
Werkkostenregeling
Participatiewet
Wet op de lijkbezorging