

Data Protection Impact Assessment¹

<naam>

Invul-Instructie:

- Alle tekst die in dit lettertype (verdana 10) staat is standaard en dient te blijven staan.
- **Alle tekst die dikgedrukt is, is een toelichting op datgene wat je bij die paragraaf in moet vullen. Daar waar de dikgedrukte tekst weggehaald dient te worden, wordt het aangegeven.**
- *Alle tekst die grijs cursief staat geeft weer dat dit een verplicht in te vullen veld is*

¹ Het [model gegevensbeschermingseffectbeoordeling Rijksdienst \(PIA\)](#) is als uitgangspunt gebruikt bij het opstellen van de standaardformat DPIA van de GGD Zuid Limburg.

Inhoudsopgave

Organisatiegegevens.....	4
Inleiding.....	5
Doel DPIA	5
Reikwijdte DPIA.....	5
1. Beschrijving kenmerken gegevensverwerkingen	6
1.1. Voorstel	6
1.2. Persoonsgegevens.....	6
1.3. Gegevensverwerkingen	7
1.4. Verwerkingsdoeleinden	7
1.5. Betrokken partijen en rolverdeling bij de gegevensverwerking	7
1.6. Belangen bij de gegevensverwerking	7
1.7. Verwerkingslocaties	8
1.8. Techniek en methode van gegevensverwerking	8
1.9. Juridisch en beleidsmatig kader.....	8
1.10. Bewaartermijnen (opslag van gegevens)	8
2. Beoordeling rechtmatigheid gegevensverwerkingen	10
2.1. Rechtsgrond – wettelijke grondslag	10
2.2. Bijzondere persoonsgegevens	10
2.3. Doelbinding (verdere verwerking)	11
2.4. Noodzaak en evenredigheid	11
2.5. Rechten van betrokkenen	11
3. Beschrijving en beoordeling risico's voor de betrokkenen.....	14
3.1. Risico's	14
3.1.1. Algemene risico's	15
3.1.1. Specifieke risico's.....	16
4. Beschrijving voorgenomen maatregelen	17
4.1. Maatregelen	17
Generieke maatregelen (GM).....	17
Specifieke technische en organisatorische maatregelen.....	18
5. Bijlagen	19
Bijlage 1. Advies Functionaris Gegevensbescherming GGD Zuid Limburg	19
Bijlage 2. Versiebeheer.....	20

Inhoud

Hoofdstuk 1 beschrijft het gehele proces van de gegevensverwerking, van gegevensverzameling tot gegevensopslag en gegevensvernietiging. Zo komen aan bod: de soort persoonsgegevens die worden verwerkt en voor welk doel; de partijen die bij de gegevensverwerking betrokken zijn en hun belangen en hoe lang de gegevens die worden verwerkt zullen worden bewaard.

In hoofdstuk 2 wordt beoordeeld of de gegevensverwerking zoals voorgesteld in hoofdstuk 1 voldoet aan de wettelijke vereisten en dus rechtmatig is. Zo wordt ingegaan op de wettelijke grondslag voor de verwerking van (bijzondere) persoonsgegevens, wordt beoordeeld of de gegevens die verwerkt worden, noodzakelijk zijn om het vastgestelde doel te bereiken en welke rechten die betrokkenen hebben ten aanzien van hun gegevens.

Hoofdstuk 3 en 4 sluiten af met het in kaart brengen van de (mogelijke) risico's die zich kunnen voortdoen bij de voorgestelde gegevensverwerking en de maatregelen die zijn of zullen worden genomen om die risico's af te wenden.

Organisatiegegevens

Organisatie	
Naam organisatie	Geneeskundige Gezondheidsdienst Zuid-Limburg (hierna: GGDZL)
Kvk-nummer	14 13 14 74
Adres	Het Overloon 2 6411 TE Heerlen

Functionaris gegevensbescherming	
Functionaris Gegevensbescherming (FG)	Nikée Adams
Registratienummer Autoriteit Persoonsgegevens (AP)	FG002119
Contactgegevens FG	FunctionarisAP@ggdzl.nl 088 8800 5181

Opstellers DPIA	
Naam	
Contactgegevens	

Additioneel geraadpleegde personen	
Geraadpleegde interne personen (naam + functie)	
Geraadpleegde externe personen (naam + functie)	

Inleiding

[tekst weghalen] Schrijf een korte inleiding over de gegevensverwerking waarop dit DPIA-rapport betrekking heeft (geef een korte samenvatting van de gegevensverwerking waarvoor je de DPIA gaat uitvoeren)

Doel DPIA

Het doel van een DPIA is om de verwerking van de persoonsgegevens te beschrijven, het doel en de grondslag van de gegevensverwerking te bepalen, de noodzaak en evenredigheid ervan te beoordelen en de aan de verwerking verbonden risico's voor de privacy van de betrokkenen te identificeren, in te schatten en maatregelen te nemen ter beperking van die risico's.

Reikwijdte DPIA

Bepaal de reikwijdte van de DPIA: welke gegevensverwerkingen, (sub)processen en applicaties vallen binnen de reikwijdte van de DPIA.

1. Beschrijving kenmerken gegevensverwerkingen

1.1. Voorstel

Beschrijf het voorstel waar de DPIA op ziet en de context waarbinnen deze plaatsvindt op hoofdlijnen.

Aanleiding

Voorstel

1.2. Persoonsgegevens

Som alle categorieën persoonsgegevens op die worden verwerkt. Geef per categorie tevens aan op wie een persoonsgegeven betrekking heeft (betrokkenen) en geef de typering: gewoon, bijzonder, strafrechtelijk of wettelijk identificerend.

Categorieën persoons-gegevens	Categorieën betrokkenen	Gewoon persoonsgegevens	Bijzonder persoonsgegevens	Wettelijk identificerend persoonsgegevens

1.3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer (procesbeschrijving en flowchart).

1.4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

1.5. Betrokken partijen en rolverdeling bij de gegevensverwerking

Beschrijf welke organisaties betrokken zijn bij welke gegevensverwerking. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, (sub-)verwerker, verstrekker en ontvanger.

- **Verwerkingsverantwoordelijke:** degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
- **Verwerker:** degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
- **Subverwerker:** degene die ten behoeve van de verwerker persoonsgegevens verwerkt
- **Verstrekker:** degene die persoonsgegevens bekend maakt of ter beschikking stelt
- **Ontvanger:** degene aan wie de persoonsgegevens worden verstrekt

Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens. Indien er tussen partijen een verwerkersovereenkomst nodig is, staat dat aangegeven in deze paragraaf.

Verwerkingsverantwoordelijke

Verwerker

Verstrekker

Ontvanger

1.6. Belangen bij de gegevensverwerking

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

Samenleving als geheel

Betrokkenen

GGD

Andere partijen

1.7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

1.8. Techniek en methode van gegevensverwerking

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi)-geautomatiseerde besluitvorming, profiling of big-data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

1.9. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

Op de verwerking van persoonsgegevens is de volgende wet- en regelgeving van toepassing:

- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet AVG (UAVG);
- *[vul aan met de voor deze gegevensverwerking relevante wet- en regelgeving]*

De volgende beleidsdocumenten zijn van toepassing op de verwerking van de persoonsgegevens:

- Informatiebeveiligingsbeleid GGD ZL;
- Privacyreglement GGD ZL;
- Huisregels voor informatieveilig werken;
- *[vul aan met de voor deze gegevensverwerking relevante beleidsdocumenten]*

1.10. Bewaartermijnen (opslag van gegevens)

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden. **[tekst hierna weghalen] Beschrijf hier zo gedetailleerd mogelijk de bewaartermijnen van de gegevens. Waar sla je de gegevens op? Hoe lang sla je ze op? Wie heeft er toegang tot deze gegevens? Wanneer en door wie worden ze vernietigd?**

Soort gegevens	Opslagplek	Wie heeft er toegang	Bewaartermijn	Vernietigen data

2. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de juridische grondslag, de noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel voorts de wijze waarop invulling gegeven wordt aan de rechten van betrokkenen. Raadpleeg indien nodig de juridisch adviseur.

2.1. Rechtsgrond – wettelijke grondslag

De verwerking van 'gewone' persoonsgegevens is toegestaan indien de gegevensverwerking gebaseerd kan worden op minimaal één van de [zes grondslagen van de AVG](#). Voor de gegevensverwerkingen van 'gewone' persoonsgegevens wordt een beroep gedaan op:

- *[benoem de grondslag(en) uit de AVG die van toepassing is/zijn voor deze gegevensverwerkingen .]*

[tekst weghalen] Wanneer de van toepassing zijnde grondslag een wettelijke verplichting en/of een (in de wet vastgelegde) taak van algemeen belang is, dan dient ook de sectorspecifieke wetgeving waarin deze wettelijke taak is vastgelegd, hier beschreven te worden. Bv. De wettelijke taak om de Gezondheidsmonitor uit te voeren is opgenomen in de Wpg (artikel 2 lid 2 onder b).

[tekst weghalen] Geef een toelichting waarom bovengenoemde grondslag(en) van toepassing zijn.

2.2. Bijzondere persoonsgegevens

Voor het verwerken van bijzondere persoonsgegevens (zoals gezondheidsgegevens) is het noodzakelijk dat er – aanvullend op het hebben van een wettelijke grondslag als hiervoor omschreven – ook een wettelijke uitzondering op het verwerkingsverbod van toepassing is, zoals bedoeld in [artikel 9 van de AVG](#).

De uitzondering op het verwerkingsverbod die van toepassing is in het kader van deze gegevensverwerking is neergelegd in artikel 9 lid 2 sub [...] *[benoem hier de van toepassing zijnde uitzondering uit artikel 9 van de AVG.*

[tekst weghalen] Motiveer waarom deze uitzondering van toepassing wordt geacht. Daarbij dient rekening te worden gehouden met het feit dat voor [5 van de 10 uitzonderingen](#) geldt dat zij een basis moeten hebben in een Nederlandse wet. Indien een van deze uitzonderingen van toepassing wordt geacht, dient ook de wettelijke bepaling uit de Nederlandse wetgeving te worden benoemd en te worden aangegeven waarom die bepaling bij deze concrete gegevensverwerking van toepassing is.

2.3. Doelbinding (verdere verwerking)

Indien persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

[tekst weghalen] Simpel gezegd: Geef hier aan of je de gegevens ook voor andere doeleinden gebruikt dan waarvoor je deze DPIA uitvoert. Als je de gegevens niet voor iets anders gaat gebruiken, kun je hier gewoon aangeven dat de gegevens niet verder worden verwerkt voor andere doeleinden. Let op: controleer ook even in je toestemmingsverklaring of je hierin toestemming vraagt voor deelname aan toekomstig onderzoek.

[tekst weghalen] Ter informatie: De AVG zegt hierover het volgende: "De AVG eist dat toestemming voor verwerking van persoonsgegevens (voldoende) specifiek is. Omdat op het moment waarop toestemming wordt gevraagd voor gebruik van persoonsgegevens voor toekomstig onderzoek veelal nog niet (voldoende) specifiek is wat dat toekomstige onderzoek inhoudt, kan er dan een probleem rijzen bij het verkrijgen van rechtsgeldige specifieke toestemming. Bij de totstandkoming van de AVG is dit onderkend als probleem en is aangegeven dat een rechtsgeldige toestemming voor 'hergebruik' van persoonsgegevens kan worden verleend, mits dat hergebruik voldoende afgebakend wordt. Dit kan bijvoorbeeld door afbakening van het onderzoeksgebied (bijvoorbeeld een specifieke aandoening en/of een specifieke behandelwijze) waarvoor de persoonsgegevens 'hergebruikt' mogen worden. In situaties waarin hergebruik van de persoonsgegevens buiten die afbakening valt, zal ofwel opnieuw toestemming moeten worden gevraagd, ofwel een beroep moeten worden gedaan op de uitzonderingsbepaling voor gebruik van persoonsgegevens voor wetenschappelijk onderzoek zonder toestemming van betrokkene."

2.4. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit:

- a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
- b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder ingrijpende wijze, worden verwezenlijkt?

2.5. Rechten van betrokkenen

Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

[tekst weghalen] Vul de informatie opgenomen bij onderstaande rechten aan indien betrokkenen in het kader van deze gegevensverwerkingen nog op meer of andere wijzen hun rechten kunnen uitoefenen

Betrokkenen hebben op basis van de AVG verschillende rechten ten aanzien van de gegevens die van hen worden verwerkt. Voor de uitoefening van die rechten is er een proces ingericht. Betrokkenen kunnen via de website van de GGD Zuid Limburg een verzoek indienen via de online formulieren die hiervoor ter beschikking zijn gesteld. Betrokkenen hebben de volgende rechten:

Recht op informatie (art. 13 AVG)

De betrokkene heeft het recht om informatie te ontvangen over de verwerking van zijn/haar persoonsgegevens. De betrokkene wordt in de eerste plaats geïnformeerd over zijn rechten op de website van de GGD Zuid Limburg.

Recht op inzage en afschrift (art. 15)

De betrokkene heeft het recht om de verwerkte persoonsgegevens in te zien en hier een kopie van te ontvangen. Het recht op inzage wordt afgehandeld conform de bij de verwerkingsverantwoordelijke geldende interne procedures.

Recht op rectificatie (art. 16)

De betrokkene heeft het recht om feitelijke onjuistheden in zijn gegevens te laten corrigeren of aanvullen. Het recht op rectificatie wordt afgehandeld conform de bij de verwerkingsverantwoordelijke geldende interne procedures.

Recht op gegevenswissing (art. 17 AVG)

De betrokkene kan verzoeken zijn persoonsgegevens te wissen, behoudens wanneer een van de uitzonderingen op het recht op gegevenswissing van toepassing is. Het recht op gegevenswissing wordt afgehandeld conform de bij de verwerkingsverantwoordelijke geldende interne procedures.

Recht op beperking van de verwerking (art. 18 AVG)

De betrokkene kan in bepaalde gevallen verzoeken om de verwerking van zijn gegevens te beperken, namelijk wanneer de gegevens die worden verwerkt onjuist zijn, de gegevens onrechtmatig worden verwerkt, de gegevens niet meer nodig zijn of wanneer de betrokkene bezwaar heeft gemaakt tegen het verwerken van zijn gegevens. Het recht op gegevenswissing wordt afgehandeld conform de bij de verwerkingsverantwoordelijke geldende interne procedures.

Recht op dataportabiliteit (art. 20 AVG)

De betrokkene heeft het recht op het overdragen van zijn gegevens indien de gegevensverwerking plaatsvindt op grond van de wettelijke grondslag toestemming of het uitvoeren van een overeenkomst. Het recht op dataportabiliteit wordt afgehandeld conform de bij de verwerkingsverantwoordelijke geldende interne procedures.

Recht van bezwaar (art. 21 AVG)

De betrokkene heeft het recht om bezwaar te maken tegen de verwerking van zijn persoonsgegevens. De betrokkene heeft dit recht indien zijn gegevens worden verwerkt voor commerciële doeleinden of wanneer de gegevens worden verwerkt op grond van

een taak van algemeen belang en de bijzondere persoonlijke situatie van de betrokkene aanleiding geeft tot het maken van bezwaar. Het recht van bezwaar wordt afgehandeld conform de bij de verwerkingsverantwoordelijke geldende interne procedures.

Recht om niet te worden onderworpen aan geautomatiseerde besluitvorming, waaronder profilering (art. 22 AVG)

Er is geen sprake van geautomatiseerde individuele besluitvorming als bedoeld in artikel 22 van de AVG.

3. Beschrijving en beoordeling risico's voor de betrokkenen

[tekst weghalen] N.B. In dit format zijn risico's (hoofdstuk 3) en maatregelen (hoofdstuk 4) in twee hoofdstukken opgesplitst. Uit de DPIA dient duidelijk te blijken welke maatregelen zijn voorgesteld/geadviseerd, welke maatregelen zijn genomen, welke maatregelen nog worden genomen en welke maatregelen niet worden genomen (en waarom niet). Er kan voor gekozen worden om hoofdstuk 3 en 4 te integreren, zo lang maar duidelijk is welke maatregelen wel en niet genomen zijn. Aangezien wij een standaard format (Rijksmodel) gebruiken, handhaven wij deze standaard indeling, maar indien een DPIA-aanvrager in een specifieke DPIA hoofdstuk 3 en 4 wilt integreren dan is dit toegestaan, mits goed beschreven.

3.1. Risico's

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in hoofdstuk 1 en 2 beschreven en beoordeeld.

Ga hierbij in ieder geval in op:

- a. Welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;**
- b. De oorsprong van deze gevolgen;**
- c. De waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;**
- d. De ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.**

De kwalificatie wordt gemaakt op basis van kans x impact = risiconiveau. Hieronder is aangegeven hoe de uiteindelijke risico calculatie plaatsvindt.

De kans en impact worden gebruikt om het niveau van het risico te bepalen, op basis van de beschreven aspecten:

- De kans (K) dat een risico effectueert; en
- De impact (I) op de organisatie of de Betrokkene als het risico is geëffectueerd.

Het risiconiveau wordt toegekend door een vooraf vastgestelde matrix die het belang van mitigerende maatregelen aangeeft. De combinaties van kans en impact zijn gegroepeerd in hoog (H, rood), midden (M, geel) en laag (L, groen). De matrix toont hoe de risico's zijn geclassificeerd gebaseerd op de impact en kans.

Kans Impact			
	Laag	Middel	Hoog
Laag	Laag	Laag	Middel
Midden	Laag	Middel	Hoog
Hoog	Middel	Hoog	Hoog

Op basis van de risiconiveaus uit de matrix staat in de tabel hieronder beschreven welke maatregelen verwacht worden.

Risiconiveau	Risico Beschrijving en te verwachten maatregel
Hoog	Als een waarneming of bevinding wordt geëvalueerd als een hoog risico, is er sterke behoefte aan corrigerende maatregelen. Een bestaand systeem kan blijven werken, maar een beveiligingsplan of andere risico-beperkende maatregel moet zo snel mogelijk worden geïmplementeerd.
Midden	Als een waarneming wordt beoordeeld als gemiddeld risico, moeten eventuele corrigerende maatregelen worden overwogen.
Laag	Als een waarneming wordt beschreven als een laag risico, kunnen corrigerende maatregelen nog steeds nodig zijn of kan het risico worden geaccepteerd.

3.1.1. Algemene risico's

[tekst weghalen] Beschrijf hier de algemene risico's die zich kunnen voordoen bij de gegevensverwerkingen waarop deze DPIA ziet. Hier beneden staan de 11 meest voorkomende risico's al weergegeven. Pas of vul deze algemene risico's aan zodat het aansluit bij de gegevensverwerking zoals in hoofdstuk 1 en 2 beschreven. Beschrijf de volgende generieke maatregelen:

1. Interne medewerkers die niet geautoriseerd zijn hebben toegang tot de gegevens, bijvoorbeeld doordat de autorisaties en rechten niet goed zijn ingesteld.
2. Onbevoegde derden van buiten de organisatie (bv. door ons ingeschakelde derden) hebben toegang tot (te veel) gegevens door onvoldoende beveiliging.
3. De gegevens worden onbedoeld gewijzigd, waardoor de juiste gegevens permanent verloren gaan
4. De gegevens worden onbedoeld permanent vernietigd, waardoor de gegevens verloren gaan

5. De gegevens die worden verzameld zijn niet noodzakelijk voor het doel waarvoor ze worden verwerkt (eisen van noodzakelijkheid en evenredigheid)
6. Betrokkenen zijn onvoldoende geïnformeerd, waardoor zij zich onvoldoende bewust zijn van de risico's, gevolgen en waarborgen van hun rechten in verband met hun persoonsgegevens
7. De gegevens worden verwerkt voor een doel dat onverenigbaar is met het doel waarvoor ze oorspronkelijk zijn verzameld
8. Gegevens worden langer bewaard dan strikt noodzakelijk is voor het doel waarvoor ze zijn verzameld, bijvoorbeeld doordat de bewaartermijnen niet vooraf zijn bepaald
9. Er doet zich een beveiligingsincident (datalek) voor, bijvoorbeeld doordat de gegevens onvoldoende zijn beschermd
10. Gegevens worden niet voldoende gepseudonimiseerd of worden gekoppeld/verrijkt met andere databronnen, waardoor de kans bestaat op depseudonimisering en herleidbaarheid
11. Bij de verwerking van persoonsgegevens worden derden ingeschakeld die de gegevens onvoldoende beveiligen, waardoor onbevoegden toegang kunnen krijgen tot de gegevens

[tekst weghalen] Per risico vul je vervolgens het volgende schema in:

[benoem hoe dit risico zich kan voordoen.]

- De kans dat dit risico zich manifesteert zonder maatregelen is *[laag/midden/hoog]*, want *[benoem waarom de kans laag/midden/hoog is dat het risico zich manifesteert].*
- De impact van dit risico zonder maatregelen is *[laag/midden/hoog]*, want *[benoem waarom de impact laag/midden/hoog is voor betrokkenen.]*

Geadviseerd wordt om de volgende maatregelen te treffen:

[benoem maatregelen die kunnen worden getroffen om de dit risico te voorkomen of te beperken.]

Risico voor Betrokkene (voor maatregelen)	<i>[Laag/midden/hoog]</i>
Risico voor Betrokkene (na maatregelen)	<i>[Laag/midden/hoog]</i>

3.1.1. Specifieke risico's

[tekst weghalen] Beschrijf hier de specifieke risico's die zich kunnen voordoen bij de gegevensverwerkingen waarop deze DPIA ziet (bv. risico's bij betrokken partijen, bv. datalek bij die partij, onrechtmatige inzage bij die partij etc). Gebruik hierbij dezelfde opzet als hierboven.

4. Beschrijving voorgenomen maatregelen

In dit hoofdstuk wordt gezien welke maatregelen dienen te worden getroffen om de in hoofdstuk 3 erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging. Voor dit onderdeel van de DPIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

4.1. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen.

Generieke maatregelen (GM)

#	Generieke maatregel (GM)	Toepassing Ja/nee/nvt	Bekendheid Ja/nee/nvt	Toelichting
1	Ondertekenen geheimhoudingsverklaring			
2	Ondertekenen integriteitsverklaring			
3	Ondertekenen overeenkomsten (bruikleen, verwerkersovereenkomst etc)			
4	Informatiebeveiligingsbeleid			
5	Privacyreglement			
6	Privacyverklaring GGDZL			
7	Privacypagina websieGGDZL			
8	Medewerkersportaal privacy			
9	Medewerkersportaal informatieveilig werken			
10	Doen van leveranciersbeoordelingen van kritische leveranciers			
11	Primaire processen classificeren en opnemen in verwerkingsregister			
12	Procesbeschrijving			
13	Veiligheidsrondes lopen			

14	Incidenten/datalekken melden			
15	Gebruik beveiligd mailen			
16	Kensingtonlocks op openbare werkplekken			
17	Vergrendelen van PC's			
18	Toegangsbeleid met bezoekersregistratie			
19	Autorisatiematrix voor toegang GGD netwerk			
20	Autorisatiematrix voor applicaties			
21	Tweefactor-authenticatie voor inloggen GGD-netwerk			
22	Tweefactor-authenticatie voor inloggen applicaties			
23	Databeveiliging door middel van encryptie tool 'bitlocker pin' op lokale harde schijf laptops			
24	Databeveiliging door middel van encryptie tool 'Bitlocker Pin' op verwisselbare USB-sticks			
25	MDM/MAM-beheer. In beheer nemen van mobile devices (zakelijk/privé). GGD krijgt mogelijkheid bij verlies/diefstal gegevens op gevoelige apps (o.a. Word, Excel, Outlook) op afstand te verwijderen			
25	Mogelijkheid tot gebruik OneDrive applicatie van Microsoft tot verbetering en veilige mogelijkheid om data met derden te delen. Dit ten opzichte van WeTransfer, Dropbox GoogleDrive e.d.			

Specifieke technische en organisatorische maatregelen

5. Bijlagen

Bijlage 1. Advies Functionaris Gegevensbescherming GGD Zuid
Limburg

Bijlage 2. Versiebeheer

Versie	Auteur	Activiteiten
0.1		
0.2		
0.3		