DPIA naam

Naam organisatie

Versie 0.1

Versiebeheer

Versie	Datum	Door	Opmerkingen
0.1			
0.2			
0.3			
0.4			
0.5			
0.6			
0.7			

Vastgesteld door	Naam	Functie	Contactgegevens

Vertrouwelijkheidsniveau

Strikt vertrouwelijk/Bedrijfsvertrouwelijk/Openbaar

Samenvatting

Samenvatting t.b.v. management

1. Inhoudsopgave

Inleiding

Data Protection Impact Assessment

Een Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling, hierna: DPIA) is een instrument om bij (voorgenomen) verwerkingen van persoonsgegevens, de risico's voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen. Op basis van de DPIA kan de verantwoordelijke voorafgaand aan de gegevensverwerking maatregelen treffen om negatieve effecten voor betrokkenen te voorkomen of te verkleinen. Een DPIA helpt om te beoordelen of een voorgenomen gegevensverwerking in lijn is met de AVG en andere relevante wetgeving op het gebied van privacy en gegevensbescherming (compliance). Het resulteert niet in een rechtmatigheidsoordeel.

Een DPIA werd vroeger ook aangeduid als PIA, *privacy impact assessment*. Volgens de AVG gaat een DPIA over de risico's voor de rechten en vrijheden van natuurlijke personen. Betrokkenen hebben een *grondrecht* op bescherming van hun persoonsgegevens en een aantal andere fundamentele *vrijheden* die geraakt kunnen worden door de verwerking van persoonsgegevens. Het recht op gegevensbescherming is dus een breder recht dan alleen het recht op privacy. Overweging 4 van de AVG licht toe: "*Deze verordening eerbiedigt alle grondrechten alsook de vrijheden en beginselen die zijn erkend in het Handvest zoals dat in de Verdragen is verankerd, met name de eerbiediging van het privéleven en het familie- en gezinsleven, woning en communicatie, de bescherming van persoonsgegevens, de vrijheid van gedachte, geweten en godsdienst, de vrijheid van meningsuiting en van informatie, de vrijheid van ondernemerschap, het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, en het recht op culturele, godsdienstige en taalkundige verscheidenheid*." In dit rapport wordt niettemin ter wille van de leesbaarheid soms de term 'privacyrisico' gebruikt om deze risico's voor de rechten en vrijheden van betrokkenen aan te duiden, en niet de juridisch correcte term 'dataprotectierisico' of 'gegevensbeschermingsrisico'.

Op grond van artikel 35 van de Algemene Verordening Gegevensbescherming (AVG) is een DPIA in bepaalde gevallen verplicht. Dit is het geval als een voorgenomen gegevensverwerking een hoog risico vormt voor de betrokkenen van wie de persoonsgegevens worden verwerkt. De Autoriteit Persoonsgegevens (AP) heeft een lijst gepubliceerd met 17 soorten verwerkingen waarvoor een DPIA in Nederland altijd verplicht is.[1] Wanneer een verwerking niet in deze lijst staat, moet een organisatie zelf beoordelen of het gaat om een gegevensverwerking die waarschijnlijk een hoog risico oplevert. De Europese toezichthouders op de bescherming van persoonsgegevens (de data protection authorities, verenigd in het Europees Comité voor de Gegevensbescherming) hebben negen criteria opgesteld om te beoordelen of het gaat om een dergelijke hoog risico verwerking. De vuistregel is dat een DPIA moet worden uitgevoerd als een verwerking aan twee of meer van de negen criteria voldoet.[2]

[1] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf .
[2] http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 .

Scope

Beschrijving scope

De *naam organisatie* is verplicht om voor deze verwerking een DPIA uit te voeren, omdat de gegevensverwerking voldoet aan tenminste 2 van de 9 criteria voor DPIA's van de Europese toezichthouders. Als vuistregel geldt immers dat als een organisatie aan twee of meer van deze criteria voldoet, een DPIA verplicht is.

De twee voor de *naam organisatie* relevante criteria zijn:

Opzet van de DPIA

De DPIA volgt de structuur van het *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)*.[8] Dit model bestaat uit de onderstaande vier delen:

A. beschrijving van de kenmerken en doeleinden van de gegevensverwerking
B. beoordeling van de rechtmatigheid van de gegevensverwerking
C. beschrijving en beoordeling van de risico's voor betrokkenen
D. beschrijving van de voorgenomen maatregelen

Deel A beschrijft de kenmerken en doeleinden van de gegevensverwerking. Ook komen de soorten persoonsgegevens, de betrokkenen, verwerkingsdoeleinden, rollen van de betrokken partijen, belangen bij de verwerking, locaties waar de gegevens worden verwerkt en bewaartermijnen aan de orde. De (technische) werking van de pagers en het informatie- en beheerssysteem (software) komt vanwege de scope van de initiële DPIA nog niet aan bod. Deze functionaliteiten kunnen pas nadat de aanbesteding is gegund bij de desbetreffende leverancier worden gecontroleerd en afgestemd. Op basis waarvan vervolgens inrichtingskeuzes gelet op functionaliteiten en principes vanuit de AVG kunnen worden gemaakt.

Deel B beoordeelt de grondslagen, de noodzaak, evenredigheid en verenigbaarheid van de voorgenomen verwerkingen in relatie tot de verwerkingsdoeleinden. De evenredigheid wordt beoordeeld in het licht van de principes van gegevensverwerking zoals opgesomd in artikel 5 van de AVG, zoals transparantie, adequate beveiliging, *privacy by design* en doelbinding. In dit deel wordt ook de rechtmatigheid beoordeeld van doorgifte van persoonsgegevens naar landen buiten de EU, en de wijze waarop de rechten van betrokkenen worden gewaarborgd.

Deel C beschrijft en beoordeelt de risico's voor de rechten en vrijheden van betrokkenen die voortvloeien uit de verwerking van persoonsgegevens.

Deel D beschrijft de aanvullende technische en organisatorische maatregelen die nodig zijn om de geconstateerde resterende privacyrisico's te verlagen of weg te nemen. Tot slot beschrijft dit deel of er sprake is van een restrisico van de gegevensverwerking na toepassing van risico verlagende maatregelen.

DEEL A

1. Voorstel

Beschrijving voorstel van de verwerking, applicatie of het proces dat DPIA-plichtig is

2. Persoonsgegevens

Het begrip persoonsgegevens is breed en behelst allerlei soorten gegevens over een persoon.

> *"persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.*

In de tabel hieronder staan de persoonsgegevens die in het kader van deze DPIA relevant zijn.

	Persoonsgegevens in het algemeen		**Bijzondere persoonsgegevens**	
		√		
		√		
		√		
		√		
		√		
		√		
		√		
		√		
		√		

Voor de volledigheid wordt verwezen naar Bijlage 1 waarin de dataset met gegevens is opgenomen.

Type persoonsgegevens	**Ja/nee**	**Verkregen van**	**Categorie persoonsgegevens**	**Categorie betrokkenen**
Persoonsgegevens in het algemeen	Ja/Nee			
Bijzondere persoonsgegevens	Ja/Nee			

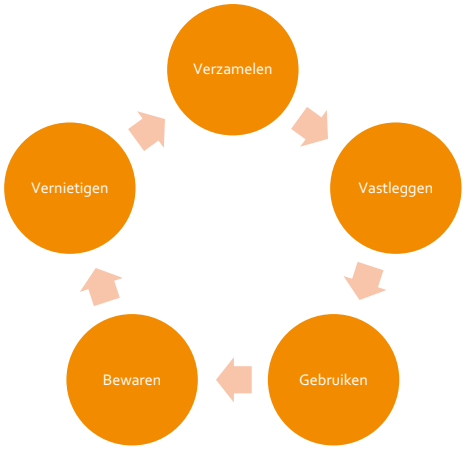
3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Het verwerken van gegevens is een breed begrip:

> *"verwerking": een bewerking of een geheel van 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;*

Het verwerken omvat de hele levenscyclus van persoonsgegevens.



4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Lijst doeleinden invoegen

Beschrijf de doeleinden/gegevensverwerkingen die door verwerkers of externe partijen worden uitgevoerd:

Lijst doeleinden invoegen per partij

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Analyseer op basis van contracten en voorwaarden of een verwerker daadwerkelijk alleen verwerker is. Als er ook eigen doeleinden worden bepaald zal de verwerker ook (deels) (gezamenlijk) verwerkingsverantwoordelijke zijn.

[kijk naar contracten en feitelijke situatie]

[controleer of er nog derde partijen zijn die buiten beeld toch gegevens verkrijgen]

Partij	**Rol**	**Functies met toegang**		
1	Verwerkingsverantwoordelijke (evt. gezamenlijk), verwerker, verstrekker of ontvanger	Functionarissen met toegang		
2				
3				
4				

Tabel opmaken

infotekst

Om de rechtmatigheid van de voorgenomen gegevensverwerkingen te kunnen beoordelen, moet inzichtelijk zijn welke organisaties (functioneel) betrokken zijn bij welke gegevensverwerking en in welke hoedanigheid: verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger.
Verwerkingsverantwoordelijk is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan, die/dat het doel van en de middelen voor de gegevensverwerkingen vaststelt. Met andere woorden: degene die formeel bevoegd is te beslissen of persoonsgegevens worden verwerkt, voor welke doeleinden deze worden verwerkt en op welke wijze deze worden verwerkt. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijke en moeten zij onderling vastleggen wie waarvoor verantwoordelijk en aansprakelijk is.
Verwerker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. De verwerker verwerkt persoonsgegevens voor de verwerkingsverantwoordelijke, dat wil zeggen volgens diens instructies en onder diens verantwoordelijkheid. De verwerker is een buiten de organisatie van de verwerkingsverantwoordelijke staande persoon of organisatie. De verwerkingsverantwoordelijke en verwerker moeten onderling schriftelijk vastleggen wie waarvoor verantwoordelijk en aansprakelijk is. Om in een concreet geval te bepalen wie de verwerkingsverantwoordelijke is en wie de verwerker is, moet naast de formele taakverdeling zoals partijen die onderling hebben afgesproken ook worden gekeken naar de feitelijke omstandigheden (waarom vindt de verwerking plaats? Wie heeft deze geïnitieerd?). Dat betekent dat enkel het schriftelijk vastleggen van de taakverdeling niet voldoende is: ook in de praktijk moet de verwerkingsverantwoordelijke zeggenschap hebben over het doel en de middelen van gegevensverwerkingen.

Ontvanger is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan aan wie/waaraan de persoonsgegevens worden verstrekt.
Verstrekker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat de persoonsgegevens ter beschikking stelt.

Bij conceptregelgeving kan het wenselijk zijn om daarin de hoedanigheid van de betrokken organisaties vast te leggen of volgens welke criteria deze wordt aangewezen. Indien een specifieke regeling over gegevensverwerkingen wordt opgesteld ten behoeve van een publiekrechtelijke taak, dient in de regeling de verwerkingsverantwoordelijke te worden aangewezen. Zo is in de Basisregistratie personen vastgelegd wanneer het college van burgemeester en wethouders en wanneer de minister verantwoordelijk is voor het bijhouden van persoonsgegevens in de basisregistratie. In bepaalde gevallen kan het ook wenselijk zijn om wettelijk voor te schrijven dat de toegang tot bepaalde persoonsgegevens beperkt blijft tot een specifieke functionaris, zoals een officier van justitie, vertrouwenspersoon of bedrijfsarts.

Bij overheidsverwerkingen zullen, voor zover niet reeds wettelijk voorgeschreven, de organisaties die (functioneel) betrokken zijn bij de gegevensverwerkingen zelf en in onderling overleg moeten bepalen wie in welke hoedanigheid de persoonsgegevens verwerkt. Tevens zal moeten worden bepaald, voor zover eveneens niet wettelijk voorgeschreven, welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens, bijvoorbeeld aan de hand van een autorisatiematrix, in relatie tot de doeleinden van de gegevensverwerking. Hierin kan tevens worden bepaald in welke gevallen en onder welke voorwaarden deze functionarissen toegang krijgen tot de persoonsgegevens.

6. Belangen bij de gegevensverwerkingen

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

Lijstje belangen

- Financiële / commerciële belangen
- Voldoen aan wettelijke plicht
- Efficiëntie en bedrijfsvoering
- Uitvoering geven aan publieke taak
- Klantrelaties / marketing
- Leveren goede dienst
- Beveiliging van de gegevens
- Fraudebestrijding
- [aanvullen]

infotekst

Bij de beoordeling van de rechtmatigheid van de gegevensverwerkingen kunnen tevens de belangen (lees: de waarde of de voordelen) die met de gegevensverwerkingen gemoeid zijn een rol spelen. Het kan hierbij zowel gaan om de private belangen van de verwerkingsverantwoordelijke, betrokkene en derden als het algemeen belang. Het gaat hier dus niet om de (mogelijk) negatieve gevolgen voor de betrokkenen. Denk hierbij bijvoorbeeld aan: bedrijfsbelangen, financiële belangen en commerciële belangen, het handhaven van juridische vorderingen, toezicht op medewerkers ten behoeve van de veiligheid of managementdoeleinden, (nationale of openbare) veiligheid, zoals de preventie van fraude, misbruik en netwerkbeveiliging, en gezondheid.

- Het belang dat gemoeid is met de gegevensverwerkingen werkt door in de toets van de noodzaak (zie punten 11 en 14 hierna).

6.1. Belangen [partij 1 - verantwoordelijke]

6.2. Belangen [partij 2 – verwerker/leverancier]

6.3. Belangen partij 3 – betrokkene

6.4. Belangen [partij 4 -]

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Europese Unie / Europese Economische Ruimte

- Ierland
- Nederland
-

Verenigde Staten. Let op Schrems juli 2020.

Let op bij Verenigd Koninkrijk ivm Brexit. Veel internationale aanbieders van cloudopslag maken al onderscheid tussen Europa en VK.

Soms is er per onderdeel van de dienst een verschil in afbakening van de verwerkingslocatie. Denk aan de basisdienst en contentopslag binnen EU, maar technische support mogelijk overal ter wereld. Splits dat dan uit.

Tabel met land en eventueel specifieke locatie. En eventueel nog invoegen eigen hosting of externe partij.

	Land	EER	Beheer hosting	
		Ja/Nee		

Eventueel visual toevoegen met landkaart (bijvoorbeeld via excel te maken)

infotekst

De locaties waar de voorgenomen gegevensverwerkingen plaatsvinden, kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Tevens heeft de verwerkingslocatie invloed op de competentie van de (leidende) privacy toezichthouder.
Om te borgen dat de regels betreffende de bescherming van persoonsgegevens niet omzeild worden door persoonsgegevens in een ander land te verwerken, bepalen de AVG en de Richtlijn dat gegevensverwerkingen buiten de Europese Unie enkel onder bepaalde omstandigheden zijn toegestaan. Dit is bijvoorbeeld het geval indien het derde land naar het oordeel van de Europese Commissie een passend beschermingsniveau heeft (een adequaatheidsbesluit) of indien gebruik wordt gemaakt van passende waarborgen om de betrokkenen te beschermen. Daarnaast zijn een aantal specifieke situaties waarin gegevensverwerkingen in een derde land toch zijn toegestaan ondanks het ontbreken van een passend beschermingsniveau en passende waarborgen, zoals uitdrukkelijke toestemming van de betrokkene.
Naast de AVG en de Richtlijn kunnen andere wettelijke regels of beleid invloed hebben op de locaties waar persoonsgegevens kunnen worden verwerkt. Denk hierbij aan het VIRBI 2013 inzake gerubriceerde overheidsinformatie en situaties waarin opslag in een overheidsdatacenter geëigend is.

8. Technieken en methoden van de gegevensverwerkingen

Beschrijf hier welke technieken en methoden worden gebruikt. Maak daarbij gebruik van visuals in het geval van informatiestromen of koppelingen bij applicaties of databases.

Geautomatiseerde besluitvorming of profiling

Er vindt geen geautomatiseerde besluitvorming of profling plaats. Dit zowel niet met uitkomsten van de geanalyseerde data als de rapportages van de geanalyseerde data. De applicaties worden enkel ingezet op het analyseren van data ten behoeve van sturings- en beleidsinformatie. Waarbij de sturingsinformatie ziet op de uitvoering door het team Werk & Inkomen, namelijk:

- personele bezetting en capaciteit ten behoeve van de behandeling en doorlooptijd van zaken;
- inzicht in de doorlooptijd van zaken;
- het tijdig bij kunnen schakelen indien de doorlooptijd van negatieve invloed is op de beslistermijn.

9. Juridisch en beleidsmatig kader

De volgende wet- en regelgeving is van toepassing op de verwerking.

9.1. Algemene wet- en regelgeving

	Wet- en regeleging		**Artikel (optioneel)**
	Algemene Verordening Gegevensbescherming	√	
	Uitvoeringswet Algemene Verordening Gegevensbescherming	√	
	Gedragscodes	X	40 AVG
	Certificering	X	42 AVG
	Adequaatheidsbesluit	X	45 AVG
	Standaard contractsbepalingen	√	46 AVG
	Bindende bedrijfsvoorschriften	X	47 AVG

9.2. Specifieke wet- en regelgeving

	Wet- en regelgeving		**Artikel (optioneel)**
		√	
	…		

9.3. Beleidsmatig kader

	Beleidsmatig kader		**Artikel (optioneel)**
	Interne beleidsdocumenten		
	…		
	…		

10. **Bewaartermijnen**

Op grond van de AVG moeten de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden worden bepaald.[3]

Voorbeeld opsomming bewaartermijn voor persoonsgegevens bij overheidsverwerkingen (IT/uitvoering):

Categorie Persoonsgegeven	Ingang bewaartermijn	Termijn van bewaring	Motivatie bewaring	Verantwoordelijkheid voor verwijdering
Naam	Vanaf moment dat de betrok-kene voor het eerst inlogt in het systeem.	365 dagen, als de gebruiker 'onthouden inloggegevens' aanklikt 30 dagen.	Deze persoonsgegevens zijn functioneel: het gegeven zorgt er voor dat je met slechts één handeling inlogt in het verschillende databases.	Functioneel beheerder

	Categorie persoonsgegevens	Ingang bewaartermijn	Termijn van bewaring	Motivatie bewaring	Verantwoordelijkheid voor verwijdering
1.					
2					
3.					

infotekst

De privacyregelgeving geeft als beginsel dat persoonsgegevens niet langer in een vorm die het mogelijk maakt de betrokkenen te identificeren, mogen worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is. Met andere woorden: indien het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd. Op dit beginsel van opslagbeperking maakt de privacyregelgeving een uitzondering indien de persoonsgegevens uitsluitend worden verwerkt ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkenen te beschermen.
Bij conceptregelgeving zal moeten worden bepaald en gemotiveerd of het al dan niet wenselijk is om een specifieke minimale of maximale bewaartermijn voor te schrijven. Aan de hand van het uitgangspunt dat de bewaartermijn in verhouding moet staan met de verwerkingsdoeleinden, moet de gekozen termijn worden gemotiveerd. Motiveer ook het niet opnemen van een bewaartermijn.
Bij overheidsverwerkingen moet worden nagegaan of regelgeving een bewaartermijn voorschrijft. Indien dat het geval is, moet de verwerkingsverantwoordelijke zich aan die termijn houden. Indien geen wettelijke bewaartermijn is voorgeschreven, moet de verwerkingsverantwoordelijke zelf bewaartermijnen vaststellen of de gegevens periodieke toetsen aan het beginsel van opslagbeperking.
Hierbij moet rekening worden gehouden met andere regelgeving over bewaartermijnen, zoals de Archiefwet 1995.
Voorbeeld opsomming bewaartermijn voor persoonsgegevens bij overheidsverwerkingen (IT/uitvoering):
Categorie Persoonsgegeven / Ingang bewaartermijn / Termijn van bewaring / Motivatie bewaring / Verantwoordelijkheid voor verwijdering

Naam / Vanaf moment dat de betrokkene voor het eerst inlogt in het systeem / 365 dagen, als de gebruiker 'onthouden inloggegevens' aanklikt 30 dagen / Deze persoonsgegevens zijn functioneel: het gegeven zorgt er voor dat je met slechts één handeling inlogt in het verschillende databases / Functioneel beheerder

[3] Let op: als een verwerkingsverantwoordelijke een bewaartermijn bepaalt, betekent dat niet automatisch dat die ook wordt nageleefd, of dat die termijn ook automatisch in software van een verwerker wordt nageleefd. Kijk ook naar gegevens in backups of logbestanden.

DEEL B

11. Rechtsgrond

De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Als uitwerking van dit beginsel is geregeld dat een gegevensverwerking alleen rechtmatig is indien deze gebaseerd kan worden op ten minste één van de volgende zes rechtsgronden:

a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
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 belangen, met name wanneer de betrokkene een kind is.

Of de gegevensverwerkingen noodzakelijk zijn, wordt beoordeeld onder punt 14.

In deze DPIA zijn de volgende relevant:

12. Bijzondere persoonsgegevens

Er worden geen bijzondere persoonsgegevens verwerkt of verstrekt vanuit Cognos naar de Azure omgeving. Dit punt kan dan ook buiten beschouwing worden gelaten.

13. **Doelbinding**

De privacyregelgeving geeft als beginsel dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en vervolgens niet verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze.

De AVG regelt dat de verdere verwerking voor een ander doel toegestaan is indien de verdere verwerking berust 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, bijvoorbeeld de nationale veiligheid, de openbare veiligheid, monetaire, budgettaire of fiscale aangelegenheden. Daarnaast wordt de verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden als verenigbaar geacht met de oorspronkelijke doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkene te beschermen.

Bij conceptregelgeving moet worden beoordeeld of het noodzakelijk is om wettelijk te regelen dat verdere verwerking toegestaan is (zie ook punt 14 hierna), bijvoorbeeld in verband met de doorbreking van een geheimhoudingsplicht.

Binnen het hierboven geschetste kader voor verwerking voor een ander doel bestaat ruimte voor een wettelijke regeling op grond waarvan sets van persoonsgegevens van meerdere partijen uit meerdere domeinen worden gecombineerd ten behoeve van een big data analyse, waarbij gegevens worden verwerkt ten behoeve van een in die wettelijke regeling vastgesteld doeleinde, dat niet met het oorspronkelijke doel waarvoor de gegevens zijn verzameld, verenigbaar is. Dit laat onverlet dat de verwerkingsverantwoordelijke die beslissingen neemt ten aanzien van individuele personen of een groep van personen op basis van de uitkomsten van die analyse zelfstandig moet voldoen aan alle eisen voor rechtmatige gegevensverwerking. Een dergelijke verwerking dient op een eigen rechtsgrond te berusten (zie punt 11).

Bij overheidsverwerkingen moet de verwerkingsverantwoordelijke zelf beoordelen of de verdere gegevensverwerking voor een ander doel toegestaan en verenigbaar is aan de hand van:

a) het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
b) de context waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke betreft;
c) de aard van de persoonsgegevens, met name bijzondere of strafrechtelijke persoonsgegevens;
d) de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkene;
e) het bestaan van passende waarborgen.

De Richtlijn staat de verdere verwerking van persoonsgegevens toe voor een doelstelling die binnen het toepassingsgebied van de Richtlijn valt, niet zijnde die waarvoor zij zijn verzameld, voor zover:

a) de verwerkingsverantwoordelijke overeenkomstig de wet gemachtigd is deze persoonsgegevens voor een dergelijk doel te verwerken; en
b) de verwerking noodzakelijk is en in verhouding staat tot dat andere doel.

De verdere verwerking voor andere doeleinden is enkel op basis van de wet toegestaan. Wanneer de persoonsgegevens voor zulke andere doeleinden worden verwerkt, is de AVG van toepassing

Doelbinding is één van de kernbeginselen uit artikel 5 van de AVG. In artikel 5(1)b is gespecificeerd dat persoonsgegevens alleen voor **welbepaalde**, **uitdrukkelijk omschreven** en **gerechtvaardigde doeleinden** mogen worden verzameld en vervolgens niet verder mogen verwerkt op een met die doeleinden onverenigbare wijze worden verwerkt. Verantwoordelijken moeten kunnen bewijzen op grond van artikel 5(2) van de AVG dat zij dit beginsel naleven (verantwoordingsplicht).

14. 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 de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden

b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder

Alle gegevensverwerkingen moeten voldoen aan de beginselen van noodzaak en evenredigheid. Het begrip noodzaak bestaat uit twee samenhangende begrippen, namelijk proportionaliteit en subsidiariteit. De persoonsgegevens die worden verwerkt, moeten noodzakelijk zijn voor het doel van de verwerking. **Proportionaliteit** betekent dat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding staat tot de verwerkingsdoeleinden. **Subsidiariteit** betekent dat de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, kunnen worden verwezenlijkt.

Evenredigheid betekent dat er een evenwicht is tussen de belangen van de betrokkene en de belangen van de verwerkingsverantwoordelijke. Een evenredige gegevensverwerking houdt in dat de hoeveelheid verwerkte gegevens niet buitensporig is in verhouding tot het doel van de verwerking. Als een verantwoordelijke zijn doel kan bereiken door minder persoonsgegevens te verwerken, moet hij de hoeveelheid verwerkte persoonsgegevens beperken tot wat noodzakelijk is.

Daarom mag een verantwoordelijke alleen die persoonsgegevens verwerken die noodzakelijk zijn om het legitieme doel te bereiken, maar geen persoonsgegevens waar hij ook buiten kan. De toepassing van het beginsel van proportionaliteit is dus nauw verwant aan de beginselen van dataprotectie uit artikel 5 van de AVG.

14.1. Beoordeling proportionaliteit

De kernvragen zijn: zijn de belangen goed afgewogen? En gaat de verwerking niet verder dan wat nodig is? Om te beoordelen of de verwerking in verhouding staat tot het belang van de verwerkingsverantwoordelijke(n), moet de verwerking voldoen aan de beginselen van artikel 5 van de AVG.

De gegevens moeten "**rechtmatig, eerlijk en transparant** worden verwerkt ten opzichte van de betrokkenen" (artikel 5, lid 1, onder a), van de AVG). Dit betekent dat de betrokkenen op de hoogte moeten worden gebracht van de verwerking van hun gegevens, dat alle wettelijke voorwaarden voor gegevensverwerking worden nageleefd en dat het evenredigheidsbeginsel in acht wordt genomen.

Aanvullen met specifieke info DPIA

14.2. Beoordeling subsidiariteit

De hamvraag bij dit onderdeel van de beoordeling van de noodzaak van de verwerkingen is of dezelfde doelen bereikt kunnen worden met minder inbreukmakende middelen.

infotekst

De privacyregelgeving geeft als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. Dit beginsel van minimale gegevensverwerking/dataminimalisatie komt verder tot uitdrukking door het gebruik van het woord 'noodzakelijk' in artikel 6 AVG en artikel 8 Richtlijn. De AVG en Richtlijn eisen hiermee dat de gegevensverwerking noodzakelijk is voor het verwezenlijken van de doeleinden. De gegevensverwerking moet daarbij voorts de toets aan de beginselen van proportionaliteit en subsidiariteit kunnen doorstaan.
Proportionaliteit betekent dat moet worden beoordeeld of de indringendheid van de voorgenomen gegevensverwerking in een redelijke verhouding staat tot het doel. Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen (zijn de beperkingen van het grondrecht en het doel dat met de verwerking wordt beoogd met elkaar in balans?). Daarbij zal onder meer moeten worden gekeken of de voorgenomen gegevensverwerking effectief is om het beoogde doel te bereiken en of de aangevoerde redenen relevant en toereikend zijn om het beoogde doel te bereiken.
Daarbij kunnen empirische onderzoeksresultaten helpen.
Bij subsidiariteit wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt. Bijvoorbeeld:

a. kan bij het gebruik van bijzondere of strafrechtelijke persoonsgegevens hetzelfde resultaat behaald worden met gebruikmaking van een combinatie van gewone persoonsgegevens?
b. kan het verwerken van de persoonsgegevens in een beperktere vorm of met minder verwerkingen?

Zo kan in bepaalde gevallen met foto's hetzelfde doel worden bereikt (bijvoorbeeld: identificatie) als met het verwerken van filmbeelden.
Het subsidiariteitsbeginsel houdt bijvoorbeeld ook in dat als persoonsgegevens openbaar gemaakt gaan worden, niet automatisch alle persoonsgegevens openbaar worden gemaakt, maar een selectie wordt gemaakt op grond van gerechtvaardigde criteria. Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht in onderdeel A betrokken.
Bij conceptregelgeving kunnen de uitkomsten van deze afweging worden meegenomen in de grondrechtentoets van het IAK.

15. **Rechten van betrokkenen**

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

		Geregeld?	**Korte beschrijving hoe?**
1.	Recht op informatie	Ja/nee	
2.	Recht op inzage		
3.	Recht op correctie		
4.	Recht op verwijdering		
5.	Recht op beperking van de verwerking		
6.	Recht van bezwaar		
7.	Recht van herroeping		

infotekst

Betrokkenen hebben op grond van de privacyregelgeving diverse rechten, waarin ook staat op welke wijze en onder welke omstandigheden zij die rechten kunnen uitoefenen. Het betreft het recht op informatie, het recht van inzage, het recht op rectificatie, het recht op gegevenswissing, het recht op beperking van de verwerking, een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens, het recht op overdraagbaarheid van gegevens, het recht van bezwaar en het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. Er zijn uitzonderingen mogelijk op de uitoefening van deze rechten, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang. Uitzonderingen moeten altijd op een nationale wet berusten, direct zijn toegestaan op grond van de bepalingen in de Europese privacyregelgeving.

Indien in conceptregelgeving een uitzondering wordt gemaakt op de rechten van betrokkenen moet worden beoordeeld of dit is toegestaan op in de privacyregelgeving genoemde gronden én moeten specifieke bepalingen worden opgenomen met betrekking tot ten minste:

a. de verwerkingsdoeleinden;
b. de categorieën van persoonsgegevens;
c. het toepassingsgebied van de ingevoerde beperkingen;
d. de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte
e. de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
f. de opslagperiodes en de toepasselijke waarborgen;
g. de risico's voor de rechten en vrijheden van betrokkenen;
h. het recht van betrokkenen om over de beperking te worden geïnformeerd, tenzij dit afbreuk kan doen aan het doel van de beperking.

Geef bij overheidsverwerkingen aan hoe invulling wordt gegeven aan de rechten van betrokkenen, bijvoorbeeld op welke wijze de betrokkenen worden geïnformeerd en hoe wordt omgegaan met een aanvraag voor correctie en wissing van gegevens. Indien de verwerkingsverantwoordelijke uitzonderingen wil maken op de uitoefening van bepaalde rechten van betrokkenen, geef aan waarom dat noodzakelijk is en op welke grond dat is toegestaan.

DEEL C

16. **Risico's**

16.1. Toelichting

Een DPIA gaat over de risico's voor betrokkenen. Dus niet zozeer over de beveiligings-, continuïteits- of andere risico's die de organisatie die de DPIA uitvoert loopt. Dit maakt de insteek verwant aan die van andere vakgebieden, maar is deze toch fundamenteel anders dan de risico analyses uit die andere vakgebieden.

In dit hoofdstuk worden de risico's bepaald en onderzocht wat de kans en gevolgen van de risico's zijn. In Deel D volgen de maatregelen waarmee de risico's eventueel beperkt (gemitigeerd) kunnen worden.

De Engelse toezichthouder ICO heeft een lijst met hoofdcategorieën van risico's opgesteld.

- Verlies van controle op het gebruik van de gegevens
- Verlies van vertrouwelijkheid
- Onmogelijkheid voor betrokkenen om hun rechten uit te oefenen
- Heridentificatie van gepseudonimiseerde gegevens
- Onrechtmatige (verdere) verwerking

Op basis van deze algemene lijst met risico kunnen de specifieke risico's binnen deze DPIA worden vastgesteld en vervolgens worden geplot in een zogenaamde risicomatrix. Zie daarvoor het figuur hieronder. De uitkomst (het risico) wordt bepaald aan de hand van de gevolgen (minimaal, enige, ernstige) en de kans (heel klein, redelijke mogelijkheid, waarschijnlijker dan niet). De invulling van de kans en de gevolgen vraagt een inschatting.

- Hoog risico → De gevolgen voor de betrokkene hebben bij het materialen van het risico forse invloed op het leven van de betrokkene
- Middel risico → De gevolgen voor de betrokkene hebben bij materialiseren van het risico geen beperkte impact op het leven van de betrokkene
- Laag risico → De gevolgen voor de betrokkene hebben materialiseren van het risico weinig of verwaarloosbare invloed op het leven van de betrokkene

Ernst van de gevolgen voor de betrokkene(n)				
	Ernstige gevolgen	Laag risico	Hoog risico	Hoog risico
	Enige negatieve gevolgen	Laag risico	Medium risico	Hoog risico

	Minimale gevolgen	Laag risico	Laag risico	Laag risico
		Heel klein	Redelijke mogelijkheid	Waarschijnlijker dan niet
		Kans (waarschijnlijkheid) dat het risico zich voordoet		

16.2. Mogelijke risico's

Bij de uitvoering van deze DPIA zijn de volgende risico's geïdentificeerd.

	Risico	**Oorzaak risico**	**Aard risico**	**Kans**	**Impact**
1.					
2.					
3.					
4.					
5.					
6.					

Hieronder volgt een korte toelichting van de risico's.

16.2.1. …

…

Samenvattend, mits …

16.3. Samenvatting van de risico's

In Afbeelding 20 hieronder zijn de risico's in kaart gebracht in de risicomatrix:

Afbeelding 20: Ingevulde risicomatrix

Ernst van de gevolgen	Ernstige gevolgen	Laag risico	Hoog risico	Hoog risico

	Enige negatieve gevolgen	Laag risico	Medium risico	Hoog risico
	Minimale gevolgen	Laag risico	Laag risico	**Laag risico**
		Heel klein	Redelijke mogelijkheid	Waarschijnlijker dan niet
		Kans (waarschijnlijkheid) dat het risico zich voordoet		

infotekst

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. 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.

Volgens de privacyregelgeving dient een PIA een beoordeling van risico's voor de rechten en vrijheden van de betrokkenen te bevatten. Aan de hand van de aard, het toepassingsgebied, de context en de doeleinden van de gegevensverwerking dient de waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkenen te worden bepaald. Op basis van een objectieve beoordeling kan vastgesteld worden of de gegevensverwerking gepaard gaat met een (hoog) risico. Hiervoor is het nodig om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.

Het gaat hier om een risicogerichte benadering die kan bestaan uit de volgende stappen:
1. risico's identificeren;
2. risico's inschatten/analyseren;
3. risico's beoordelen/evalueren.
Deze benadering zal in grote lijnen vergelijkbaar zijn met een risicoafweging in het kader van informatiebeveiliging. Daarom kan ook gebruik gemaakt worden van informatie die daaruit naar voren is gekomen. Anders dan bij deze risicoafweging die gericht is op de betrouwbaarheidseisen voor informatiesystemen, en daarmee de risico's voor de verantwoordelijke (zoals aanpassing, vertrouwen, publiciteit, toezicht en handhaving, dienstverlening, betrouwbare informatie), ziet de risicoafweging van de PIA op de risico's voor de betrokkenen.
De privacyregelgeving schrijft niet voor op welke wijze de risicoanalyse moet worden uitgevoerd. Het verdient aanbeveling om aan te sluiten bij internationale standaarden, bijvoorbeeld van de International Organization of Standardization (ISO), Eenduidige Normatiek Single Information Audit (ENSIA) en Organisation for Economic Co-operation and Development (OECD).

1. Risico's identificeren

De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een kans op het optreden van een negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van persoonsgegevens.
Bij rechten en vrijheden van de betrokkenen moet in eerste instantie aan het recht op privacy worden gedacht, maar ook aan andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van godsdienst en het verbod van discriminatie. Het voordoen van de (hypothetische) situatie kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokkene. Hierbij kan gedacht worden aan de volgende situaties:
- waar de gegevensverwerking kan leiden tot:
- 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;
- wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;
- wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;

- wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt; of
- wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

2. Risico's inschatten

Vervolgens moeten de benoemde risico's worden gekwalificeerd door het inschatten van de kans dat een dreiging zich voordoet en de mogelijke gevolgen daarvan voor de betrokkenen. Met andere woorden: wat zijn de gevreesde gevolgen en hoe groot is de impact daarvan op de betrokkenen? En hoe treden deze in werking en hoe waarschijnlijk is dat? Deze vragen zijn niet gericht op zwart-wit antwoorden, maar op een afweging. Aan de hand hiervan moet een risiconiveau worden bepaald.

De impact/ernst van de risico's hangt af van de context van de verwerkingen: de aard van de persoonsgegevens, de aard van de verwerkingen en de doeleinden waarvoor de gegevens worden verwerkt.

De kans dat de risico's zich voltrekken is mede afhankelijk van de middelen die de verwerkingsverantwoordelijke gebruikt bij de gegevensverwerking. Alsook van de aard van de persoonsgegevens.

Persoonsgegevens die de sleutel vormen voor toegang tot geldelijke middelen of waarmee een betrokkene te chanteren is, zijn aantrekkelijk voor hackers. Denk hierbij aan de inloggegevens voor DigiD of een datingwebsite.

De kans dat zich gevolgen voordoen voor de rechten en vrijheden van de betrokkenen, kan tevens verband houden met de (mate van) beveiliging van de persoonsgegevens. De al dan niet opzettelijke:

- vernietiging en verlies (beschikbaarheid);
- wijziging (integriteit);
- ongeoorloofde toegang en verstrekking (vertrouwelijkheid);

van persoonsgegevens, kan leiden tot schade voor de betrokkene.

Voor het inschatten van de risico's kan het behulpzaam zijn om de betrokkenen of hun vertegenwoordigers te consulteren.

Big data-verwerkingen kunnen specifieke risico's voor de betrokkene met zich brengen. Zo kan een algoritme een correlatie ontdekken die weliswaar in statistische zin logisch is, maar die kan leiden tot vooroordelen en stereotypering, discriminatie en sociale uitsluiting of anderszins impact heeft op de betrokkenen, bijvoorbeeld bij sollicitaties, het aangaan van leningen en afsluiten van verzekeringen. Ook bestaat het risico dat de betrokkene onderworpen is aan big data-besluitvorming die hij niet begrijpt en waar hij geen invloed op heeft.

3. Risico's beoordelen

Definieer aanvaardbare risicowaarden en beoordeel of de risico's aanvaardbaar zijn.

DEEL D

17. Maatregelen

- Maatregelen koppelen aan de genoemde risico's. Dat kan met de nummers als referentie.
- Maak voor de maatregelen onderscheid tussen welke betrokken partijen de maatregelen moeten treffen.
- Beoordeel of na het treffen van de maatregelen er geen hoge risico's meer resteren.

17.1. Overzicht van maatregelen

Nr.	Risico	Soort Maatregelen	Aanbevolen maatregel
1.			
2.			

Risk no.	Omschrijving risico	Risico beoordeling	Maatregelen
1		Laag / medium/ hoog	
2			
3			
5			
6			

17.2. Beoordeling risico's na nemen maatregelen

Als er nog het nemen van de maatregelen nog hoge risico's overblijven, dan is consultatie bij Autoriteit Persoonsgegevens nodig.

Op basis van bovenstaande analyse volgt dat na het nemen van de maatregelen

17.3.Conclusie

Korte samenvatting uitkomsten.

Indien alle maatregelen worden getroffen, dan is uiteindelijk de uitkomst…

De uiteindelijke aanbeveling is om de software/proces/dienst/systeem [kies een optie]

1. uit te rollen
2. aan te passen op de volgende wijze
3. af te blazen

infotekst

Denk bij maatregelen bijvoorbeeld aan: het extra informeren van de betrokkenen, een extra keuze-, inspraak- of bezwaarmogelijkheid voor de betrokkenen, periodieke controles, toezicht verstevigen, verhogen bewustwording en dataminimalisatie.

Daarnaast kunnen de maatregelen ook beveiligingsmaatregelen omvatten. De privacyregelgeving geeft als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op een dusdanige manier wordt verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

De verwerkingsverantwoordelijk moet passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. In het begrip passend ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het begrip passend duidt mede op een proportionaliteit tussen de maatregelen en erkende privacyrisico's. Naarmate de risico's groter zijn, worden zwaardere eisen gesteld aan de beveiliging van de persoonsgegevens. Er is geen verplichting om altijd de zwaarste beveiliging te nemen. Enkel is vereist dat de maatregelen met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn. Deze maatregelen moeten het risico tot een aanvaardbaar niveau brengen. Beveiligingsrisico's volledig reduceren is niet mogelijk. Dit betekent dat er altijd een restrisico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe hij tot dit restrisico is gekomen en waarom dit aanvaardbaar wordt geacht.
Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en controlcyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.

Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismen.
Ter illustratie noemt de AVG de volgende maatregelen:
a. pseudonimiseren en versleutelen van persoonsgegevens;
b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.
Daarnaast kan worden gedacht aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:
- fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- opslag van gegevens in een kluis;
- project-, risico- en incidentenmanagement;
- data opsplitsen;
- dataminimalisatie;
- back-ups;
- integriteitscontroles;
- meerfactor-authenticatie;
- monitoring en logging;
- controle van toegekende bevoegdheden;
- privacybewustzijn- en beveiligingstrainingen;
- managementrapportages over risicobeheer;
- beperken inzageniveau;
- periodiek een audit of hack- of penetratietest uitvoeren;
- richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- responsible-disclosurebeleid;
- geheimhoudingsverklaringen;
- service level agreements (met boeteclausules);
- verwerkersovereenkomsten;
- screening personeel en VOG-verklaring.

Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die voortvloeien uit de Baseline Informatiebeveiliging Rijksdienst (BIR).

De Richtlijn noemt tot slot de volgende maatregelen:
a. controle op de toegang tot de apparatuur;
b. controle op de gegevensdragers;

c. opslagcontrole;
d. gebruikscontrole
e. controle op de toegang tot gegevens;
f. transmissiecontrole;
g. invoercontrole;
h. transportcontrole; en
i. herstelmogelijkheid.

De Richtlijn verplicht tot het bijhouden van logbestanden van bepaalde vormen van verwerkingen, opdat het mogelijk is de reden, datum en het tijdstip van die handelingen te achterhalen en indien mogelijk de identiteit van de persoon die de persoonsgegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die persoonsgegevens.
Bij conceptregelgeving: ook op het niveau van regelgeving kunnen maatregelen worden getroffen. Denk hierbij aan het voorschrijven van maximum bewaartermijnen, het beperken van inzage in en besluiten over persoonsgegevens tot bepaalde functionarissen of geheimhoudingsverplichtingen.

18. **Advies FG**

Beschrijf hier het advies van de FG

Bijlage 1: