Gegevensbeschermingseffectbeoordeling (PIA)
Feitelijke registratie CIMS

VWS/RIVM/DVP/Feitelijke registratie CIMS

Directie Bedrijfsvoering

Bilthoven, 8 december 2020

Vaststelling verwerkersverantwoordelijke: Selecteer/typ datum
Naam: Typ naam/functie

Advies functionaris voor gegevensbescherming: Selecteer/typ datum
Naam: Typ naam/functie

Advies CIO: Selecteer/typ datum
Naam: Typ naam/functie

Gegevensbeschermingseffectbeoordeling (PIA)

VWS/RIVM/DVP/Feitelijke registratie CIMS

Directie Bedrijfsvoering

Contact:

Ministerie van VWS, directie RIVM
Bedrijfsvoering
DVP

Versie: 0.1

Inhoudsopgave

Inleiding

De PIA voor het Rijksvaccinatieprogramma-CIMS (Covid-19 Informatie en monitoring systeem), Feitelijke registratie CIMS vormt een belangrijk onderdeel om inzicht te verschaffen in de wijze waarop door RIVM-DVP met persoonsgegevens en bijzondere persoonsgegevens wordt omgegaan. Het programma CIMS maakt voor de uitoefening van de wettelijk vastgestelde taken gebruik van grote aantallen persoonsgegevens en bijzondere persoonsgegevens. Om iedereen in de gelegenheid te stellen gevaccineerd te worden tegen Covid-19 wordt gebruik gemaakt van een afslag van gegevens uit de BRP. Hiervoor is een apart autorisatiebesluit opgesteld en beschikbaar op basis waarvan de feitelijke registratie van vaccinatiegegevens per individu plaats kan vinden.
De feitelijke registratie van vaccinatiegegevens is er op gericht om .

De Minister van VWS is verantwoordelijk voor [ ], voor de daar uit voortvloeiende uitvoering en voor het uitvoeren van de DPIA. In de praktijk ligt die verantwoordelijkheid bij het RIVM.

De verwerking van gegevens door partijen ("prikkers") op de uitvoeringslocatie valt buiten de scope van de onderhavige PIA. Het RIVM is de ontvanger van deze gegevens en tevens ook verwerker voor landelijke gegevens.

Betrokken bij het DPIA proces:

Aanvrager/opdrachtgever [vaststelling DPIA] : Hoofd. Dienst Vaccinvoorziening en Preventieprogramma's, RIVM DVP

Organisatie onderdelen betrokken bij de coördinatie en uitvoering van de Registratie Vaccinatie COVID-19

- *Informatiemanager tevens Privacy Coördinator* Dienst Vaccinvoorziening en Preventieprogramma's, RIVM DVP
- *DVP- BIS /Functioneel ontwerper CIMS*
- *Productowner CIMS Clientportaal en accountmanager rijksvaccinatieprogramma*

Procesbegeleiders vanuit RIVM

- Privacy Officer RIVM
- Gezondheidsjurist RIVM-CVB
- Adviseur Informatiebeveiliging CIO-Office
- Chief Information Security Officer
- Chief Information Officer
- Security Officer Shared Service Centre Campus (SSC)

Procesbegeleiders vanuit VWS

- Privacy jurist, VWS Directie WJZ
- CISO en CIO VWS kern

Observator

- Functionaris Gegevensbescherming, VWS.

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel

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

Een van de wettelijke taken van het RIVM is het uitvoeren van het Rijksvaccinatieprogramma. Onderdeel van het Rijksvaccinatieprogramma wordt de COVID-19 vaccinatie. Hiervoor is een wetswijziging in de maak die in januari 2021 van kracht wordt (aanpassing Besluit Publieke Gezondheid). Dit betekent dat mogelijk de feitelijke registratie van vaccinatiegegevens al eerder gaat beginnen dan dat dit besluit is aangepast. Hiervoor is nog geen aparte grondslag aanwezig. Het systeem dat hier voor zorg gaat dragen is het Covid-19 Informatie en monitoring systeem, CIMS.
Deze GEB maakt het mogelijk inzicht te verschaffen in de noodzakelijke verwerking van persoons- en vaccinatiegegevens van de personen ten behoeve van de doelstelling van centrale registratie in CIMS.

2. Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

Klik hier om infotekst te verbergen

Beschrijf allereerst alle te verwerken categorieën van persoonsgegevens. Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
Natuurlijke personen wil zeggen mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in beginsel geen persoonsgegeven. Deze informatie kwalificeert weer wel als persoonsgegeven indien die ook betrekking heeft op een levende persoon.
Om te bepalen of iemand identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om de persoon te identificeren.
Gepseudonimiseerde (ook wel: versleutelde) gegevens worden als persoonsgegevens beschouwd. Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende

gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eis verbonden dat deze aanvullende gegevens apart worden bewaard en maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.
Anonieme en geanonimiseerde gegevens zijn geen persoonsgegevens. Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie het gegeven betrekking heeft, niet (meer) identificeerbaar is. Het anonimiseren van persoonsgegevens als zodanig is overigens weer *wel* een verwerking van persoonsgegevens.
Voorbeelden van persoonsgegevens zijn: naam, voorvoegsel, adres, telefoonnummer, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, MAC-adres, KvK- nummer, voertuigidentificatienummer, winst eenmanszaak, bankrekeningnummer en -saldo, IQ, functie, opleiding, inkomens- en vermogensgegevens, kredietwaardigheid, persoonlijke voorkeuren, loonschaal, verslag van een functioneringsgesprek en (wan)gedrag. Ook metadata – informatie over informatie – zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Voorbeelden van metadata zijn: welke browser of telefoon iemand gebruikt, wanneer een document is opgesteld of voor het laatste bewerkt en de geschreven taal. Ook locatie-informatie en geografische informatie kwalificeren als persoonsgegevens als de informatie herleidbaar is tot een persoon. Denk hierbij aan de koppeling van gegevens uit de basisregistratie adressen en gebouwen aan andere gegevens en het monitoren van de locaties van voertuigen.

Typen
Stel vervolgens de aard van de te verwerken categorieën van persoonsgegeven vast. De AVG onderscheidt drie typen van persoonsgegevens – gewone, bijzondere en strafrechtelijke persoonsgegevens – en stelt verschillende eisen aan een rechtmatige verwerking daarvan. De gedachte hierachter is dat hoe gevoeliger de aard van de persoonsgegevens, hoe groter de effecten voor de betrokkenen zijn.

Bijzondere persoonsgegevens
Hieronder een limitatieve opsomming van categorieën van bijzondere persoonsgegevens:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens over seksueel gedrag of seksuele gerichtheid.

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekers-app worden verwerkt, ziekte- en verzuimgegevens van werknemers, ledenlijst van een politieke partij, relatiestatus op sociale media. Let op: uit beeldmateriaal zoals foto's en camerabeelden kunnen soms ook bijzondere persoonsgegevens, zoals etnische afkomst of medische gesteldheid, worden afgeleid.

Genetische gegevens
Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over zijn fysiologie of gezondheid en die met name voortkomen uit een analyse van een biologisch monster van die persoon. Denk hierbij aan: chromosomen, DNA of RNA en erfelijke ziekten.

Biometrische gegevens
Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking

met fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd. Denk hierbij aan: vingerafdrukken, irispatroon, gezichtsprofiel, toetsaanslaganalyse, looppatroon, stemgeluid en slaapritme. Foto's vallen overigens alleen onder de definitie van biometrische gegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie mogelijk maken.

Gegevens over gezondheid
Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon. Denk hierbij aan: gewicht, hartslag, handicap, ziekterisico of verleende gezondheidsdiensten.

Strafrechtelijke persoonsgegevens
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (hierna: strafrechtelijke persoonsgegevens) zijn een apart type persoonsgegeven. Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Voorbeelden hiervan zijn: proces-verbaal, sepotbeslissing, strafblad, relaas verhoor en aanvraag voor een toevoeging in een strafzaak.

Wettelijke identificatienummers
Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Denk hierbij aan: een burgerservicenummer (BSN), BIGnummer (beroepen in de individuele gezondheidszorg), A-nummer (basisregistratie personen), onderwijsnummer, strafrechtketennummer en kenteken. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers.

Overige persoonsgegevens
Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk worden in dit model aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens wil overigens niet zeggen dat geen sprake is van een hoog privacyrisico. Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog privacyrisico met zich brengen. Hierbij kan gedacht worden aan:

- gegevens over de financiële of economische situatie van de betrokkene;
- gegevens over overtredingen van wettelijke voorschriften, bestuurlijke en/of tuchtrechtelijke maatregelen of sancties;
- (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- gegevens die betrekking hebben op kwetsbare groepen;
- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits)fraude;
- communicatieen locatiegegevens.

Betrokkenen
Benoem tot slot de categorieën van betrokkenen van wie de persoonsgegevens worden verwerkt. Denk hierbij aan: medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers of ingezetenen van een gemeente. De omvang en categorie van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere (zie ook de anderszins gevoelige persoonsgegevens). Denk bijvoorbeeld aan: minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, medewerkers van inlichtingen- en veiligheidsdiensten, klokkenluiders of informanten van politie of justitie.

Betrokkenen hebben op grond van de privacyregelgeving bepaalde rechten, zoals het inzage- en correctierecht.

De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader. Die specifieke bescherming geldt met name voor het gebruik van persoonsgegevens van kinderen voor marketingsdoeleinden, het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. Zo is wanneer het kind jonger is dan 16 jaar zo'n verwerking slechts rechtmatig, indien de toestemming of machtiging tot toestemming wordt verleend door de ouder of voogd. Ook heeft de leeftijd van betrokkenen gevolgen voor de wijze waarop hij ge'informeerd moet worden.
In het kader van de Richtlijn kan het onderscheid worden gemaakt tussen:

a. personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;
b. personen die voor een strafbaar feit zijn veroordeeld;
c. slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit; en
d. andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek naar strafbare feiten of een daaruit voortvloeiende strafrechtelijke procedure, personen die informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met een van de personen bedoeld onder a en b.

Bij **conceptregelgeving** kan het wenselijk zijn om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen. Wanneer de verwerking onder de werkingssfeer van de Richtlijn valt, is het verplicht om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen.

1. Gewone persoonsgegevens: op basis van aangeleverde lijsten worden persoonsgegevens gechecked met hetgeen in CIMS staat (clientbeheer). BSN + zorgnummer, NAW-gegevens, incl. postcode/huisnummer, geboortedatum
2. Vaccinatiegegevens per individu: batchnummer van het vaccin, productnaam, toedieningsdatum, uitvoerder.

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

VERWERKINGEN
Na het aanleveren van vaccinatiegegevens per individu vindt verwerking van deze gegevens plaats in CIMS. Het importeren van de aangeleverde gegevens wordt geautomatiseerd door middel van een script. Vervolgens wordt handmatig gekeken naar mogelijk oorzaken van geconstateerde fouten.
Naast persoonsgegevens wordt ook het selectiecriterium meegestuurd. Dit betreft het vaststellen van de doelgroep, namelijk op medische indicatie, beroepsgroep en leeftijdsindicatie.

4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Klik hier om infotekst te verbergen

De privacyregelgeving geeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijk voorwaarde om te kunnen beoordelen of de voorgenomen gegevensverwerkingen rechtmatig zijn (onder B) en om vast te stellen welke maatregelen moeten worden getroffen om de risico's (onder C) te voorkomen of verkleinen (onder D). Omschrijf daarom per voorgenomen gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk.
Bij verwerkingsdoeleinden kan gedacht worden aan: beveiligen van gebouwen en objecten, behandelen van personeelszaken, opsporen van strafbare feiten, direct marketing, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoeleinden moeten zoveel mogelijk worden toegespitst op de concrete gegevensverwerking, waarbij het algemene overkoepelende doel kan worden gebruikt als kapstok waaraan verschillende subdoelen kunnen worden gehangen. bijvoorbeeld:

- e-mailadres: noodzakelijk voor communicatie met betrokkene;
- ip-adres: noodzakelijk ter verificatie dat alleen vanuit een bepaalde locatie contact wordt gemaakt met het systeem;
- adresgegevens: noodzakelijk om een beschikking naar de betrokkene te kunnen toezenden;
- financiële gegevens: noodzakelijk om vast te stellen of de betrokken partij in aanmerking komt voor een toeslag;
- strafrechtelijke gegevens: noodzakelijk om een screening te kunnen uitvoeren.

Wanneer de persoonsgegevens niet rechtstreeks bij de betrokkene worden verkregen (met andere woorden: de persoonsgegevens zijn afkomstig van een andere persoon of organisatie dan wel uit een bestaand databestand), is het noodzakelijk om de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld te herleiden. De privacyregelgeving geeft namelijk als beginsel dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Met andere woorden: de verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, mag enkel indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld (zie voor de beoordeling van de verenigbaarheid punt 13 hieronder). Met verdere verwerking wordt

gedoeld op gebruik van persoonsgegevens die al eerder voor een bepaald doel zijn verzameld. Denk hierbij aan verstrekkingen van persoonsgegevens aan een andere organisatie die niet oorspronkelijk, ten tijde van het verzamelen van de gegevens, was beoogd.

Bij **conceptregelgeving** wordt het doel van de gegevensverwerking in de regeling zelf vastgelegd of op zijn minst benoemd in de memorie of nota van toelichting. Een wettelijke doelomschrijving bevordert de rechtszekerheid omdat hierdoor een nadere invulling is gegeven aan het beoordelingskader.
Bij **overheidsverwerkingen** stelt de verwerkingsverantwoordelijke het doel van de gegevensverwerkingen zelf vast. Bij overheidsverwerkingen ter uitvoering van regelgeving moet binnen het doel worden gebleven dat daarin is vastgesteld. Het verdient de voorkeur de verwerkingsdoeleinden zoveel mogelijk op het niveau van werk- en organisatieprocessen te enten.

Op basis van artikel 6b van de Wet publieke gezondheid draagt de minister via het RIVM zorg voor de regie op en de coördinatie van de uitvoering, alsmede de registratie, bewaking en evaluatie van het rijksvaccinatieprogramma. Het ministerie van VWS is voornemens om het Besluit publieke gezondheid te wijzigen ten behoeve van de opname van het COVID-19 vaccin in het Rijksvaccinatieprogramma. Daarmee zal - indien een COVID-19 vaccin beschikbaar komt - de wettelijke taak van het RIVM ten aanzien van de uitvoering van het COVID-19 vaccin zijn vastgelegd. Als onderdeel van de vaccinatiestrategie van het COVID-19 vaccin zal het RIVM bepaalde leeftijdsdoelgroepen selecteren en oproepen om zich te laten vaccineren. Daarnaast zal het RIVM de van de uitvoerder(s) ontvangen vaccinatiegegevens van gevaccineerde moeten koppelen aan een persoon in CIMS. Het doel hiervan is:

1. Goede en veilige patiëntenzorg: elke arts dient bij twijfel een centraal register te kunnen raadplegen om zekerheid te verkrijgen over covidvaccinaties.
   N.B.: dit zal in eerste instantie via een tussenstap gaan, aangezien het zorgverlenerportaal nog niet gerealiseerd is. Tevens bestaat er op dit moment nog veel onduidelijkheid over de identificatiemiddelen voor zorgverleners die door een portaal gebruikt kunnen worden. Inzage voor zorgverleners zou bijvoorbeeld op afspraak kunnen, waarbij contact wordt opgenomen met het regiokantoor van DVP. Procedures hiervoor zijn beschikbaar.
2. Bestrijding van de pandemie: beschikbaarheid van landelijke data ten tijde van de bestrijding van de COVID-19 uitbraak t.b.v. monitoren van bijwerkingen en zo nodig ingrijpen.
3. Waarschuwen van personen bij calamiteiten en het inrichten van aansprakelijkheidswaarborgen (zie gevoerde rechtzaken ten tijde van de de Mexicaanse griep)
4. Uitvoeren van de vaccinatiecampagne o.b.v. selectiecriteria medische indicatie, leeftijd en beroepsgroep
5. Beperken administratieve lasten t.b.v. snel handelen: Als er onverhoopt sprake is van een kwaliteitsafwijking in een productiebatch kan deze eenvoudig teruggeroepen worden ('recall').
6. Praktisch belang voor de burger, door op het juiste moment uitnodigen voor een tweede vaccinatie en het kunnen leveren van een vaccinatiebewijs in een latere fase.

4. 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.

Betrokken partij	Rol	Toegankelijk voor
RIVM-DVP	Verantwoordelijk/ontvanger /verstrekker/verwerker	Clientbeheerders, mdw. Primair proces CIMS, functioneel beheerders, medisch adviseurs
Ordina BV	Verwerker als technisch applicatiebeheerder CIMS	applicatiebeheer Ordina
SSC-Campus/IV Organisatie	Beheer CIMS	Beheerders
GGD-arts infectieziektenbestrijding	Verstrekker/ontvanger kunnen informatie opvragen	RVP-medewerkers regiokantoren DVP

4. Belangen bij de gegevensverwerking

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

Algemeen belang: voor RIVM voldoen aan wettelijk taak, in het kader van de volksgezondheid namelijk het registreren van gegeven Covid-19 vaccinaties. Tevens wordt het mogelijk de vaccinatiegraad te kunnen berekenen aan de hand van binnengekomen vaccinatiegegevens per persoon, afgezet tegen oproepgegevens.
Privaat belang: belang voor direct betrokkenen, namelijk de gevaccineerden zelf. Mogelijkheid tot centrale uitgifte vaccinatiebewijzen vraagt om up to date gegevens uit de BRP.
Belang zorgverleners: voor zorgverleners is het van belang dat centrale registratie van gevaccineerden mogelijk is wanneer er problemen ontstaan met eigen systemen.
Financieel belang: verrekeningen tbv zorgverleners, maar ook leveranciers. Verrekening met zorgverleners is nog niet besproken of besloten.

4. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Klik hier om infotekst te verbergen

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) privacytoezichthouder.

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.

Nederland

4. 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, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Klik hier om infotekst te verbergen

Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, profilering en big data-verwerkingen.

Geautomatiseerde besluitvorming

Uitsluitend op geautomatiseerde verwerking gebaseerde besluiten die voor de betrokkenen rechtsgevolgen hebben of hem anderszins in aanmerkelijke mate treffen, zijn in beginsel verboden.

Voor verwerkingen die onder de werkingssfeer van de AVG vallen, geldt dat dit verbod niet van toepassing indien het besluit:

a. noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
b. is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of
c. berust op de uitdrukkelijke toestemming van de betrokkene.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn geldt dit verbod niet indien het besluit:

a. wettelijk is toegestaan; en
b. voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkenen, waaronder ten minste het recht op menselijke tussenkomst.

Profilering

Onder profilering wordt verstaan: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Bepaalde gegevens, zoals de resultaten van een zoekopdracht met een zoekmachine, kunnen in combinatie met elkaar een risicoprofiel doen ontstaan. De kans hierop bestaat vooral wanneer meerdere registers met elkaar worden gecombineerd. Er kan sprake zijn van profilering wanneer:

- op basis van een combinatie van persoonsgegevens, zoals het automerk in combinatie met de leeftijd van de betrokkene wordt besloten iemand extra te controleren;
- gebruik wordt gemaakt van de gegevens die websitebezoekers achterlaten om de doelgroep van de website mee vast te stellen.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn, geldt dat profilering die leidt tot discriminatie op grond bijzondere persoonsgegevens verboden is.

Big data

Big data is als zodanig niet gedefinieerd in de privacyregelgeving, maar hangt als verschijnsel nauw samen met geautomatiseerde besluitvorming en profilering. *Big data* staat voor het verschijnsel dat grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen worden geanalyseerd waarbij geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau. In de kern komt het bij *big data*-analyses neer op het zoeken naar correlatie (onderlinge samenhang tussen twee reeksen van waarnemingen), in tegenstelling tot causaliteit (betrekking van oorzaak en gevolg). Toepassing van *big data* brengt specifieke risico's mee en vergt daarom ook specifieke maatregelen (zie onder D).

Nieuwe technologieën

Ook grote verschuivingen in de werkwijze, de manier waarop persoonsgegevens worden verwerkt en de technologie die daarbij gebruikt wordt, kunnen gevolgen hebben voor betrokkenen. Denk aan: intelligente volgsystemen op basis van GPS, biometrie en nieuwe vormen van identificatie.

Onderdeel van CIMS is de CIMS-machine. Dit is een algoritme dat in eigen beheer door RIVM-DVP geparametriseerd kan worden. Dit algoritme heeft twee functies:

- Het evalueren van uitgevoerde vaccinaties, bv bepalen of het interval tussen twee vaccinaties voldoende lang is of dat de juiste producten zijn gebruikt.
- Het plannen van vaccinaties, bv bij product A moet een tweede vaccinatie met product A 4 weken na de eerste gepland worden, bij een persoon met een medische indicatie wordt een serie met product B gepland.

De parameters voor de CIMS-machine worden opgesteld en getest door de medisch adviseurs en een beheerder van CIMS. Deze parameters worden vastgesteld op basis van de richtlijnen voor COVID-vaccinatie die door de medisch adviseurs

4. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

De Covid-19-vaccinatie wordt onderdeel van het Rijksvaccinatieprogramma zoals dat in de Wet publieke gezondheid (Wpg) is opgenomen. Artikel 6b Wpg is de basis voor het landelijke vaccinatieprogramma. Bij algemene maatregel van bestuur, in dit geval het Besluit publieke gezondheid, wordt vastgesteld welke vaccinaties onderdeel zijn van het rijksvaccinatieprogramma en welke groepen in aanmerking komen voor welke vaccinaties. In artikel 11 van het Besluit wordt de vaccinatie voor Covid-19 opgenomen. Deze aanpassing zal pas later een feit zijn dan dat de vaccinaties daadwerkelijk zijn gestart. Dit betekent dat apart naar de onderbouwing voor het verwerken van gegevens gekeken moet worden.
Het RIVM draagt namens de Minister zorg voor de regie op en de coördinatie van de uitvoering, alsmede de registratie, bewaking en evaluatie van het vaccinatieprogramma (artikel 6b lid 2 Wpg). Deze taak volgt tevens uit artikel 3 Wet op het RIVM jo. artikel 2 Besluit ex artikel 3, eerste lid, onderdeel a, van de Wet op het RIVM. Ook de gegevensverwerking die noodzakelijk is voor de uitvoering van het rijksvaccinatieprogramma, alsmede voor de monitoring en evaluatie van het programma is onderdeel van de taak van het RIVM.
Artikel 6c Wpg beschrijft de algemene taak van het RIVM tot het verrichten van werkzaamheden bij de bestrijding van infectieziekten is opgenomen. Op grond van lid 2 van dit artikel is RIVM bevoegd de persoonsgegevens, waaronder gegevens over gezondheid, te verwerken die noodzakelijk zijn voor de uitvoering van deze taak.

Het RIVM ontvangt gegevens uit de Basisregistratie Personen om personen uit te kunnen nodigen voor deelname aan het vaccinatieprogramma, op basis van de Wet basisregistratie personen en het Autorisatiebesluit d.d. 19 november 2020 met kenmerk 2020-0000660990 (bijlage X). Het betreft zowel gegevens van ingezetenen als gegevens van niet-ingezetenen (geprivilegieerde en NAVO-militairen), waarvan de gegevens zijn opgenomen in het deel Registratie Niet-Ingezetenen (RNI) van het BRP. De noodzakelijkheid van de verwerking van de betreffende gegevens is beoordeeld door de Rijksdienst voor Identiteitsgegevens (RvIG) en beschreven in de toelichting bij het autorisatiebesluit.
De vaccinering van asielzoekers vindt een basis in de Regeling verstrekkingen asielzoekers en andere categorieën vreemdelingen 2005. Het RIVM ontvangt de gegevens van deze personen van het Centraal Orgaan opvang Asielzoekers (COA) teneinde de taken omtrent de vaccinering uit te kunnen voeren.
N.B.: het is op dit moment nog niet duidelijk op basis van welke grondslag de gegevens van verpleeghuisartsen, ARBO-artsen en bedrijfsartsen verwerkt mogen worden.

Voor de uitvoering van het Rijksvaccinatieprogramma is centrale registratie het uitgangspunt, gelet op het grote belang van centrale registratie vanwege de individuele en volksgezondheidsbelangen. Het RIVM draagt zorg voor deze centrale registratie, voor Covid-19 in het CIMS. Centrale registratie is evenwel niet verplicht. Deelnemers aan het rijksvaccinatieprogramma kunnen er voor kiezen hun gegevens niet centraal te laten registreren. In de toekomst zal dit worden vormgegeven door het vragen van toestemming aan de deelnemers, zowel voor deelname aan de vaccinatie als voor registratie van de vaccinatie- en persoonsgegevens in het centrale registratiesysteem. Gelet op de korte termijn van realisatie van het vaccinatieprogramma voor COVID-19 en de veelheid en diversiteit aan betrokken uitvoerders in het vragen van expliciete toestemming voor registratie van gegevens in het centrale registratiesysteem vanaf de start van het vaccinatieprogramma niet mogelijk. Er zal – totdat de expliciete toestemmingsprocedure is ingeregeld – gewerkt worden met een opt-outprocedure. Dat wil zeggen dat deelnemers bij het RIVM aan kunnen geven dat hun gegevens niet verwerkt mogen worden in het centrale vaccinatieregistratiesysteem. RIVM zal de gegevens van een persoon die bezwaar maakt tegen deze gegevensverwerking niet verwerken in het CIMS. Bij de uitnodiging voor het vaccinatieprogramma en via diverse kanalen, zoals de website van het RIVM, zal hierover gecommuniceerd worden.
Dit is mede gerechtvaardigd vanuit het perspectief van de noodzakelijkheid voor de infectieziektebestrijding en pandemie mede gekeken naar de taak van algemeen belang van het RIVM in de infectieziektebestrijding, zoals die volgt uit artikel 6c Wpg en artikel 3 Wet op het

RIVM.
Doel is immers de bevolking van een vaccinatie te kunnen voorzien ter bescherming van de volksgezondheid en ter bestrijding van een pandemie. Tevens is het doel veiligheid van de burger. Daar waar bij andere vaccinaties het doel ligt op preventie van individuele infecties en uitbreken en het onderhouden van groepsbescherming, hebben we hier te maken met een nieuwe aandoening, een nieuw vaccin en de bestrijding van een pandemie.

RIVM verwerkt het BSN-nummer teneinde de gegevens afkomstig uit de BRP betrouwbaar te kunnen koppelen aan de gegevens die zij van de uitvoerders van de vaccinatie ontvangen. Zorgverleners zijn op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg verplicht om het BSN-nummer te gebruiken met als doel te waarborgen dat de in het kader van de verlening van zorg te verwerken persoonsgegevens op die client betrekking hebben (artikel 4 Wabvpz). Om zeker te kunnen stellen dat het RIVM in alle gevallen de doorgegeven vaccinatie plaatst in het dossier van de juiste persoon plaats, moet het RIVM van de toediener de tevens naam en adres gegevens, de geboortedatum en de geslachtsaanduiding ontvangen. Naast BSN zijn deze persoonsgegevens noodzakelijk om fouten (zoals verschrijvingen, onduidelijkheden bij tweelingen) te achterhalen.

5. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

Klik hier om infotekst te verbergen

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):

Naam	Vanaf moment dat de betrokkene voor	365 dagen, als de gebruiker 'onthouden	Deze persoonsgegevens	Functioneel beheerder

het eerst inlogt in het systeem.	inloggegevens' aanklikt 30 dagen.	zijn functioneel: het gegeven zorgt er voor dat je met slechts één handeling inlogt in het verschillende databases.

Onderscheid moet worden gemaakt in een clientregister en het vaccinatieregister Covid-19. Het clientregister bevat de clientrecords zoals aangemaakt op basis van de BRP-en COA - gegevens. Het bijbehorende vaccinatieregister Covid-19 wordt gevuld wanneer de vaccinatiegegevens van zorgverleners worden aangeleverd. Vaccinatiegegevens zijn in principe 20 jaar bewaarplichtig, gebaseerd op wijziging van Burgerlijk Wetboek hoofdstuk 7. De Memorie van Toelichting op de Wpg maakt duidelijk dat vaccinatiegegevens doorgegeven aan het RIVM in het kader van het rijksvaccinatieprogramma, waar Covid-19 vaccinatie ook onder valt, minimaal 15 jaar bewaard worden.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

6. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

Klik hier om infotekst te verbergen

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.

Ten aanzien van de rechtsgronden c (wettelijke plicht) en e (taak van algemeen belang) geldt dat deze moet worden vastgesteld bij of krachtens de wet. De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn. Met betrekking tot rechtsgrond e (de taak van algemeen belang) geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving ook expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak gegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak tevens worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

De Richtlijn gegevensbescherming opsporing en vervolging voor dat een gegevensverwerking door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid alleen rechtmatig is indien die verwerking gebaseerd is op de wet.

Bij **conceptregelgeving** zal de regeling veelal tot gevolg hebben dat de verwerkingsverantwoordelijke de gegevensverwerking kan baseren op de rechtsgrond genoemd onder c (wettelijke verplichting). Dit is het geval indien de gegevensverwerking noodzakelijk is ter uitvoering van de wettelijke verplichting en indien de verwerkingsverantwoordelijke belast is met de uitvoering van de wettelijke plicht. Daarnaast kan regelgeving tot gevolg hebben dat een overheidsorgaan de gegevensverwerking kan baseren op de rechtsgrond genoemd onder e (taak van algemeen belang). De publieke taak wordt (of is reeds) wettelijk vastgelegd waarbij, naast andere onderwerpen, volgens de Aanwijzingen voor de regelgeving ook aandacht moet worden geschonken aan de daarbij noodzakelijke gegevensverwerkingen. In regelgeving kan ook worden voorgeschreven dat toestemming van de betrokkene vereist is om persoonsgegevens te verwerken, en daarmee de andere rechtsgronden uitsluiten.

Bij **overheidsverwerkingen** zal het overheidsorgaan de voorgenomen gegevensverwerkingen moeten baseren op één van de zes rechtsgronden. De rechtsgrond genoemd onder f geldt niet voor gegevensverwerkingen in het kader van de uitoefening van publieke taken. Wel kan deze rechtsgrond gebruikt worden voor gegevensverwerkingen in de bedrijfsvoering, zoals cameratoezicht, bezoekersregistratie en toegangscontrole. In veel situaties zal de rechtsgrond genoemd onder a (toestemming) evenmin kunnen dienen als rechtsgrond voor gegevensverwerkingen door overheidsorganen, omdat de betrokkene in de gegeven situatie niet vrijelijk toestemming kan geven.

Indien de gegevensverwerkingen gebaseerd worden op de rechtsgrond genoemd onder f (het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde), dan stelt de AVG als eis dat de belangen of de

grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder mogen wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of de derde.

De gegevensverwerking door het RIVM in het CIMS is noodzakelijk om aan een wettelijke verplichting te voldoen die op het RIVM rust krachtens de Wpg, te weten het voeren van regie op en de coördinatie van de uitvoering, alsmede de registratie, bewaking en evaluatie van het vaccinatieprogramma (artikel 6b). De wettelijke verplichting van het RIVM volgt tevens uit artikel 3 eerste lid onder c van de Wet op het RIVM en het Besluit ex artikel 3 eerste lid onder a van de Wet op het RIVM, waarin aan het RIVM als taak wordt opgedragen:

- de landelijke aansturing en begeleiding van het Rijksvaccinatieprogramma uit te voeren en de regionale uitvoering te coördineren;
- de inkoop, opslag en distributie van de vaccins te verzorgen;
- en de noodzakelijke gegevensverwerking voor de uitvoering van het RVP alsmede voor de monitoring en evaluatie van het programma uit te voeren.

De grondslag in de AVG is taak van algemeen belang (artikel 6 eerste lid onder e AVG).
De taken die aan het RIVM zijn opgedragen ten aanzien van de bestrijding van infectieziekten (artikel 6c Wpg en artikel 3 Wet op het RIVM) dienen het algemeen belang (artikel 6 eerste lid onder e AVG).

6. Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

Klik hier om infotekst te verbergen

De AVG verbiedt de verwerking van bijzondere persoonsgegevens. Op dit verwerkingsverbod gelden de volgende uitzonderingen:

a. de betrokkene heeft uitdrukkelijke toestemming gegeven;
b. de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van arbeids- en sociaalzekerheidsrecht;
c. de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
d. de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
e. de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
f. de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
g. de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
h. de verwerking noodzakelijk is voor preventieve en arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid, medische diagnosen, het verstrekken van gezondheidzorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en –diensten of sociale stelsel en diensten;
i. de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;
j. de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Verdere uitzonderingen zijn te vinden in nationale regelgeving.

De AVG bepaalt daarnaast dat verwerking van strafrechtelijke gegevens alleen is toegestaan door of onder toezicht van de overheid of als dit bij wet geregeld is (zie voor de definitie van strafrechtelijke gegevens de

toelichting bij punt 2).

De verwerking van nationale identificatienummers is alleen toegestaan ter uitvoering van de wet of voor doeleinden die bij wet zijn bepaald. Overheidsorganen kunnen bij de uitvoering van hun publieke taak gebruik maken van het burgerservicenummer, zonder dat daarvoor nadere regelgeving vereist is.

De Richtlijn schrijft voor dat verwerking van bijzondere persoonsgegevens slechts is toegestaan wanneer de verwerking strikt noodzakelijk is, geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van betrokkene, en:

a. wettelijk is toegestaan;
b. noodzakelijk is om vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen; of
c. die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.

Bij **conceptregelgeving** kan van het verbod op de verwerking van bijzondere of strafrechtelijke persoonsgegevens worden afgeweken, mits passende waarborgen worden geboden ter bescherming van persoonsgegevens en andere grondrechten van de betrokkene.

Er worden gegevens betreffende de gezondheid verwerkt en er worden gegevens verwerkt over het land van herkomst, waaruit ras of etnische afkomst kan blijken, zodat er sprake is van verwerking van bijzondere persoonsgegevens.
De verwerking van bijzondere persoonsgegevens in het CIMS is noodzakelijk om redenen van algemeen belang op het gebied van volksgezondheid (artikel 9 lid 2 onder i AVG), te weten het voorzien van de bevolking van een vaccinatie ter bescherming van de volksgezondheid en ter bestrijding van een pandemie. De noodzakelijkheid van gegevensverwerking voor deze taak van algemeen belang is zowel in artikel 6c Wpg als in artikel 3 Wet op het RIVM beschreven.

De gegevens worden enkel verwerkt door personen op wie uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht rust, dan wel door personen die krachtens een overeenkomst tot geheimhouding zijn verplicht.
Tevens wordt het BSN van personen verwerkt. Dit BSN wordt verkregen uit de BRP, waarvoor de grondslag is gelegen in de Wet Basisregistratie Persoonsgegevens en het daarop gebaseerde autorisatiebesluit. Het BSN wordt verwerkt teneinde de wettelijke taken van het RIVM uit te kunnen voeren en in het algemeen belang van de volksgezondheid.

6. Doelbinding

Indien de 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.

Klik hier om infotekst te verbergen

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.

De gegevens worden niet voor een ander doel verwerkt dan het doel waarvoor de gegevens verkregen worden, te weten het wettelijk vastgelegde doel: het voeren van regie op en de coördinatie van de uitvoering, alsmede de registratie, bewaking en evaluatie van het vaccinatieprogramma.

Data uit het CIMS kan gebruikt worden voor het doen van wetenschappelijk onderzoek. Het doen

van wetenschappelijk onderzoek wordt niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd (artikel 5 eerste lid onder b AVG), mits de verwerking voldoet aan artikel 89 AVG. Daaruit volgt kort gezegd dat de verwerking ten behoeve van wetenschappelijk onderzoek onderworpen is aan passende waarborgen, die er voor zorgen dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen. Voorts volgt uit artikel 9 tweede lid onder j AVG en artikel 24 UAVG dat het verwerken van bijzondere persoonsgegevens ten behoeve van wetenschappelijk onderzoek is toegestaan mits het onderzoek een algemeen belang dient, het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost en bij de uitvoering van het onderzoek is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.
Uitgangspunt bij het gebruik van gegevens uit CIMS voor wetenschappelijk onderzoek is het gebruik van anonieme gegevens. Voor dergelijk gebruik is geen toestemming van de betrokkene nodig. Indien er gebruik wordt gemaakt van herleidbare gegevens wordt toestemming gevraagd aan de deelnemer, tenzij dat onmogelijk is of een onevenredige inspanning kost (conform artikel 24 UAVG en artikel 7:458 BW).
Aanvragen voor gebruik van gegevens uit CIMS voor wetenschappelijk onderzoek worden beoordeeld door een aparte en onafhankelijke commissie, te weten de Commissie [naam invullen]. Deze commissie beoordeeld of en hoe voldaan is aan de hiervoor beschreven waarborgen en de gegevensverwerking past binnen de wettelijke kaders.
N.B.: er bestaat een commissie voor aanvragen data uit Praeventis, vnl. ten behoeve van epidemiologisch onderzoek. Deze commissie zal ook ingezet worden voor aanvragen data uit CIMS. Hierover lopen gesprekken.

7. 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 betrokkene minder nadelige wijze, worden verwezenlijkt?.**

Klik hier om infotekst te verbergen

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:

- kan bij het gebruik van bijzondere of strafrechtelijke persoonsgegevens hetzelfde resultaat behaald worden met gebruikmaking van een combinatie van gewone persoonsgegevens?
- 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.

Voor alle bij genoemde gegevensverwerkingen geldt:

a. De persoonsgegevens zijn van belang om het vaccinatieprogramma voor Covid-19 uit te kunnen voeren, te weten het uitnodigen van personen die in aanmerking komen voor vaccinatie, het verstrekken van de vaccinatie, het registreren van de vaccinatie en het nemen van eventuele noodzakelijke vervolgacties, zoals het oproepen voor een tweede vaccinatie, het registreren van bijwerkingen en het doen van een recall.
   De gegevens die uit het BRP (en van het COA) verkregen worden zijn noodzakelijk voor de uitvoering van het vaccinatieprogramma en zijn ook beperkt tot enkel de noodzakelijke gegevens. Verwezen wordt naar de toelichting bij het autorisatiebesluit voor de onderbouwing van die noodzakelijkheid en de proportionaliteit. Voor het COA-bestand geldt dat gekeken moet worden naar beperking van de aangeleverde gegevens. Vooralsnog voorziet een aparte procedure hoe om te gaan met de COA-gegevens na verwerking in de verplichting om deze gegevens ook daadwerkelijk te verwijderen.
   Er bestaat geen andere manier dan de aansluiting op het BRP om de betreffende persoonsgegevens op dergelijke gestructureerde wijze te verkrijgen. Datzelfde geldt voor gegevens van het COA, PROBAS en het PIVA-register.
   De gegevens die door uitvoerders over de vaccinatie van de betrokkene verstrekt worden zijn beperkt tot de gegevens die noodzakelijk zijn voor de genoemde doeleinden. De gegevens die betrekking hebben op de indeling in risicogroepen zijn enkel beperkt tot het feit dat een persoon in een risicogroep valt en in welke risicogroep (medische indicatie, beroep) en bevatten geen informatie over het waarom een persoon in een betreffende risicogroep valt (bijvoorbeeld astma).
b. De verwerkingsdoeleinden kunnen redelijkerwijs niet op een andere, voor de betrokkene minder 'nadelige' manier worden verwezenlijkt.

Periodiek wordt opnieuw beoordeeld of alle persoonsgegevens nog steeds nodig zijn voor het uitvoeren van de wettelijke taken van het RIVM.

7. Rechten van de betrokkene

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.

Klik hier om infotekst te verbergen

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.

Voor de volgende rechten zijn procedures en werkinstructies voor die gegevens die in het kader van het Rijksvaccinatieprogramma worden verzameld, aanwezig:

1. Inzage
2. Verwijderen/anonimiseren:
3. Bezwaar
4. Afzien deelname/intrekking toestemming

Deze beschikbare procedures voor het rijksvaccinatieprogramma algemeen worden apart beoordeeld voor geschiktheid voor het programma CIMS.
Uitzondering op het verwijderen van gegevens uit CIMS geldt vanwege art. 17, lid 3 onder c AVG: in het kader van het algemeen belang voor de
Wanneer verzoeken om inzage gaan toenemen betekent dit dat opschaling plaats moet vinden. Hierover lopen reeds gesprekken met infopunt van RIVM. Daarnaast wordt een clientportaal ingericht om de verzoeken in te kunnen dienen.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

8. Risico's

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.

Klik hier om infotekst te verbergen

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 ongedaanmaking 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.

1. uitwisseling van gegevens met diverse partijen kunnen in geval van verstoringen aan het systeem of netwerk leiden tot verlies of incorrecte vaccinatieoverzichten.
   a. Impact van verstoring in proces gegevensuitwisseling: verkeerde gegevens kunnen leiden tot verkeerde handelingen bij ontvangende partij. Daarnaast ontbreken van inzicht in juiste vaccinaties.
   b. Kans: groter dan gemiddeld.

2. Opschalen personeel ihkv grootschalige verwerking kan leiden tot onbevoegde toegang.
   a. Impact: vrij groot.
   b. Kans: middel.

3. CIMS-machine berekent op verkeerde manier:
   a. Impact: gemiddeld, mogelijk te laat voor 2e oproep.
   b. Kans: klein

4. Verwerking csv-bestand op basis van script gaat niet op de juiste manier. Mogelijk dat gegevens ergens anders terecht kunnen komen, of verkeerde registratie plaats gaat vinden
   a. Impact: onduidelijk.
   b. Kans: na testen vrij klein.

5. Het testen met niet-productie gegevens zorgt mogelijk voor onbetrouwbare testresultaten voor geautomatiseerd importeren van gegevens. N.B. script wordt opgeleverd door Ordina.
   a. Impact: gemiddeld
   b. Kans: groot

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

9. Maatregelen

Beoordeel welke technische, organisator ische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Klik hier om infotekst te verbergen

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.

Big Data

Bij Big data-analyses (zie punt 8) waarbij persoonsgegevens worden verwerkt, dient, gelet op de daarmee gepaard gaande risico's, in het bijzonder aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg ervoor dat naarmate de mogelijkheden van patroonherkenning bij de toepassing van big data minder zijn, een goede validatie door experts op het desbetreffende vakgebied plaatsvindt om het risico van foutieve uitkomsten zoveel mogelijk te reduceren.
- Zorg ervoor dat de data zoveel als met een redelijke inspanning mogelijk is, up to date zijn, de te gebruiken datasets een zo gering mogelijke bias (afwijking) bevatten en dat de te gebruiken algoritmen en analysemethoden deugdelijk zijn.
- Bepaal, rekening houdend met de potentiële impact van de toepassing, de foutmarge die bij de toepassing mag optreden.
- Zorg ervoor dat nuttige informatie aan betrokkenen wordt verschaft over de gebruikte logica achter de analyse en dat voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegevens in gebruikte algoritmen en analysemethoden.

Bij de toepassing van de uitkomsten van big data-analyses dient aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg voor menselijke tussenkomst in het proces van geautomatiseerde besluitvorming.
- Naarmate de potentiële negatieve impact voor de betrokkene groter wordt, neemt de noodzaak voor een goede validatie en een weging van de uitkomsten navenant toe.

Hier kunt u aanvullende punten toevoegen: selecteer de tab *Invoegen*, kies *Snelonderdelen, Aanvullend punt*

Voeg hier wanneer gewenst een afsluitende alinea toe. Denk bijvoorbeeld aan:
- Lessen uit deze PIA
- Volgende stappen etc.


Maatregelen
nemen
Privacybewustwording
PIA
Doelbinding
Noodzaak
Effecten in kaart
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond
Met open vizier