|  |
| --- |
| **Beschrijving van noodzakelijke kenmerken en risico’s bij het (a) starten van een nieuwe verwerking /verzameling van persoonsgegevens of (b) het actualiseren of registreren van een bestaande verwerking/verzameling.** |
| Uiteraard dient elke verwerking en/of voorgenomen verwerking van persoonsgegevens volledig te voldoen aan het gestelde in de WBP en straks de AVG. Wanneer onderstaande stappen gevolgd worden bij het beschrijven/beoordelen van een verwerking EN de uitkomsten van deze stappen worden vastgelegd, dan is dat niet alleen een verantwoorde start om te voldoen aan de WBP, maar naderen we hiermee ook al de eisen die de Europese Privacy-verordening gaat stellen, namelijk het register van verwerkingen en de risico-inventarisatie met maatregelen. Deze beschrijving/risico-inventarisatie (PIA) dient op grond van de Verordening ten minste het volgende te bevatten:* een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
* een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
* een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
* de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan de Wet/Verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

Uiteraard hoeft niet alles in een keer en kan met onderstaande handreiking in meerdere stappen tot het gewenste resultaat gekomen worden: (stap 1) beschrijven verwerkingen, (stap 2) benoemen risico’s per verwerking en (stap 3) beschrijven maatregelen. |
| **Nr.** | **Onderdeel/item** | **Toelichting** | **STAP 1:****Beschrijving van de verwerking** | **STAP 2:****Risico, kans, impact** | **STAP 3:****Maatregelen** |
|  |  |  | *Beschrijf de gevraagde kenmerken van de voorliggende verwerking. Geef de verwerking waar nodig ook een voor de hand liggende naam (vaak applicatienaam)* | *Wat is onvolledig, wat kan misgaan, wat kan rechtmatigheid, beschikbaarheid, continuïteit, kwaliteit, juistheid, volledigheid van de verwerking beïnvloeden en wat zijn andere risico’s voor de persoonlijke levenssfeer van betrokken.* | *Wat kun je doen om de risico’s te beperken (stoppen met verwerking, verzekeren of uitbesteden zijn ook opties!)* |
|  | **Formuleer het doel van de verwerking: waarom wil je dit gaan verzamelen, verwerken en wat wil je ermee bereiken.** | *niet alleen relevant om vooraf eens goed na te denken en te beoordelen wat je wilt bereiken, maar ook om te toetsen of een eventuele uitbreiding van bestaande functionaliteit nog onder het oorspronkelijke doel valt. Daarnaast is het doel van de verwerking ook de toets verderop voor proportionaliteit/subsidiariteit, passende beveiliging etc.* | Het Elektronisch Cliënten Dossier (ECD) is een samenstel van een aantal verschillende technische systemen (applicaties/software). Het doel van het ECD (ofwel het samenstel van de systemen als verwerking van persoonsgegevens) is het beoordelen, plannen, leveren, evalueren en declareren van zorg en ondersteuning, de communicatie met cliënten en de kring van betrokken familie en/of contactpersonen. Naast deze zorggerichte doelen is ook het voldoen aan wettelijke verplichtingen (dossiervoering, JW, WMO, WLZ, JW) reden om deze verwerking te voeren. | *Risico kan zijn dat beschikbare gegevens voor andere doelen worden gebruikt, anders dan de samenhangende doelen die hieronder al zijn benoemd.* | *(Project)verantwoordelijke dient (samen met leverancier en evt CCvR-vertegenwoordiging) hiervoor te waken en alert te zijn op schuivende doelen* |
| 2. | **Wordt de verwerking van persoonsgegevens voor een samenhangend doel verwerkt / zijn er verbanden met andere verwerkingen of is er sprake van uitbreiding of hergebruik van een bestaande verwerking voor iets anders?** | *doelbinding is dat persoonsgegevens niet verder worden verwerkt dan voor het doel waarvoor zij zijn verkregen. Een verdere of uitgebreide verwerking is alleen toegestaan indien deze verenigbaar is met het oorspronkelijk doel waarvoor de persoonsgegevens zijn verkregen. Slechts in uitzonderingsgevallen kan van het principe van een verenigbare verdere verwerking van persoonsgegevens worden afgeweken. Deze uitzonderingsgronden zijn opgenomen in artikel 43 WBP en op deze gronden mag je de “bestaande gegevens/verwerkingen” hergebruiken buiten het oorspronkelijke doel. Fraudebestrijding en/of afhandeling van stafbare feiten valt onder deze uitzondering.* | Naast bovengenoemde doelen wordt deze verwerking gebruikt voor (wetenschappelijk) onderzoek, interne kwaliteitsbeoordeling, opleiding/training. Dit zijn verwerkingsdoelen die direct ondersteunend zijn aan en derhalve passend bij de primaire doelstellingen. | *Risico kan zijn dat er meer gegevens worden verwerkt en/of dat nieuwe/andere combinaties van verzamelde data worden gebruikt.**(function-creep en data-creep)* | *(Project)verantwoordelijke dient (samen met leverancier en evt CCvR-vertegenwoordiging) hiervoor te waken en alert te zijn op schuivende doelen* |
| 3. | **Toets de grondslag: is er een wettelijke basis die je het recht geeft om persoonsgegevens te verwerken/verzamelen?** | *verwerken mag alleen op één van de grondslagen die de WBP geeft in artikel 8. Een van deze bepalingen geeft je het recht om deze gegevens te verwerken. Meest toegepast zijn b (bijvoorbeeld bij zorgovereenkomst, arbeidsovereenkomst, gebruiksovereenkomst etc.), c (vrijwel alles wat met declareren, fiscale verantwoording, milieu, ruimtelijke ordening, volksgezondheid etc. heeft te maken) en f (elk zwaarwegend belang van de organisatie of een derde, afgewogen tegenover het belang van degene van wie gegevens worden verwerkt). Toestemming als grondslag moet je proberen te vermijden en alleen maar gebruiken als het echt niet onder een van de andere te passen is, toestemming kan immers altijd ingetrokken worden en dan heb je een uitdaging.* 1. *de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend,*
2. *de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst,*
3. *de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is,*
4. *de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene,*
5. *de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt of,*
6. *de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.*
 | 1. Wettelijke verplichting: registratie en verantwoordingsplichten uit JW, WMO, WLZ, WGBO, ZVW etc.
2. Nakomen overeenkomst: invulling van de afspraken uit de zorg/behandeling/dienstverleningsovereenkomst met cliënt.
3. Kwaliteitsbelangen van verantwoordelijke en de doelstellingen voor interne evaluatie en ontwikkeling van organisatie en dienstverlening.
4. In alle andere gevallen toestemming vragen (let op: onder AVG en Wet Clientenrechten Elektronische uitwisseling ander toestemmings-regime!!)
 | *Grondslagen verder geen risico: wettelijk getoetst en passend.* | *Geen actie, wel bewaken/evalueren.* |
| 4.  | **Welke persoonsgegevens worden er verwerkt/zijn er voornemens verwerkt te worden? Let hierbij ook op of er bijzondere persoonsgegevens verwerkt worden of gaan worden?** | *aan de hand van het doel van de verwerking wordt de toets op subsidiariteit (je kunt dit doel niet op een andere manier bereiken, die minder ingrijpend is voor de betrokkenen) en proportionaliteit (de inbreuk op de persoonlijke levenssfeer van de betrokkenen is niet onevenredig in verhouding tot het doel van de verwerking, hoeveel gegevens heb je nodig om het doel te halen?). Voor deze afweging moeten alle relevante factoren worden meegenomen: niet alleen hoeveelheid gegevens, maar ook wijze van verkrijging, verwerking, kans of fouten en datakwaliteit, risico’s voor misbruik en mogelijkheden voor controle etc.* *Om een indicatie te krijgen welke gegevens passend zijn voor een welbepaald doel, kan gekeken worden naar het Vrijstellingsbesluit WBP.**Voor de verwerking van bovengenoemde bijzondere persoonsgegevens geldt een streng regime. Het uitgangspunt is dat het niet is toegestaan deze bijzondere gegevens te verwerken, tenzij dit door de Wbp wordt toegestaan. Zie hiervoor de artikelen 16 t/m 24 Wbp.* | 1. Persoonlijke gegevens (NAW en bereikbaarheidsgegevens van cliënten en familie),
2. Persoonlijke gegevens medewerkers (beperkt),
3. Financiële gegevens cliënt/ vertegenwoordiger/gezin,
4. Gezondheidsgegevens (indicatie, zorgvraag, onderzoeken en onderzoeksresultaten, diagnoses en behandelplannen, evaluaties en rapportages),
5. Gegevens inzake seksuele geaardheid voor zover relevant,
6. Strafrechtelijke gegevens voor zover relevant.
 | *Teveel of te gedetailleerde gegevens verzameld en verwerkt.*  | *Toets regelmatig of analyse en bevindingen passen bij de verzamelde data: kan zelfde kwaliteit bereikt worden met minder of andere data(sets)?**Periodiek uitkomsten evalueren (projectverantwoordelijke, leverancier, CCvR, privacy-officer?)* |
| 5.  | **Met wie worden deze persoonsgegevens uitgewisseld?** | *veel van de gegevens die een organisatie verwerkt moeten ergens in de keten gedeeld worden, bijvoorbeeld voor inhoudelijke overdracht of declaratie en verantwoording. De uitwisseling met deze partijen heeft niet alleen een technische component die beschreven/beoordeeld moet worden (welk middel, welk formaat, welke beveiliging, welke encryptie etc.) maar zeker zo belangrijk een “proportionaliteit” component (heb je alles wel nodig wat je vraagt of waartoe je bevoegdheid hebt om te vragen, bijvoorbeeld gemeentes onder WMO of Jeugdwet). Op zijn minst moeten partijen in kaart zijn met wie uitgewisseld wordt/gaat worden. Ook vast vooruit denken op de aankomende “wet cliëntenrechten bij elektronische verwerking van gegevens” waarbij een ander toestemmingsregime gaat heersen.* | 1. Uitwisseling met administratieve verantwoordelijken zoals Gemeente, Zorgkantoor, CAK, CIZ,
2. Uitwisseling met zorginhoudelijk betrokken verantwoordelijken en/of bewerkers (onderaannemers zorg, 1e-lijners, ziekenhuizen, collega-instellingen),
3. Technische uitwisseling met hosters/saas in de rol van bewerker.
 | *Uitwisseling met andere verantwoordelijke is een verwerking die op zich ok moet voldoen aan WBP/AVG.* *Teveel (omvang en detaillering) gevraagd of geleverd,* *onduidelijke rol, bevoegdheden, grondslagen andere partij,* *afhankelijkheid van andere partij (b.v. bij financiering),* *uitwisseling bij calamiteiten en ad-hoc situaties (afweging).* |  |
| 6. | **Op welke wijze zijn de persoonsgegevens beveiligd en waar is dat terug te vinden?**  | *de verantwoordelijke moet zorgen voor passende technische en organisatorische beveiligingsmaatregelen om hiermee de persoonsgegeven te beschermen tegen verlies of enige andere vorm van onrechtmatige verwerking. De te nemen beveiligingsmaatregelen dienen in principe op basis van een risicoanalyse (deze) vooraf tot stand te komen. Dit ziet minimaal op autorisaties, rechten, geheimhoudingsplichten en vertrouwelijkheidsafspraken, technische beveiliging (binnen de organisatie en tijdens uitwisseling met derden) bij import/export, maatregelen om juistheid van gegevens te borgen/controleren etc. Deze maatregelen moeten wel helder en controleerbaar zijn. Goede gewoonte is (onderdelen van) de beveiliging periodiek door bijvoorbeeld de accountants mee te laten testen/beoordelen.* | In samenspraak met o.a xx samen vast te stellen (huidig en gewenst). | *Risico is altijd technische kwetsbaarheid. Dit risico is niet 100% af te dekken. Derhalve duidelijke organisatorische afspraken (verantwoordelijkheden) en processen vastleggen* | *Eerste actie: samenkomst collega’s om maatregelen te bespreken (Anette, Marc, Peter, Reinier, Stephan)* |
|  | **Afsluiten, waar nodig, van een bewerkers-overeenkomst.** | *een bewerker is een partij die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. Indien er een bewerker voor de verwerking van persoonsgegevens is ingeschakeld, dienen afspraken hierover te worden vastgelegd in een bewerkersovereenkomst. De afspraken die met een bewerker moeten worden gemaakt zijn beschikbaar in een model-bewerkersovereenkomst.* | Wanneer systemen/verwerking gehost en/of SaaS, dan afsluiten Verwerkingsovereenkomst (Bewerkersovereenkomst) |  |  |
|  | **Wat is de bewaartermijn voor de verwerking van persoonsgegevens?** | *persoonsgegevens mogen niet langer mogen bewaard dan noodzakelijk is voor het doel waarvoor ze worden verwerkt. In een aantal gevallen zijn er duidelijke wettelijke bewaartermijnen. Wanneer die er niet zijn, gaat het om een valide beargumentering waarom een bepaalde bewaartermijn - gelet op het doel van de verwerking - noodzakelijk is en/of onder welke omstandigheden hiervan afgeweken kan worden (bijvoorbeeld bij incidenten en/of lopende rechtszaken).* | Basistermijnen voor belangrijkste componenten uit het ECD:1. Gegevens tbv behandeling: 15 jaar,
2. BOPZ: 5 jaar
3. Financieel: max 2 jaar na einde overeenkomst

Hiervan mag op goede gronden en/of na verzoek van betrokkenen worden afgeweken | *Risico is dat gegevens niet worden verwijderd of juist te vroeg worden verwijderd of dat samenhang verloren gaat* | *Opnemen als aandachtspunt in jaar-evaluatie.* |
| 9. | **Informatieplichten verantwoordelijke/rechten betrokkene?** | *het is goed (en verplicht) om vooraf betrokkenen te informeren over wie, wat, waar, waarom etc. en de mogelijkheden voor inzage, correctie, wijziging en bezwaar helder aan te geven. Per verwerking dus voorbereiden op berichtgeving naar betrokkenen maar ook voorbereiden op het ontvangen van reacties van betrokkenen. Benoem dus per verwerking bijvoorbeeld een inhoudelijk aanspreekpunt (voor aanpassingen, opvragen, inzage, kwaliteit) en een technisch aanspreekpunt. De beschrijving die met dit overzicht van een verwerking wordt gemaakt is de informatie-set die je aan een betrokkenen moet kunnen verschaffen, zeker onder het strengere compliance-regime van de aankomende AVG* | 1. Privacyreglement (formele tekst),
2. Handreiking Cliënten (informele tekst en toelichting),
3. Samenvatting en/of overzicht van deze inventarisatie voor geïnteresseerden?
 | *Met duidelijke communicatie beperkt risico. Risico derhalve op onduidelijke, gefragmenteerde of niet verstrekte informatie.* | *CCvR houdt vinger aan de pols en geeft feedback uit de organisatie.**Houdt informatieverstrekking niet alleen op papier maar breng het ook in MDO’s en/of cliënt/familiegesprekken om begrip te toetsen.* |
| 10. | **Valt de hierboven beschreven verwerking of het voornemen mogelijk onder bijzondere bevoegdheden van de OR ex hoofdstuk IV-A van de WOR?** | *het is niet zozeer een eis vanuit WBP, AVG of anderszins, maar het blijkt dat ook interne afstemming/toestemming bij een aantal verwerkingen noodzakelijk is. Een aantal systemen/verwerkingen/verzamelingen dienen, alvorens tot start wordt overgegaan, vooraf aan de OR te worden aangeboden. In de praktijk zijn hiervoor 2 sporen bruikbaar:*1. *Vooraf alles afstemmen met de OR voor instemming over het proces en de zorgvuldigheidstoetsen in het proces en daarna de toepassing in de lijnorganisatie, zonder actieve rol meer van de OR (is immers al geweest)*
2. *Procesafstemming vooraf met de OR, maar daadwerkelijke verwerkingen in de praktijk per stuk/individueel ter instemming aan de OR voorleggen.*

*Beide sporen zijn formeel bruikbaar en het verschil zit in de praktische toepasbaarheid, workload en mogelijke vertragingen bij toestemming/instemmingsverzoeken. Best practice zal dus meestal zijn om vooraf alle zorgvuldigheidseisen met de OR af te stemmen en te beschrijven in de procedures rondom de voorgenomen verwerking. De daadwerkelijke praktische uitvoering kan dan vanuit de lijn verder ter hand worden genomen.* | Nee, geen rol voor de OR. Wel CCvR betrekken. |  |  |