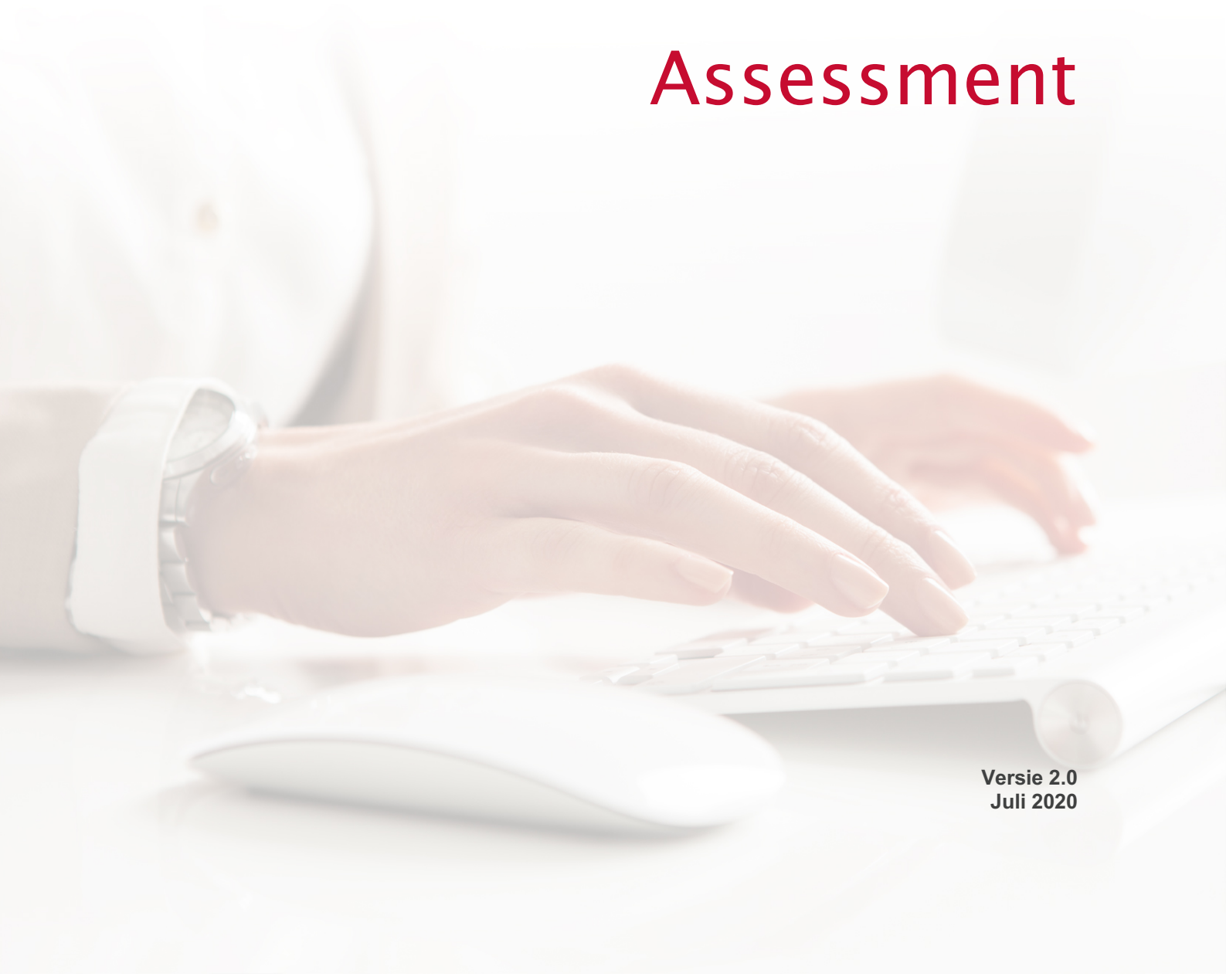
NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA Handreiking Data Protection Impact Assessment



Versie 2.0
Juli 2020

Colofon

Verantwoording

Deze handreiking is uitgegeven door de NOREA, de beroepsorganisatie van IT-auditors in Nederland, en is ontwikkeld om opdrachtgevers en opdrachtnemers van Data Protection Impact Assessments (DPIA, in het Nederlands een Gegevensbeschermingseffectbeoordeling (GEB)) handvatten te bieden om de DPIA uit te voeren in lijn met de Europese Algemene Verordening Gegevensbescherming (AVG). De handreiking kan worden gebruikt voor alle typen organisaties. Het faciliteert het multidisciplinaire team, waarvan de IT-auditor deel kan uitmaken in de rol van adviseur, dat de DPIA uitvoert.

De handreiking is niet bedoeld als instrument om het DPIA-proces te auditen.

Leeswijzer

In het kader van de DPIA heeft de NOREA twee documenten gepubliceerd:

1. De **NOREA Handreiking Data Protection Impact Assessment** (dit document): het bestaat uit een introductie (onder andere wat is een DPIA, wanneer is de DPIA verplicht, wie voert het uit, relatie risicomanagement), een toelichting op de vragen uit het DPIA Raamwerk en enkele bijlagen;
2. Het **NOREA Data Protection Impact Assessment Raamwerk**: het bestaat uit de te beantwoorden vragen, waarmee wordt voldaan aan de vereisten uit de AVG met betrekking tot de DPIA, die na beantwoording ervan leiden tot de DPIA-rapportage

Deelnemers werkgroep

De volgende personen hebben namens de NOREA Kennisgroep Privacy en Werkgroep DPIA aan deze handreiking en het Raamwerk DPIA een bijdrage geleverd:

Han Boer RE CISM, ir. Jan de Heer RE, Henk van der Linde RA, mr. Winfried Nanninga RE CIA MMC, mr drs. Jeroen van Puijenbroek RE CIPP/E CIPM FIP, drs. Ed Ridderbeekx RE CISA CIPP/E,

Coördinatie en redactie

Versie 1.0-1.2: drs. Erik Köning EMITA en Wolter Karssenberg RE CIPP/E CIPM
Versie 2.0: mr. drs. Jeroen van Puijenbroek RE CIPP/E CIPM FIP

Postbus 7984, 1008 AD Amsterdam
telefoon: 020-3010380 | e-mail: norea@norea.nl | www.norea.nl

Versiebeheer		
Versie Datum	Datum	Wijzigingen
1.0	Mei 2013	Publicatie eerste versie
1.1	Juni 2015	Reacties en suggesties verwerkt
1.2	November 2015	Toevoegen meldplicht datalekken
2.0	Juni 2020	Geheel herzien

Inhoudsopgave

A. Introductie

1. Inleiding

Op grond van de Algemene Verordening Gegevensbescherming (AVG) dient elke organisatie die persoonsgegevens verwerkt aantoonbaar te voldoen aan de eisen van de AVG (art 5 lid 2 AVG). De European Data Protection Board (EDPB), de Europese privacy toezichthouders), vaardigt onder andere richtlijnen uit over de uitleg van kernbegrippen van de AVG. Zij heeft aangegeven dat een Data Protection Impact Assessment (DPIA), in het Nederlands aangeduid met Gegevens-beschermingseffectbeoordeling (GEB; hierna wordt alleen de term DPIA gebruikt), "een belangrijk verantwoordingsinstrument is omdat ze de verwerkingsverantwoordelijke niet alleen helpt om aan de eisen van de AVG te voldoen, maar ook om aan te tonen dat passende maatregelen zijn genomen teneinde ervoor te zorgen dat de verordening wordt nageleefd. Met andere woorden: De uitvoering van een DPIA is een proces voor het verwezenlijken en aantonen van naleving."[1].

De NOREA Handreiking DPIA en het NOREA DPIA Raamwerk zijn in lijn met de door de EDPB gestelde criteria voor een aanvaardbare DPIA (zie bijlage 0 voor de criteria). In bijlage 0 zijn de overige documenten opgenomen waarop de Handreiking en het Raamwerk zijn gebaseerd. In bijlage III zijn de begrippen uit de AVG opgenomen; daar waar in dit document 'privacy' staat geschreven wordt 'bescherming van persoonsgegevens' bedoeld.

2. Wat is een DPIA?

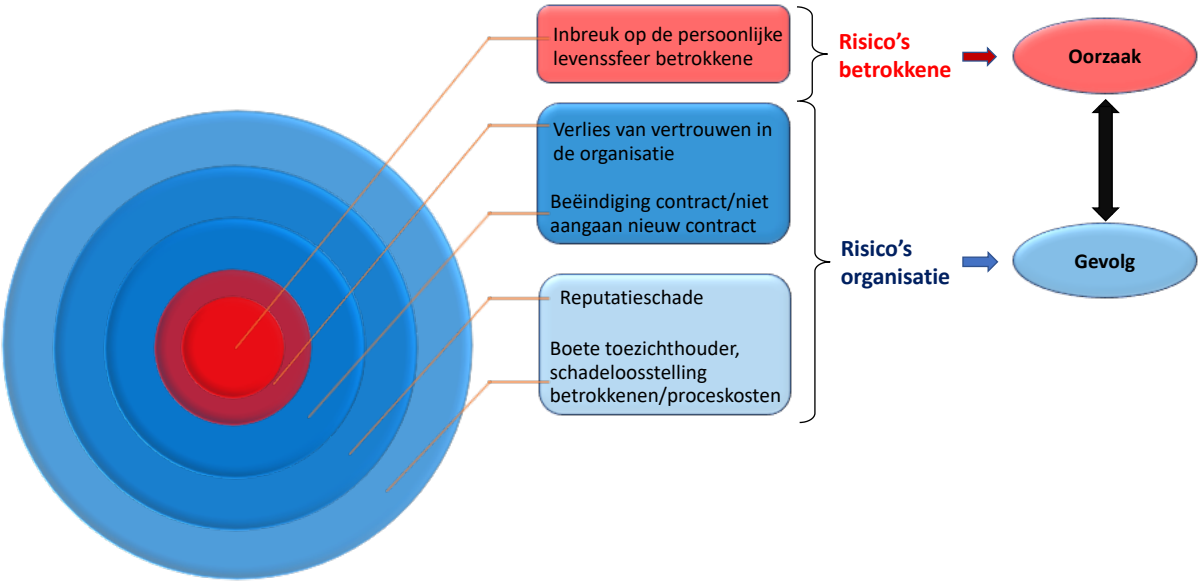
Een DPIA is een instrument om de gegevensverwerking te beschrijven, de rechtmatigheid van de verwerking te beoordelen, de risico's ervan vast te stellen en vervolgens maatregelen te bepalen om de mogelijke negatieve gevolgen te voorkomen of te verlagen tot een aanvaardbaar niveau.

Over welke 'risico's van een gegevensverwerking' hebben we het dan? In artikel 35 AVG staat geschreven "risico's voor de rechten en vrijheden van natuurlijke personen (redactie: de betrokkene/het individu)". In de praktijk wordt de nadruk vaak meer gelegd op de risico's voor de organisatie dan op de risico's voor betrokkenen. De negatieve gevolgen voor de organisatie (reputatieschade, verlies van klantvertrouwen, omzetverlies, marktwaarde verlies, boetes, schadeloosstelling/proceskosten, et cetera) zijn uiteraard ook belangrijk maar zijn het gevolg van de inbreuk op de rechten en vrijheden van de betrokkenen. In figuur 1 is dit grafisch

[1] WP248.rev01 "Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking 'waarschijnlijk hoog risico inhoudt' in de zin van Verordening 2016/79" (okt. 2017).

weergeven. Dit alles kan tot gevolg hebben dat niet de juiste maatregelen worden genomen om de 'echte' risico's te voorkomen of te mitigeren.

Met privacyrisico wordt in dit document bedoeld primair het risico voor de rechten en vrijheden van betrokkene als gevolg van de verwerking van persoonsgegevens en secundair het daaruit voortvloeiende risico voor de organisatie die de persoonsgegevens verwerkt.



figuur 1: Gelaagdheid privacyrisico (bron: "Privacy Impact Assessments in practice – Result of a descriptive field study"[2])

3. Wat is het doel van een DPIA?

Met het uitvoeren van een DPIA kan een organisatie de privacyrisico's van een project, beleid, programma, dienst, product of ander initiatief, in een vroeg stadium op een gestructureerde en transparante wijze in beeld brengen. Door vroegtijdig inzicht te hebben in de belangrijkste risico's en hierop te anticiperen worden kostbare aanpassingen in processen, herontwerp van systemen of het stopzetten van een project voorkomen, en kunnen juridische kosten en/of negatieve publiciteit worden voorkomen of gereduceerd. De resultaten van de DPIA zijn gebaseerd op de beoordeling van de uitkomsten van of juist input voor Privacy by Design & by Default. Inzicht in de negatieve gevolgen van de privacyrisico's kan het management helpen bij een betere onderbouwing van de risicobereidheid ('risk appetite') van de organisatie. Daarnaast helpt de DPIA bij het verhogen van privacybewustzijn binnen de organisatie en het verbeteren van de kwaliteit van gegevensverwerking. Een DPIA helpt ook bij het anticiperen en reageren op maatschappelijke privacybezwaren en kan helpen bij het verkrijgen van maatschappelijk

[2] J. van Puijenbroek en J.H. Hoepman, 'Privacy Impact Assessment in Practice – The Results of a Descriptive Field Study in the Netherlands'

vertrouwen doordat de organisatie privacybescherming zichtbaar in het ontwerp van een project meeneemt. Een bijkomend voordeel van de DPIA is, zoals eerder al aangegeven, dat de organisatie de naleving aan de AVG ermee kan aantonen.

De in de DPIA beschreven maatregelen om de privacyrisico's te verkleinen of te voorkomen, worden door de organisatie gebruikt om een plan van aanpak op te stellen met te nemen acties voordat aangevangen kan worden met de gegevensverwerking. Als de organisatie de gegevensverwerking gaat uitbesteden dan kunnen de beschreven maatregelen worden gebruikt voor het opstellen van de inkoopvereisten waaraan de service leverancier (verwerker) moet voldoen.

4. Wanneer is de DPIA verplicht?

In de AVG is op hoofdlijnen aangegeven wanneer het uitvoeren van DPIA verplicht is. Dat is het geval als een gegevensverwerking waarschijnlijk een 'hoog' privacyrisico oplevert voor de personen van wie de organisatie gegevens verwerkt. De organisatie moet dit zelf bepalen. Deze risicoanalyse wordt niet beschouwd als onderdeel van de DPIA (de aan de gegevensverwerking verbonden risico's voor de rechten en vrijheden van natuurlijke personen inschatten en maatregelen bepalen om deze aan te pakken) maar als een drempeltoets.

De volgende criteria kunnen haar daarbij helpen.

De AVG geeft in artikel 35 lid 3 AVG aan dat er in ieder geval een DPIA moet worden uitgevoerd als een organisatie:

- systematisch en uitgebreid persoonlijke aspecten evalueert gebaseerd op geautomatiseerde verwerking, waaronder profilering, en daarop besluiten baseert die gevolgen hebben voor mensen;
- op grote schaal bijzondere persoonsgegevens of strafrechtelijke gegevens verwerkt;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht)

De Autoriteit Persoonsgegevens (AP) heeft daarnaast op haar website een lijst van soorten verwerkingen opgesteld waarvoor het uitvoeren van een DPIA verplicht is (zie Bijlage IV). De lijst is niet uitputtend.

Het kan zijn dat een verwerking niet op deze lijst staat. In dat geval moet de organisatie zelf beoordelen of de verwerking een 'hoog' privacyrisico oplevert voor de betrokkenen. Om deze beoordeling te maken heeft de de EDPB een lijst met negen criteria opgesteld (zie Bijlage 0). Als vuistregel geldt dat een DPIA moet worden uitgevoerd als de verwerking aan twee of meer van deze criteria voldoet.

De vraag of voor een bepaalde gegevensverwerking het wel/niet verplicht is om een DPIA uit te voeren op grond van de AVG (verwerking houdt een 'hoog' risico in voor de betrokkene), is vanuit het perspectief van privacyrisicomanagement (zie hoofdstuk 7), minder relevant. Privacyrisicomanagement beoogt bedreigingen op het gebied van het verwerken van persoonsgegevens te beheersen en kansen te benutten en zo de prestatie van de organisatie te verbeteren. In dat kader zou een organisatie (bijna) altijd de privacyrisico's van een product/proces/systeem moeten willen beoordelen.

Als ervoor wordt gekozen om geen DPIA uit te voeren, dan moet dit onderbouwd worden vastgelegd als onderdeel van de verantwoordingsplicht. De vastgestelde privacyrisico-classificatie van de verwerking en de toelichting daarop zouden in het Register van verwerkingsactiviteiten kunnen worden opgenomen.

Door wie en hoe wordt bepaald of een DPIA moet worden uitgevoerd, waar dit besluit wordt vastgelegd en of de Functionaris voor de gegevensbescherming (FG) – indien aanwezig – hierover moet worden geraadpleegd, zou de organisatie in haar privacybeleid of een separaat DPIA-beleid kunnen opnemen (zie ook hoofdstuk 8).

5. Wanneer wordt een DPIA uitgevoerd?

5.1. Nieuwe verwerkingen

Volgens de AVG moet een DPIA worden uitgevoerd vóórdat de organisatie met de gegevensverwerking aanvangt. Vanuit risicomanagement oogpunt is dit ook logisch; "Beter voorkomen dan genezen". De AP adviseert "start met de DPIA zo vroeg als praktisch gezien mogelijk is in de ontwerpfase van de gegevensverwerking". Dit zou betekenen dat een organisatie al met de DPIA start bij de beginfase van het product-/dienstontwikkelingsproces (project). Het raadzaam dat de organisatie tijdens de ontwikkeling meerdere keren een privacyrisicoanalyse uit te voeren. Bijvoorbeeld:

- *Scoping:* in deze fase wordt bijvoorbeeld ingegaan op de belangrijkste privacyrisico's en meer strategische vragen zoals "Willen we dit soort gegevensverwerkingen als organisatie wel?" en "Lopen we met deze verwerking een maatschappelijk privacyrisico?" Op basis hiervan zou een schifting kunnen worden gemaakt tussen welke nieuwe productvoorstellen wel/niet verder worden uitgewerkt.

- *Business case*: een van de op te leveren 'deliverables' van de businesscase-fase zou de DPIA moeten zijn.

- *Ontwikkeling:* de resultaten uit de DPIA worden meegenomen tijdens de ontwikkeling van de gegevensverwerking, mede om te voldoen aan de wettelijke vereisten principes van Privacy by Design en Privacy by Default.

- *Testen en valideren*: om vast te stellen dat de uiteindelijk gekozen oplossingsrichtingen tijdens de bouw van de gegevensverwerking de onderkende privacyrisico's hebben weggenomen, dan wel gemitigeerd, wordt geadviseerd om een DPIA opnieuw te laten uitvoeren/te evalueren

Het gedurende meerdere projectfasen uitvoeren van een DPIA zou een vast onderdeel moeten zijn van het product-/projectontwikkelingsproces. Geadviseerd wordt dat de organisatie dit opneemt in het DPIA-beleid.

5.2. Bestaande gegevensverwerkingen

Op grond van de AVG moet ook voor de bestaande gegevensverwerkingen, voor zover dat nog niet heeft plaatsgevonden, een DPIA worden uitgevoerd. De organisatie zal de meest risicovolle gegevensverwerkingen als eerste willen analyseren; een DPIA op uitvoeren. Om dit te inventariseren kan de organisatie voor de bestaande gegevensverwerkingen het ingeschatte privacyrisico van de verwerking (hoog/midden/laag) vastleggen. De meest logische plek hiervoor is het Register van verwerkingsactiviteiten.

Voor bestaande gegevensverwerkingen wordt geadviseerd, in het verlengde van het advies bij product-/projectontwikkeling, dat de organisatie de DPIA een vast onderdeel laat zijn van het changemanagementproces.

5.3. Evaluatie DPIA

Het uitvoeren van een DPIA is een continu proces, geen eenmalige activiteit. De organisatie dient de DPIA periodiek te actualiseren, of eerder als er belangrijke wijzigen zijn opgetreden. De AP noemt als voorbeeld een periodiciteit van 1 keer per 3 jaar.

6. Wie voert de DPIA uit?

De DPIA wordt bij voorkeur uitgevoerd door een multidisciplinair team van medewerkers omdat privacy een multidisciplinaire insteek behoeft. De resultaten van de DPIA worden bij een team beter dan wanneer de DPIA door één persoon wordt uitgevoerd doordat de verschillende deelnemers ieder vanuit hun eigen invalshoek het project kunnen bekijken. Hierbij kan worden gedacht aan de opdrachtgever en de opdrachtnemer van het project, de inhoudelijk deskundigen (project, privacy, techniek, informatiebeveiliging, juridisch, organisatorisch, risicomanagement, data analytics) alsmede uitvoerders. De IT-auditor kan afhankelijk van zijn kennis en ervaring als adviseur een of meerdere rollen vervullen. In bijlage VI is een overzicht opgenomen van de rollen/deelnemers die betrokken kunnen worden bij een DPIA. Afhankelijk van de gegevensverwerking kan het verstandig zijn om verwerkers of ketenpartners bij de DPIA te betrekken.

Het is vanuit de AVG wenselijk dat de betrokkenen of hun vertegenwoordigers, als onderdeel van het DPIA-proces, naar hun mening wordt gevraagd over de voorgenomen verwerking. Zij komen mogelijk met andere privacyrisico's en/of beoordelen de impact ervan anders. Geadviseerd wordt dat de organisatie haar standpunt over het wel/niet consulteren van betrokkenen of hun vertegenwoordigers onderbouwd opneemt in het DPIA-beleid.

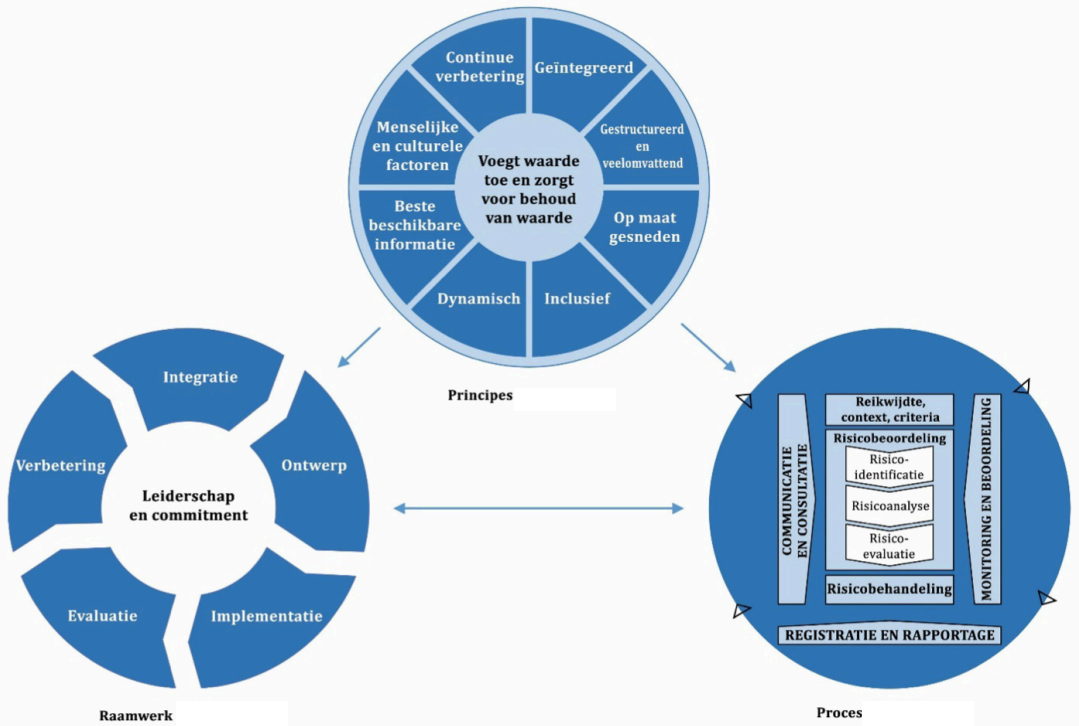
Als de organisatie een FG heeft aangesteld, dan wordt als onderdeel van het DPIA-proces ook het advies van de FG ingewonnen. Dit geeft extra zekerheid dat de DPIA voldoende inzicht biedt in de risico's en er voldoende maatregelen worden getroffen om deze af te dekken.

Komt uit de DPIA naar voren dat de te verwerken persoonsgegevens een hoog risico oplevert èn kunnen er geen (of onvoldoende) maatregelen worden getroffen om dit risico te beperken, dan dient de organisatie de AP hierover voorafgaand te raadplegen.

7. NOREA DPIA Raamwerk en ISO 31000/31010

7.1. (Privacy) Risicomanagement

Elke organisatie, ongeacht type en omvang van die organisatie, wordt geconfronteerd met externe en interne factoren en invloeden die ertoe leiden dat het onzeker is of zij haar doelstellingen zal behalen. Het effect van onzekerheid op het behalen van doelstellingen (oftewel risico) dient te worden gemanaged. Risicomanagement is daarmee een hulpmiddel om bedreigingen (negatieve effecten) te beheersen en kansen (positieve effecten) te benutten en zo de prestaties van een organisatie, project of product te verbeteren. ISO 31000 is de mondiale norm die door veel organisatie wordt gebruikt voor risicomanagement. Dat is de reden waarom de NOREA in deze handreiking gekozen heeft voor deze norm. Binnen ISO31000 is het managen van risico's gebaseerd op drie elementen, te weten: Principes, Raamwerk en Proces. In figuur 2 is dit grafisch weergegeven.



figuur 2: Risicomanagement (bron: NEN-ISO31000:2018 Risicomanagement - Richtlijnen)

Het topmanagement moet ervoor zorgen dat risicomanagement geïntegreerd wordt in alle activiteiten en besluitvormingsprocessen van de organisatie met als gevolg dat het onderdeel wordt van de governance van de organisatie. Daarom is in het Raamwerk voor risico-management een apart onderdeel opgenomen over de integratie (inbedding) van risico-management in de organisatie. Onderdeel van het raamwerk van risicomanagement is de Plan-Do-Check-Act cyclus (in figuur 2: Ontwerp, Implementatie, Evaluatie en Verbetering).

Privacyrisico's zijn een van de vele typen risico's die moeten worden gemanaged. Privacy-risicomanagement dient een integraal onderdeel te zijn van risicomanagement en dus ook te worden geïntegreerd in alle activiteiten en besluitvormingsprocessen van de organisatie.

7.2. DPIA

Onderdeel van privacyrisicomanagement is het uitvoeren van DPIA's. Zoals eerder al aangegeven worden in de DPIA op basis van de beschrijving van de gegevensverwerking de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen beoordeeld en maatregelen beschreven om de risico's te mitigeren. Respectievelijk risicobeoordeling (risk assessment) en risicobehandeling (risk treatment). Deze zijn onderdeel van het Proces van risicomanagement op basis van ISO31000 (zie ook rechtsonder in figuur 2).

Risicobeoordeling (risk assessment)

Risicobeoordeling is het gehele proces van:

- *Risico-identificatie:* risico's vinden, herkennen en beschrijven die een organisatie zouden kunnen helpen of juist verhinderen haar doelstellingen te bereiken
- *Risicoanalyse:* inzicht krijgen in de aard van risico en de kenmerken ervan, waaronder het risiconiveau.
- *Risico-evaluatie:* het vergelijken van de resultaten van de risicoanalyse om te bepalen waar aanvullende actie vereist is. Dit kan leiden tot een besluit om:
    - verder niets te doen;
    - na te denken over opties voor risicobehandeling (risk treatment);
    - verdere analyse uit te voeren om beter inzicht in het risico te hebben;
    - bestaande beheersmaatregelen te handhaven;
    - doelstellingen te herzien.

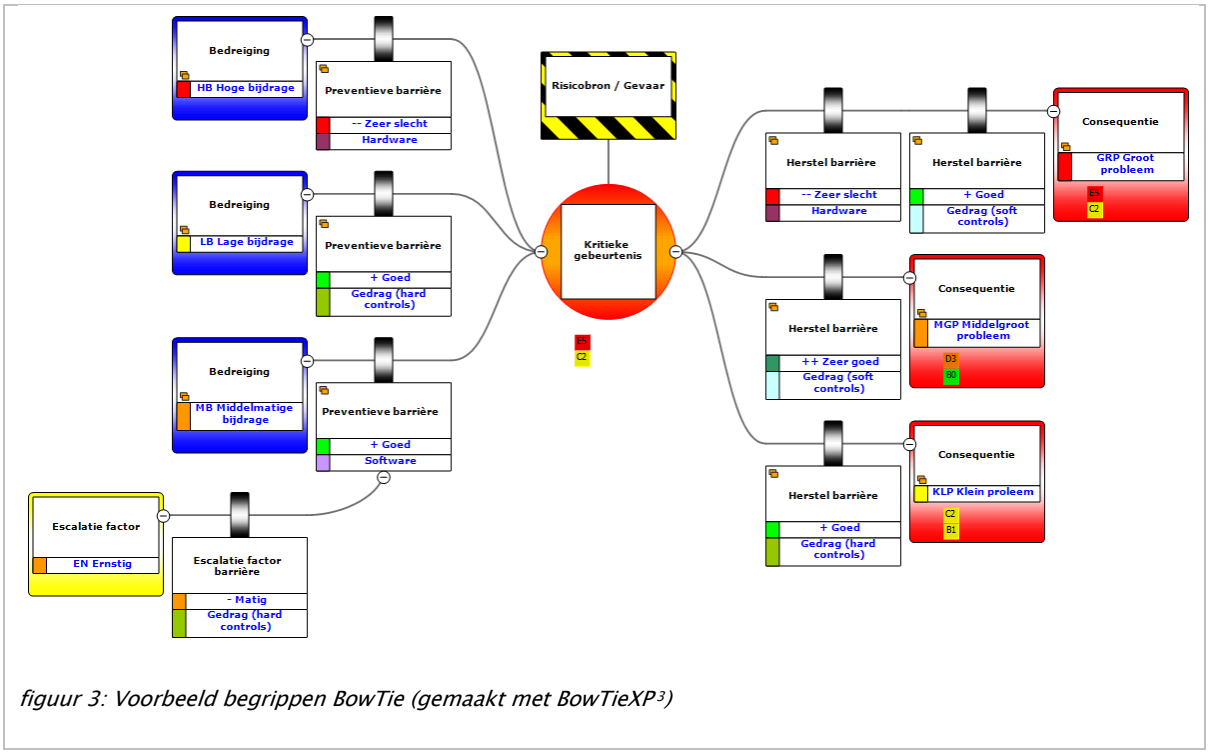
In ISO 31010 zijn verschillende methodieken/technieken beschreven voor het uitvoeren van risicobeoordeling (risk assessment). Het staat het team/degene die de DPIA uitvoert vrij om een bepaalde techniek te kiezen; deze is niet voorgeschreven.

BowTie-methodologie voor risicobeoordeling (risk asssessment)

In het NOREA DPIA Raamwerk is gekozen om de BowTie methodologie (vlinderdasmodel) als voorbeeld uit te werken voor risicobeoordeling. De BowTie techniek is bij uitstek een krachtig instrument om expliciet de negatieve gevolgen van risico's te analyseren en in kaart te brengen. Hierdoor worden niet alleen betere maatregelen getroffen maar wordt door de visualisatie ook een groter draagvlak bij de stakeholders van de DPIA bewerkstelligd. Dit kan tevens bijdrage tot een betere onderbouwing van de risk appetite van de organisatie.

In een BowTie-diagram worden in één figuur, concrete bedreigingen en consequenties alsmede bestaande/mogelijke preventieve- en herstelmaatregelen snel en begrijpelijk in kaart gebracht. Centraal staat de kritieke gebeurtenis/ongewenste gebeurtenis. Links staan de oorzaken of bedreigingen, rechts de gevolgen of consequenties. De BowTie techniek kan zowel op papier als met behulp van software worden uitgevoerd. In figuur 3 zijn de verschillende begrippen van de BowTie techniek weergegeven.

Het model is verder toegelicht in hoofdstuk 0 van eenheid 'B. Toelichting DPIA Raamwerk' (pagina 34).



figuur 3: Voorbeeld begrippen BowTie (gemaakt met BowTieXP[3])

[3] BowTieXP: zie https://www.cgerisk.com/products/bowtiexp/

Risicobehandeling (risk treatment)

Het doel van de risicobehandeling (risk treatment) is het selecteren en implementeren van opties voor het aanpakken van risico's.

Risicobehandeling omvat een iteratief proces van:

- het formuleren en selecteren van opties voor risicobehandeling;
- het plannen en implementeren van risicobehandeling;
- het beoordelen of de behandeling doeltreffend is;
- het beslissen of het resterende risico aanvaardbaar is;
- het overgaan tot verdere behandeling indien dit niet aanvaardbaar is.

7.3. Prospectieve en retrospectieve analyse

Vanuit het perspectief van privacyrisicomanagement zou niet alleen vooruit moeten worden gekeken ter voorkoming van incidenten (prospectieve analyse) maar dient ook te worden teruggekeken en te worden geleerd van incidenten (retrospectieve analyse). De risico-beoordeling van de DPIA is een prospectieve analyse; zonder dat er iets is voorgevallen. De analyse naar aanleiding van een incident, bijvoorbeeld een datalek op een bepaalde gegevensverwerking, is een retrospectieve analyse. De uitkomsten van deze retrospectieve analyse kunnen tot gevolg hebben dat de organisatie besluit om een reeds uitgevoerde DPIA op de betreffende gegevensverwerking te evalueren of, als er nog geen DPIA was uitgevoerd, alsnog een DPIA uit te voeren.

De in het hierboven opgenomen kader vermelde BowTie methodologie kan zowel voor prospectieve als retrospectieve analyses worden gebruikt en is daardoor voor Privacy analyses een krachtig instrument.

8. Inbedding DPIA in de organisatie

Voor veel organisaties geldt dat ze een privacybeleid moeten opstellen op grond van de AVG als onderdeel van de treffen passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat ze de Verordening uitvoeren (art. 24 AVG). De AVG spreekt van ‘wanneer dit in verhouding staat tot de verwerking’, of te wel rekening houdend met de aard, de omvang, de context en het doel van de verwerking. Ten aanzien van privacybeleid wordt al snel beschouwd dat ‘dit in verhouding staat’. De te treffen maatregelen worden geëvalueerd en indien nodig geactualiseerd (PDCA-cyclus)

Het is verstandig dat de organisatie vanuit het algemene privacybeleid specifiek beleid definiërt voor het uitvoeren van een DPIA (al dan niet in een separaat document). Hierin geeft de organisatie onder andere aan in welke gevallen een DPIA wordt uitgevoerd, wanneer de DPIA wordt uitgevoerd, wie de DPIA uitvoert, hoe deze wordt uitgevoerd, wie geconsulteerd moet worden, wie waarvoor verantwoordelijk is en hoe naleving wordt vastgesteld.

Zowel op grond van de AVG als vanuit de risicomanagement (ISO31000) worden de maatregelen geëvalueerd en indien nodig geactualiseerd. De Check van de PDCA-cyclus kan ten aanzien van de DPIA op twee niveaus worden ingestoken, te weten:

- Organisatieniveau: Wordt het DPIA-beleid nageleefd, wordt voldaan aan de randvoorwaarden?
- Verwerkingsniveau: Wat is de kwaliteit van de individueel uitgevoerde DPIAs?

Indien een organisatie een privacymanagement applicatie gebruikt zal het DPIA-proces hier zeer waarschijnlijk ook onderdeel van uitmaken. Op welke manier het DPIA-proces is ingebed in de privacymanagement applicatie is afhankelijk van de organisatie en de mogelijkheden van de applicatie. Dit kan bijvoorbeeld variëren tussen het als bijlage opslaan van de DPIA-rapportage in de applicatie tot het opnemen van alle individuele vragen uit het DPIA Raamwerk in de applicatie en het opslaan van dat de antwoorden in de applicatie.

9. Relatie DPIA en Security Risk Assessment (SRA)

Privacy en informatiebeveiliging zijn niet los van elkaar te zien, maar overlappen elkaar ook niet volledig. Informatiebeveiliging gaat over de bescherming van alle soorten gegevens tegen onbedoelde inzage, wijziging en verlies (Betrouwbaarheid, Integriteit en Beschikbaarheid). Privacy gaat alleen over persoonsgegevens maar omvat daarentegen onder andere ook vereisten ten aanzien van de rechtmatigheid van de verwerking en het nakomen van de rechten van de betrokkenen.

Bekende standaarden voor informatiebeveiliging zijn ISO 27001/27002 (algemeen toepasbaar), NEN 7510/ 7512/7513 voor de zorg en de BIO (Baseline Informatiebeveiliging Overheid) waaraan alle publieke organen moeten voldoen. Onderdeel van deze standaarden is het uitvoeren van een informatiebeveiligingsrisicoanalyse, een zogenaamde Security Risk Assessment (SRA). Deze SRA kan ook worden gebruikt om te voldoen aan artikel 32 AVG waarin staat dat organisaties passende technische en organisatorische maatregelen dient te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen.

De SRA, maakt in principe geen direct onderdeel uit van de DPIA maar wordt apart uitgevoerd. Dit omdat het uitvoeren van een SRA op zich al genoeg tijd kost, informatiebeveiliging anders naar verhouding een te groot deel van de aandacht vraagt binnen de DPIA en informatie-beveiliging niet specifiek is ingericht voor persoonsgegevens maar voor alle gegevens (incl.

persoonsgegevens). Dit betekent dat idealiter een SRA dient te zijn uitgevoerd vóórdat feitelijk met de DPIA wordt gestart. In de DPIA wordt zoveel mogelijk gesteund op de resultaten van de meest recent uitgevoerde SRA. Als dat niet kan dan zal een aanvullende SRA in de DPIA worden uitgevoerd dan wel zal de SRA moeten worden gecompleteerd. In sommige gevallen kan het effectiever zijn om de DPIA vóór de SRA uitvoeren, bijvoorbeeld indien een DPIA wordt uitgevoerd voor een gegevensverwerking die uitbesteed gaat worden of waarvoor een systeem/applicatie wordt aangekocht en de leverancier nog onbekend is. In zo'n geval worden vaak twee DPIA's uitgevoerd. De eerste ten behoeve van de leveranciersselectie en de tweede als aanvulling op de eerste nadat de leverancier is geselecteerd.

B. Toelichting DPIA Raamwerk

In deze eenheid van de handreiking wordt een toelichting gegeven op het NOREA DPIA Raamwerk. De vragen in het raamwerk zijn opgesplitst in drie delen. In deel I wordt de gegevensverwerking beschreven, in deel II wordt de rechtmatigheid van de gegevensverwerking beoordeeld en in deel III worden aan de gegevensverwerking verbonden risico's voor de rechten en vrijheden van natuurlijke personen ingeschat en maatregelen bepaald om ze aan te pakken.

In het document 'NOREA DPIA Raamwerk' zijn de vragen uit deze eenheid opgenomen die na beantwoording ervan leiden tot de DPIA-rapportage.

De vragen in het DPIA Raamwerk zijn gebaseerd op de AVG. Dat wil niet zeggen dat het DPIA Raamwerk niet kan worden gebruikt voor het uitvoeren van een DPIA voor een verwerking van persoonsgegevens waarvoor de AVG niet van toepassing maar waarvoor wel een DPIA moet worden uitgevoerd zoals de Wet Politiegegevens (art. 4c Wpg) of de Wet justitiële en strafvorderlijke gegevens (art 7b Wjsg). Alleen sommige vragen zijn niet van toepassing of moeten anders worden beantwoord (bijvoorbeeld transparantie, grondslag, rechten van betrokkenen). Het team/degene die een DPIA uitvoert voor een gegevensverwerking waarop de Wpg, Wjsg of een andere wet van toepassing is, zal zelf de relevantie van de vragen en de juistheid van de voorgedefinieerde antwoorden in het DPIA Raamwerk moeten vaststellen.

Deel I: Beschrijving gegevensverwerking

Een beschikbare systematische beschrijving van de (beoogde) verwerking en de verwerkings-doeleinden is essentieel bij de behandeling en uitwerking van de DPIA.

1. Contextanalyse

1.1. Beschrijf in hoofdlijnen het project/systeem/applicatie/et cetera waar de DPIA betrekking op heeft. Wat zijn de doelen van en eisen aan het project/systeem/applicatie? Hoe draagt het project/systeem/applicatie bij aan het realiseren van de organisatiedoelen?

Om een DPIA te kunnen uitvoeren is meer informatie nodig dan over de gegevens-verwerking alleen. De verwerking staat niet op zich maar maakt onderdeel uit van een project/proces/systeem dat op haar beurt weer moet bijdragen aan het realiseren van de organisatiedoelen. In deze contextanalyse willen we daar meer zicht op krijgen. Deze informatie kan ook van belang zijn bij het beoordelen van de belangenafweging (in geval van gerechtvaardigd belang als rechtsgrond, zie vraag 2.2) of de beoordeling van het subsidiariteitsbeginsel (zie vraag 6.1). Bij nieuwe projecten kan bijvoorbeeld gebruik worden gemaakt van de informatie uit de projectbeschrijving/business case. Bij bestaande verwerkingen kan bijvoorbeeld worden aangesloten op een systeem-

beschrijving. Gebruikt het project nieuwe technologieën? Wat is de omvang van de gegevensverwerking?

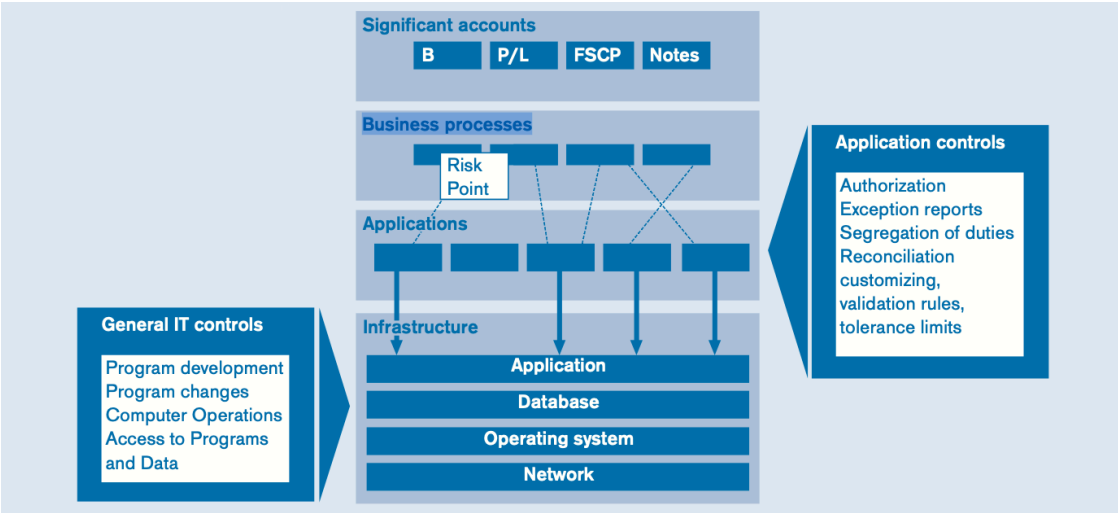
1.2. Beschrijf de relevante bedrijfsprocessen en geef een beschrijving van de gegevensstroom/-stromen met andere bedrijfsprocessen en tussen afdelingen (en eventuele derden).

Geef de stroom van de persoonsgegevens grafisch weer; een visuele walkthrough van het proces. Van wie krijgt de organisatie de persoonsgegevens (rechtstreeks van de betrokkene of anders), waar en hoe ontvangen we deze, welke functionarissen spelen een rol in het proces, wat doen ze met de gegevens, aan wie worden ze verstrekt (binnen en buiten de organisatie) en hoe (op papier en/of elektronisch). Hierbij kan onderscheid worden gemaakt tussen primaire, besturings- en ondersteunende processen.

- Primaire proces: organisatie specifieke processen – geeft typologie weer – gerelateerd aan output van (externe) klanten – geeft bestaansrecht van organisatie
- Besturings proces: activiteiten die benodigd zijn om de organisatie en de processen te kunnen besturen – management control et cetera
- Ondersteunende proces: processen die nodig zijn om het primaire proces te faciliteren –gerelateerd aan mensen, middelen et cetera

1.3. Geef een beschrijving van de “geraakte” (persoonsgegevens bevattende) IT-systemen en/of interfaces naar andere platforms.

Bepaal inzicht in de samenhang van applicaties, databases, operating systems en netwerken. In figuur 4 is ter illustratie hiervan een grafische weergave hiervan opgenomen. Stel vast waar de persoonsgegevens zijn opgenomen voor het project/systeem waar de DPIA betrekking op heeft. Van belang hierbij is het vaststellen van de kernapplicaties voor de onder vraag 1.2 vermelde primaire, besturings- en ondersteunende processen.



figuur 4: Samenhang van de IT-infrastructuur (bron: "SOX IT eerste praktijkervaring en toekomstige ontwikkelingen"[4])

1.4. Benoem, naast de Algemene Verordening (AVG) en de Uitvoeringswet AVG (UAVG), de op de gegevensverwerking van toepassing zijnde wet- en regelgeving.

Hieronder volgen enkele voorbeelden van algemene en sectorale materiewetten die van toepassing zijn in bepaalde sectoren naast de AVG en UAVG (algemene wet). Deze voorbeelden zijn niet uitputtend maar bedoeld als indicatie.

Arbeidssector:

- Burgerlijk wetboek (algemene wet)
- Wet op de Identificatieplicht
- Invorderingswet/Uitvoeringsregeling verplicht gebruik BSN
- Wet op de loonbelasting
- Algemene wet inzake rijksbelastingen
- Diverse sociale zekerheidswetten
- Ziektewet
- Participatiewet
- Wet op de ondernemingsraden
- Arbeidsomstandighedenwet
- Wet allocatie arbeidskrachten door intermediairs (Waadi)

Gemeentelijke sector:

- Burgerlijk wetboek (algemene wet)
- Gemeentewet

[4] M.A. Franken en M.A.P. op het Veld, "SOX IT eerste praktijkervaring en toekomstige ontwikkelingen", Compact 2007/1

- Sociaal domein: Jeugdwet, Wet Maatschappelijke Ondersteuning (Wmo), Participatiewet, Wet schuld/hulpverlening
- Veiligheid, toezicht en handhaving: veelheid aan wetten (samenhang ondermijning, handhaving e.d.)
- Ruimtelijke Orde: Omgevingswet
- Publiekszaken: Wet Basisregistratie Personen

Onderwijssector:

- Burgerlijk wetboek (algemene wet)
- Stelsel van onderwijswetgeving

Zorgsector:

- Burgerlijk wetboek (algemene wet)
- Wet geneeskundige behandelingsovereenkomst (onderdeel uit het Burgerlijk Wetboek deel 7)
- Wet kwaliteit, klachten en geschillen in de zorg
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
- Wet gebruik burgerservicenummer in de zorg

Financiële sector:

- Burgerlijk wetboek (algemene wet)
- Wet financieel transacties (Wft)
- Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)
- Pensioenwet

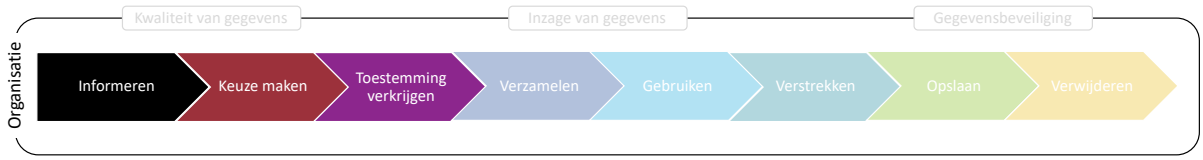
Marketing

- Wet telecommunicatie (onder andere spamverbod, cookies)

2. Informatielevenscyclusfasen: Informeren, Keuze maken en Toestemming verkrijgen

Bij de beschrijving van de verwerking wordt aangesloten bij de informatielevenscyclus uit het NOREA Privacy Control Framework.[5] Dit hoofdstuk gaat in op de fasen van de informatielevenscyclus die betrekking hebben op een rechtmatige, behoorlijke en transparante verzameling van persoonsgegevens. De personen over wie gegevens worden verzameld dienen te worden geïnformeerd over onder andere wie hun gegevens verzamelt, welke gegevens worden verzameld voor welk doel en wat de grondslag is.

[5] NOREA Handreiking Privacy Control Framework v2.0 (aug. 2019).



figuur 5: Informatielevenscyclus (fasen Informeren, Keuze maken en Toestemming verkrijgen)

2.1. Beschrijf de wijze waarop de betrokkenen worden geïnformeerd over de gegevensverwerking.

Voor het individu dient het transparant te zijn dat hen betreffende persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt en in hoeverre de persoonsgegevens worden verwerkt of zullen worden verwerkt. De organisatie dient de betrokken persoon tijdig te informeren over de gegevensverwerking waarbij de informatie eenvoudig toegankelijk en begrijpelijk moet zijn; er moet duidelijke en eenvoudige taal worden gebruikt. Het informeren gebeurt vaak via een privacyverklaring/ privacystatement.

Wat en *wanneer* er moet worden geïnformeerd is afhankelijk van de wijze van verkrijgen van de persoonsgegevens.

- Wanneer de organisatie de persoonsgegevens *bij de persoon zelf* verzamelt dan informeert de organisatie de betrokkene bij/voorafgaand aan de verkrijging.
- Wanneer de organisatie de persoonsgegevens *niet bij de persoon* zelf verzamelt dan informeert de organisatie de betrokkene:
  - binnen een redelijke termijn (max. 1 maand) na verkrijging; of
  - uiterlijk op het moment van het eerste contact met de betrokkene indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene; of
  - uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt indien verstrekking van de gegevens aan een andere ontvanger worden overwogen.

Wat moet er worden geïnformeerd?

- Identiteit en contactgegevens van de verwerkingsverantwoordelijke;
- Contactgegevens van de Functionaris Gegevensbescherming (FG) – iniden aanwezig;
- Doelomschrijving;
- Grondslag van de verwerking;
- Nadere informatie is nodig ingeval van de volgende grondslagen:
  - Gerechtvaardigde belang: de gemaakte belangenafweging;
  - Toestemming: mogelijkheid deze in te trekken;
- Categorieën ontvangers;
- Doorgifte naar “derde land” en welke passende of geschikte waarborgen;

- Bewaartermijnen
- Rechten van betrokkenen;
- Hoe klachten in te dienen bij de AP;
- Of de verstrekking een wettelijke of contractuele verplichting is en wat de gevolgen zijn bij niet verstrekken
- Geautomatiseerde beslissingen en profilering

Aanvullende informatie indien de persoonsgegevens niet bij de betrokkene wordt verzameld.

- Welke persoonsgegevens er worden verwerkt
- Van wie de persoonsgegevens zijn verkregen

2.2. Bepaal per verwerkingsdoel de grondslag van de gegevensverwerkingen geef een toelichting.

De specifieke doeleinden waarvoor de persoonsgegevens worden verzameld moeten expliciet en gerechtvaardigd zijn en te zijn vastgesteld wanneer de persoonsgegevens worden verzameld.

Een gegevensverwerking is alleen rechtmatig als deze op ten minste een van de in artikel 6 lid 1 AVG genoemde voorwaarden (grondslagen) is gebaseerd. Bepaal per verwerkings-doel of geclusterde gelijksoortige verwerkingsdoelen de grondslag. Kan de verwerking niet op een van onderstaande grondslagen worden gebaseerd, dan is de gegevens-verwerking per definitie onrechtmatig en mag deze niet worden uitgevoerd. De grondslagen zijn:

a. **Toestemming;** de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;

b. **Overeenkomst;** 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. **Wettelijke verplichting;** de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

d. **Vitaal belang;** de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;

e. **Taak van algemeen belang;** 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. **Gerechtvaardigd belang;** 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.

In de hierboven genoemde zes voorwaarden (grondslagen) zit geen volgordelijkheid. De voorwaarde 'Toestemming' komt feitelijk als laatste rechtmatigheidsgrondslag. Anders gezegd, als geen van de rechtmatigheidsgrondslagen onder artikel 6 lid 1 punten b. tot en met f. AVG kunnen worden toegepast, dan wordt beoordeeld of de persoonsgegevens op basis van toestemming van de betrokkene kunnen worden verwerkt.

Voor de grondslagen 'c. Wettelijke verplichting' en 'e. Taak van algemeen belang' zijn in de UAVG nadere regels opgenomen. Voor zover van toepassing dient door het team/degene die DPIA uitvoert vastgesteld te worden wat dat betekent voor die specifieke DPIA.

Als de grondslag voor de gegevensverwerking "Gerechtvaardigd belang" is, beschrijf dan de gemaakte afweging tussen het belang van de verwerkingsverantwoordelijke of van een derde en de inbreuk op de persoonlijke levenssfeer van de betrokkene.

2.3. Als de grondslag voor de gegevensverwerking "Toestemming" is, beschrijf dan op welke wijze toestemming wordt verkregen, hoe dit wordt vastgelegd en hoe de toestemming kan worden ingetrokken.

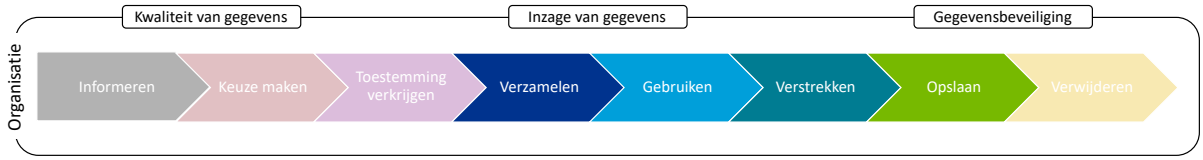
Wanneer de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming (actieve handeling of verklaring) heeft gegeven voor de aanvang van verwerking van zijn persoonsgegevens. Hierbij mag de toestemmingsverklaring geen onderdeel zijn van algemene voorwaarden.

De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet. Alvorens de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld. Het intrekken van de toestemming moet even eenvoudig zijn als het geven ervan.

Toestemming moet vrijelijk gegeven zijn (moeilijk indien er een hiërarchische verhouding bestaat, bijvoorbeeld in de verhouding werkgever-werknemer en overheid-burger)

3. Informatielevenscyclusfasen: Verzamelen, Gebruiken, Verstrekken en Opslaan

In deze fasen van de informatielevenscyclus worden gestructureerde en ongestructureerde gegevens verzameld/gecreëerd en opgeslagen. De verzamelde gegevens moeten toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. De persoonsgegevens moeten juist en actueel zijn en de integriteit en vertrouwelijkheid moeten zijn gewaarborgd. In deze fasen worden persoonsgegevens gebruikt (geraadpleegd, gewijzigd, aangevuld, verrijkt, et cetera) en verstrekt binnen en buiten de organisatie. Betrokkene kunnen een beroep doen op hun rechten.



figuur 6: Informatielevenscyclus (fasen Verzamelen, Gebruiken, Verstrekken en Opslaan)

3.1. Beschrijf per categorie van betrokken natuurlijke personen: de categorieën van persoonsgegevens die worden verzameld, of het bijzondere persoonsgegevens en/of gegevens van strafrechtelijke aard zijn, het verwerkingsdoel en de bewaartermijn.

Voor zover de DPIA een bestaande gegevensverwerking betreft, neem zoveel mogelijk gegevens over van de betreffende verwerking uit het Register van verwerkingsactiviteiten. Indien nodig, pas de bestaande verwerking in het Register aan nadat de DPIA is goedgekeurd. Betreft de DPIA een geheel nieuwe gegevensverwerking? Vul dan het Register na goedkeuring van de DPIA.

Bijzondere categorieën van persoonsgegevens zijn: verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met oog op identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele geaardheid.

Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is, dient de verwerkingsverantwoordelijke termijnen vast te stellen voor het wissen van gegevens. De opslagperiode van de persoonsgegevens moet tot een strikt minimum worden beperkt. In de AVG zijn geen concrete bewaartermijnen voor persoonsgegevens opgenomen. Wel in andere wet- en regelgeving specifieke bewaartermijnen genoemd waaraan de organisatie zich dient houden.

3.2. Indien er bijzondere persoonsgegevens en/of gegevens van strafrechtelijke aard worden verwerkt, geef dan aan welke uitzondering op het verwerkingsverbod van toepassing is.

Bijzondere persoonsgegevens zijn op grond van de AVG verboden te worden verwerkt tenzij een van de in de AVG vermelde uitzonderingen van toepassing is. De uitzonderingen op het verwerkingsverbod “bijzondere persoonsgegevens” (art. 9 lid 2 AVG) zijn:

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 het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht;

c. de verwerking is noodzakelijk ter bescherming van de vitale belangen;

d. de verwerking wordt verricht door stichtingen en verenigingen in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen;

e. de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt

f. noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechten handelen binnen de rechtsbevoegdheid;

g. noodzakelijk om redenen van zwaarwegend algemeen belang;

h. de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, … dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten ...;

i. noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid

j. noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden

Op grond van art. 10 AVG mogen gegevens met betrekking tot strafrechtelijke veroordelingen of strafbare feiten alleen onder toezicht van de overheid worden verwerkt. In art. 32 UAVG zijn de algemene uitzonderingsgronden inzake gegevens van straf-rechtelijke aard beschreven. Deze komen overeen met de hierboven genoemde uitzonderingsgronden voor bijzondere persoonsgegevens a., c., e., f., g. en j (art. 9 lid 2 AVG). Voor de overige uitzonderingsgronden wordt verwezen naar art. 33 UAVG.

3.3. Indien het burgerservicenummer (BSN) wordt verwerkt, geef dan aan welke grondslag hiervoor van toepassing is.

Artikel 87 van de AVG geeft de lidstaten de mogelijkheid om specifieke wetgeving te maken voor het gebruik van het nationaal identificatienummer. In Nederland is dit onder meer de Wet algemene bepalingen burgerservicenummer, de Wet gebruik burgerservicenummer in de zorg en de Invorderingswet/ Uitvoeringsregeling verplicht gebruik BSN. In Nederland mag het BSN niet worden verwerkt tenzij dit in dit in wet- of regelgeving is opgenomen.

3.4. Indien profilering, (semi-)geautomatiseerde besluitvorming, et cetera plaatsvindt, beschrijf de wijze waarop dit plaats vindt en onderbouw waarom dit noodzakelijk is.

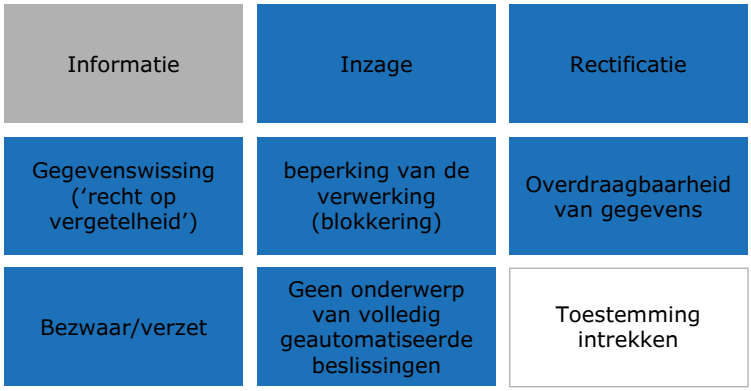
Profilering, (semi) geautomatiseerde besluitvorming, monitoring, et cetera zijn gegevensverwerkingen die naar hun aard een grote inbreuk op de rechten en vrijheden van de betrokkenen kunnen hebben. De AVG definieert profilering als “elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd”. Geautomatiseerde besluitvorming heeft een ander toepassingsgebied en kan profilering gedeeltelijk overlappen of het resultaat zijn van profilering. Uitsluitend geautomatiseerde besluitvorming is het nemen van besluiten met technologische middelen en zonder menselijke tussenkomst. Onderbouwing van de noodzaak is voor de beoordeling van het subsidiariteitsbeginsel (zie vraag 6.1) dan ook belangrijk.

3.5. Beschrijf de maatregelen die waarborgen dat de persoonsgegevens juist zijn op het moment van verzamelen/vastleggen en hoe wordt gerealiseerd dat deze actueel blijven.

Zijn er procedures, instructies, systeembeschrijvingen, et cetera waaruit blijkt dat de persoonsgegevens juist zijn op het moment van verkrijgen (bijvoorbeeld verschillende vormen van inputvalidatie) en hoe ze actueel worden gehouden (bijvoorbeeld periodieke controle).

3.6. Beschrijf de wijze waarop uitvoering wordt gegeven als de betrokkene zijn rechten inroept (recht op inzage; rectificatie; gegevenswissing; beperking van de verwerking; overdraagbaarheid van gegevens; bezwaar; niet onderworpen worden aan geautomatiseerde individuele besluitvorming, waaronder profilering).

In figuur 7 zijn de rechten van de betrokkenen weergegeven. Hoewel de verwerkingsverantwoordelijke verplicht is betrokkene te informeren (zie vraag 2.1) wordt het ook als een recht beschouwd. Evenals de voorwaarde van het intrekken van toestemming (zie vraag 2.3). De overige rechten in figuur 7 (blauw) dient de betrokkene in te roepen.



figuur 7: Rechten betrokkenen

Voor de DPIA is het belangrijk dat voor de in scope zijnde gegevensverwerking aan de in te roepen rechten kan worden voldaan. In hoeverre is hier bij de ontwikkeling van het product/systeem al rekening mee gehouden (Privacy by Design)? Het gaat hier om de specifieke uitvoering van ieder verzoek tot de uitoefening van rechten en niet om een algemene procedure 'Rechten betrokkenen' (separaat of als onderdeel van het privacybeleid). Kan bijvoorbeeld een gedeelte van de persoonsgegevens worden gewist als de betrokkene daarom verzoekt of kan een (deel) van de verwerking worden geblokkeerd voor een individuele betrokkene, et cetera.

3.7. Indien de rechten van de betrokkene worden beperkt, bepaal op welke wettelijke uitzondering (art. 23 AVG) van toepassing is.

Slechts in uitzonderingsgevallen mogen de rechten van de betrokkenen worden beperkt (nationale veiligheid, landsverdediging, openbare veiligheid, de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, et cetera). In art 23 AVG zijn deze beschreven.

3.8. Als de organisatie een goedgekeurde gedragscode (cf. art. 40 AVG) naleeft of een certificaat (cf. art. 42 AVG) heeft die betrekking heeft op de gegevensverwerking, benoem deze en beschrijf hoe borging hiervan plaatsvindt. In geval van certificering benoem ook de externe instelling die het certificaat heeft uitgegeven.

Gedragscode

Een groep verantwoordelijken of verwerkers (bijvoorbeeld een branche of sector) kan een gedragscode opstellen voor de manier waarop deze groep omgaat met persoonsgegevens. In een gedragscode maakt de groep de algemene normen uit de AVG concreter. De AP kan de gedragscode goedkeuren. Organisaties binnen de groep kunnen zich vervolgens aansluiten bij de gedragscode. Daarmee leggen zij vast dat zij zich houden aan de in de gedragscode opgenomen bepalingen voor de bescherming van persoonsgegevens.

Certificaat

Het AVG-certificaat[6] is een nieuw instrument in de AVG. De verwerkingsverantwoordelijke of verwerker kan met dit certificaat aantonen dat zij persoonsgegevens volgens de vereisten van de AVG verwerkt. Een certificatie-instelling beoordeelt op basis van een certificatieschema of een product, proces of dienst van de organisatie in aanmerking komt voor een AVG-certificaat

Beoordeling Gedragscode/Certificaat

Als in de DPIA wordt verwezen naar een goedgekeurde gedragscode of een AVG-certificaat, wordt dan aannemelijk gemaakt dat de gedragscode/certificaat de (voorgenomen) gegevensverwerking volledig afdekt; is de scope hetzelfde? Hoe wordt vastgesteld dat de gedragscode wordt nageleefd? Welke externe certificerende instelling heeft het certificaat uitgegeven? En is deze instelling geaccrediteerd door de Raad van Accreditatie?

3.9. Beschrijf op hoofdlijnen de technische en organisatorische beveiligingsmaatregelen om de integriteit en vertrouwelijkheid van de persoonsgegevens te waarborgen.

Neem de resultaten op van de apart uitgevoerde informatiebeveiligingsrisicoanalyse, een zogenaamde Security Risk Assessment (SRA), met betrekking tot de gegevensverwerking. Beschrijf ook eventuele aanvullende maatregelen, met name voor de opslag en/of het transport van gevoelige persoonsgegevens, en hoe is gewaarborgd dat toegang tot de persoonsgegevens alleen wordt verleend als dit noodzakelijk is voor de uitvoering van de taak ('need to know').

Van belang is aan te geven op welke nationale of internationale standaarden de uitgevoerde SRA is gebaseerd. Bekende internationale standaarden zijn de NEN-ISO 27001/27002, et cetera De nationale standaarden zijn vaak gebaseerd op die internationale standaarden, bijvoorbeeld de NEN 7510, 7512 en 7513 in de zorg en de BIO (Baseline Informatiebeveiliging Overheid) waaraan alle publieke organen moeten voldoen. Als de SRA in haar beoordeling hiervan niet gebruik heeft gemaakt dan dient de toereikendheid van het gehanteerde normenkader aanvullend te worden beoordeeld.

3.10. Beschrijf op hoofdlijnen de getroffen maatregelen om de gevolgen van een datalek voor de betrokken personen wiens gegevens zijn gelekt zoveel mogelijk te beperken en in de toekomst te voorkomen.

[6] Op het moment van publicatie van deze handreiking zijn er nog geen goedkeurde AVG-certificaten. In dit certificeringsproces spelen zowel de Raad van Accreditatie als de Autoriteit Persoonsgegevens een rol.

Uit de risicoanalyse kan blijken dat bepaalde typen incidenten niet 100% kunnen worden voorkomen, of dat dit alleen kan tegen onaanvaardbaar hoge kosten. Dan moet er een goed uitgewerkt plan klaarliggen wat de organisatie gaat doen om de gevolgen van zo'n incident zo veel mogelijk te beperken.

3.11. Beschrijf de ontvangers binnen de organisatie aan wie de persoonsgegevens worden verstrekt.

Op basis van de beschreven procesplaten/diagrammen (zie vraag 1.2) is inzichtelijk aan wie de persoonsgegevens worden verstrekt, binnen de organisatie.

3.12. Beschrijf de ontvangers buiten de organisatie aan wie de persoonsgegevens worden verstrekt, wat hun rol (verwerkingsverantwoordelijke of verwerker) is en waar deze gevestigd zijn.

Op basis van de beschreven procesplaten/diagrammen (zie vraag 1.2) is ook inzichtelijk aan wie de persoonsgegevens worden verstrekt buiten de organisatie. Geef aan of de ontvangende organisatie onderdeel is van het concern waartoe de verstrekkende organisatie behoort.

Voor de ontvangers buiten de organisatie wordt vastgesteld of deze de rol van 'verwerkingsverantwoordelijke (al dan niet in gezamenlijkheid)' of van 'verwerker' vervult omdat de AVG aanvullende eisen stelt als persoonsgegevens worden verstrekt aan een verwerker. Deze aanvullende eisen moeten ervoor zorgen dat het beschermingsniveau voor de betrokkene gelijk blijft ongeacht wie de persoonsgegevens verwerkt. Die verantwoordelijkheid blijft op de organisatie rusten wanneer de verwerking of een deel daarvan wordt uitbesteed aan een verwerker. De uitbestedende organisatie moet:

- De verwerker voorafgaand beoordelen;
- Een verwerkersovereenkomst afsluiten met de verwerker;
- De naleving van verwerkersovereenkomst toetsen.

Als persoonsgegevens worden doorgegeven (verstrekt en/of ter beschikking gesteld) aan landen buiten de Europese Economische Ruimte (EER)[7] ('derde landen') of internationale organisaties dan is een passend beschermingsniveau zoals binnen de Europese Unie (EU) niet gegarandeerd. Daarom gelden voor dergelijke doorgiften speciale regels. Voorafgaande aan de verstrekking buiten de EU/EER toetst de organisatie of aan de wettelijke vereisten is voldaan.

[7] EER: Lidstaten van de Europese Unie (EU) + IJsland, Noorwegen en Liechtenstein. Het Verenigd Koninkrijk heeft op 31 januari 2020 de EU verlaten. Er geldt nu een overgangsperiode, tot en met 31 december 2020. Tijdens die overgangsperiode verandert er niets.

Doorgifte buiten de EU/EER vindt voornamelijk plaats op basis van het adequaatheids-besluit, modelcontracten en uitdrukkelijke toestemming van de betrokkene. Daarnaast kunnen concerns voor doorgiften tussen entiteiten die deels buiten de EU/EER zijn gevestigd gebruik maken van Binding Corporate Rules (BCR).

- *Adequaatheidsbesluit*: De Europese Commissie (EC) heeft een lijst opgesteld met landen die een gegevensbeschermingsniveau bieden die vergelijkbaar is met de AVG. [8] Voor Amerika geldt hierbij specifiek dat de ontvangende Amerikaanse organisatie het Privacy Shield moet hebben ondertekend.

- *Modelcontracten/Standard Contractual Clauses:* Als er geen sprake is van een adequaatheidsbeslissing, dan moet er een andere passende waarborg zijn als een organisatie persoonsgegevens wil doorgeven aan een land buiten de EU. Dat kan met een modelcontractbepaling (ook wel standard contractual clauses of SCC's genoemd) die door de EC is vastgesteld. Deze zijn:

    - Een modelcontract voor doorgifte tussen twee verantwoordelijken waarbij de een gevestigd is binnen de EU en de ander daarbuiten;

    - Een modelcontract voor doorgifte van een verantwoordelijke gevestigd binnen de EU naar een verwerker (degene die in opdracht van de verantwoordelijke persoonsgegevens verwerkt) in een derde land

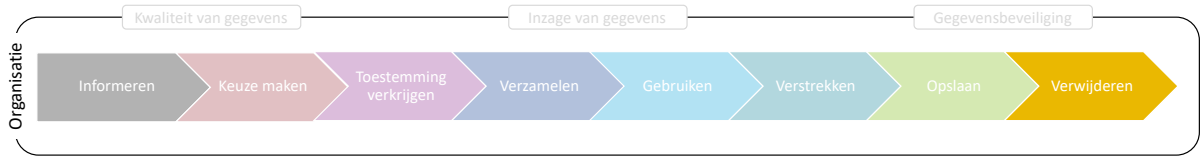
- *Binding Corporate Rules (BCR):* Als een internationale organisatie of multinational (kortweg concern) vestigingen heeft binnen en buiten de Europese Unie (EU) waartussen persoonsgegevens worden doorgegeven dan kan het concern interne gedragscodes opstellen voor gegevensverkeer binnen het eigen concern, de BCR. In de BCR (een 'global privacy policies') legt het concern de waarborgen vast voor de bescherming van persoonsgegevens bij doorgiften naar entiteiten binnen het concern die gevestigd zijn in een land zonder passend beschermingsniveau. Alle werknemers en entiteiten binnen het concern (ook de Nederlandse en Europese vestigingen) moeten zich houden aan de privacy policy.

- *Uitdrukkelijke toestemming van de betrokkene:* De betrokkene dient hierbij te zijn ingelicht over de risico's die dergelijke doorgiften voor hem kunnen inhouden bij afwezigheid van het adequaatheidsbesluit en van passende waarborgen.

[8] De landenlijst is te vinden op de site van de AP (https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu?qa=adequaatheidsbesluit&scrollto=1)

4. Informatielevenscyclusfasen: Verwijderen

In deze fase van de informatielevenscyclus worden persoonsgegevens verwijderd of geanonimiseerd omdat ze niet langer bewaard mogen worden dan noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt.



figuur 8: Informatielevenscyclus (fase Verwijderen)

4.1. Beschrijf de wijze waarop invulling wordt gegeven om na afloop van de beschreven bewaartermijn (zie vraag 3.1) de persoonsgegevens aantoonbaar te verwijderen of te anonimiseren.

Wanneer de door de organisatie vastgestelde bewaartermijn is verlopen (zie vraag 3.1), moeten de persoonsgegevens worden vernietigd dan wel geanonimiseerd. Aan anonimiseren worden strengen eisen gesteld. Het anonimiseren van persoonsgegevens zodat de overgebleven gegevens ook echt onherleidbaar zijn en blijven, wordt steeds lastiger.

Enkele vragen die de organisatie kan stellen bij verwijderen van de persoonsgegevens rekening zijn: Hoe vindt de vernietiging plaats? Gebeurt dit handmatig of (semi)geautomatiseerd? Hoe kan worden aangetoond dat de persoonsgegevens zijn vernietigd? Hoe wordt omgegaan met bestanden waarin persoonsgegevens zitten met verschillende bewaartermijnen? Kan een gedeelte van de gegevens worden verwijderd? Hoe wordt omgegaan met het verwijderen van persoonsgegevens die zijn opgenomen in backup-bestanden. Et cetera.

Deel II: Rechtmatigheidsbeoordeling

Op basis van de beschrijving van de gegevensverwerking (deel I) wordt in dit deel de rechtmatigheid van de gegevensverwerking vastgesteld. De grondslag wordt beoordeeld, de noodzaak en evenredigheid van de gegevensverwerking en of de betrokkenen hun rechten afdoende kunnen uitoefenen.

5. Grondslag

5.1. Beoordeel de grondslag/grondslagen waarop de gegevensverwerking is gebaseerd (zie antwoord op vraag 2.2, 3.2 en 3.3).

Indien de grondslag een 'Wettelijke verplichting' of 'Taak van algemeen belang' is, beoordeel dan tevens of de genoemde wetgeving en de clausules uit die wetgeving voldoende basis zijn voor de rechtmatigheidsgrondslag om het doel te realiseren. Als de grondslag voor de gegevensverwerking "Gerechtvaardigd belang" is, beoordeel dan of de beschreven afweging tussen het belang van de verwerkingsverantwoordelijke of van een derde en de inbreuk op de persoonlijke levenssfeer van de betrokkene.

Als er bijzondere persoonsgegevens of gegevens van strafrechtelijke aard worden verwerkt, beoordeel dan of de aangehaalde uitzonderingsgrond op het verwerkings-verbod terecht als rechtsgrond kan worden gebruikt. Als het BSN wordt verwerkt, beoordeel dan de grondslag.

6. Noodzaak en evenredigheid

6.1. Beoordeel de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden.

Oftewel beoordeel of aan de proportionaliteits- en subsidiariteitsvereisten wordt voldaan. In de Handleiding AVG van het Ministerie van Veiligheid en Justitie[9] staat hierover:

Allereerst moet de verwerking proportioneel zijn. Dit betreft de vraag naar effectiviteit en evenredigheid. Als u met de verwerking van de gegevens niet het gestelde doel kunt bereiken, of dat is zeer onwaarschijnlijk, dan is deze verwerking niet snel proportioneel. Het tweede element van de proportionaliteitstoets betreft de evenredigheid. Het legitieme doel dat wordt nagestreefd moet in verhouding staan tot het feit dat daarvoor persoonsgegevens moeten worden verwerkt.

Subsidiariteit betreft de vraag of het genoemde doel niet op een andere, minder ingrijpende wijze (bijvoorbeeld door géén of minder persoonsgegevens te verwerken) kan worden bereikt. Wanneer u bijvoorbeeld vermoedens heeft dat één specifieke medewerker fraude pleegt, is het niet noodzakelijk om alle werknemers te controleren.

Nog eventuele openstaande vragen voor wat betreft noodzaak en evenredigheid kunnen mogelijk worden beantwoord op basis van de goedgekeurde gedragscode (zie vraag 3.8).

[9] https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming

7. Uitoefening rechten betrokkenen afdoende

7.1. Beoordeel of de betrokkenen hun rechten afdoende kunnen uitoefenen en of zij daarover tijdig en transparant zijn geïnformeerd (zie antwoord op vragen 2.1, 3.7 en 3.7).

Als de betrokkenen hun rechten niet afdoende kunnen uitoefenen is de gegevens-verwerking niet rechtmatig.

Indien op grond van de antwoorden op de vragen 5.1 tot en met 7.1 wordt vastgesteld dat de gegevensverwerking niet rechtmatig is, wordt geadviseerd om er eerst voor te zorgen dat de gegevensverwerking alsnog rechtmatig wordt voordat wordt doorgegaan met de risico-beoordeling en risicoafhandeling (deel III). Als uiteindelijk blijkt dat een bepaalde gegevens-verwerking niet rechtmatig kan worden gemaakt dan zou de eindconclusie van de DPIA moeten zijn dat niet mag worden aangevangen met de betreffende gegevensverwerking of, in geval van een bestaande gegevensverwerking, moet worden gestopt met die gegevensverwerking.

Deel III: Risicobeoordeling en Risicobehandeling

Op basis van de beschrijving van de gegevensverwerking (deel I) worden de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen beoordeeld en maatregelen beschreven om de risico's aan te pakken. Respectievelijk risicobeoordeling (risk assessment) en risicobehandeling (risk treatment).[10]

Hoewel een organisatie de AVG moet naleven, compliant moet zijn, wil dat niet zeggen dat er helemaal geen risico's voor de rechten en vrijheden van de betrokkene mogen zijn. Elke gegevensverwerking houdt immers een risico in voor de betrokkene. Het risico nadat maatregelen zijn getroffen (het zogenaamde restrisico) mag alleen niet te hoog zijn (zie hieronder de vragen 8.2 en 8.3). In deel II van Raamwerk is de rechtmatigheid van de gegevensverwerking al beoordeeld.

In plaats van 'risico's voor de rechten en vrijheden van natuurlijke personen' wordt in de praktijk vaak de term 'privacyrisico' gebezigd. Hierbij ligt de nadruk vaak meer op de risico's voor de organisatie dan op de risico's voor de betrokkenen De negatieve gevolgen voor de organisatie (reputatieschade, verlies van klantvertrouwen, omzetverlies, marktwaarde verlies, boetes, schadeloosstelling/proceskosten, et cetera) zijn uiteraard ook belangrijk (secundair) maar zijn vaak het gevolg van de inbreuk op de rechten vrijheden van de betrokkenen (primair). Daarnaast is de term 'privacyrisico' een containerbegrip geworden waarbij oorzaken, gevolgen en soms zelfs maatregelen als 'risico' worden getypeerd. Dit alles kan tot gevolg hebben dat niet de

[10] Risiciobeoordeling en Risicobehandeling zijn onderdelen uit het Proces Risicomanagement van NEN31000

juiste maatregelen worden genomen om de 'echte' primaire risico's te voorkomen of te mitigeren.

Met privacyrisico wordt in dit document bedoeld primair het risico voor de rechten en vrijheden van betrokkene als gevolg van de verwerking van persoonsgegevens en secundair het daaruit voortvloeiende risico voor de organisatie die de persoonsgegevens verwerkt.

Een gestructureerde risicobeoordeling (risk assessment) waarbij de nadruk ligt op de concrete negatieve gevolgen voor de betrokkenen is essentieel voor de effectiviteit van de DPIA.

8. Risicobeoordeling (Risk assessment)

Voor risicobeoordelingen kunnen allerlei technieken worden gebruikt.[11] **Het staat het team/degene die de DPIA uitvoert vrij om een bepaalde techniek te kiezen.** Los van de gekozen techniek kan worden gesteld dat een risicobeoordeling grofweg bestaat uit drie onderdelen/fasen, te weten risico-identificatie, risicoanalyse en risico-evaluatie.

8.1. Voer de Risico-identificatie uit

Het eerste onderdeel van de risicobeoordeling is de *risico-identificatie*. De risico-identificatie is met name bedoeld om de risico's te vinden, herkennen en beschrijven.

Ter illustratie: Uitwerking risico-identificatie met behulp van BowTie

In het NOREA DPIA Raamwerk is gekozen om de BowTie methodologie (vlinderdasmodel) als voorbeeld uit te werken voor de risicobeoordeling. Met BowTie worden concrete oorzaken, negatieve gevolgen en maatregelen begrijpelijk in kaart gebracht. De BowTie methodologie kan zowel op 'papier' als met behulp van software worden uitgevoerd.

Voordat de uit te voeren stappen voor de risico-identificatie voor de DPIA met behulp van BowTie worden uitgewerkt zijn in eerst de belangrijkste BowTie begrippen toegelicht.

Begrip	***Omschrijving***
Risicobron/Gevaar (Hazard)	*De Risicobron, ook wel het Gevaar genoemd, beschrijft de gewenste staat of activiteit; is onderdeel van normale bedrijfsprocessen. Het woord 'gevaar' suggereert dat het ongewenst is, maar in feite is dit het tegenovergestelde: het is precies wat de organisatie nodig heeft om zaken te doen. Het is het proces dat schade kan veroorzaken, maar zonder het proces worden er geen zaken gedaan.*

[11] In NEN31010 staan verschillende technieken beschreven voor het uitvoeren van een risicobeoordeling (riskassessment). Het is een uitwerking van de het onderdeel Risicobeoordeling het Proces Risicomanagement van NEN31000.

Kritieke gebeurtenis (TopEvent)	*Zolang het proces (Risicobron) wordt beheerst, vindt het zich in de gewenste staat. Bepaalde gebeurtenissen kunnen echter een afwijking op of verlies van controle over het proces (Risicobron) veroorzaken. In de BowTie-methodologie wordt zo'n gebeurtenis Kritieke gebeurtenis (TopEvent) genoemd. De Kritieke gebeurtenis hoeft op zich nog geen grote ramp te zijn maar als het niet op de juiste manier wordt gemitigeerd kan het leiden tot meer negatieve gevolgen (consequenties). Als er meerdere Kritieke gebeurtenis van toepassing zij worden er meerdere BowTie-diagrammen gemaakt; voor elke combinatie Risicobron/Kritieke gebeurtenis (Hazard/TopEvent) één.* *Voor de DPIA zijn hieronder mogelijke Kritische gebeurtenissen vermeld (in algemene termen en niet limitatief). Deze zijn gebaseerd op de beheersdoelstellingen (Contol Objectives) van het NOREA Privacy Control Framework:* *1. Persoonsgegevens zijn niet toereikend, ter zake dienend of te beperkt tot wat noodzakelijk is voor de geformuleerde doeleinden waarvoor zij worden verwerkt;* *2. Persoonsgegevens zijn niet juist en/of volledig;* *3. Persoonsgegevens worden verwerkt voor andere doeleinden dan wel verstrekt/beschikbaar gesteld of anderszins aan andere derden dan die zijn geformuleerd;* *4. Betrokkenen kunnen hun rechten niet/niet volledig uitoefenen waardoor persoonsgegevens niet juist en/of volledig zijn, niet verwijderd zijn, er geen beperking op de verwerking plaats vindt, et cetera;* *5. Er vindt ongeautoriseerde toegang, verstrekking of inbreuk plaats van persoonsgegevens;* *6. Er vindt onopzettelijke of ongeautoriseerde wijziging van persoonsgegevens plaats;* *7. Er vindt onopzettelijke verlies of ongeautoriseerde verwijdering van persoonsgegevens plaats.*
Bedreigingen (Threats)	*De Bedreigingen zijn de mogelijke oorzaken van de ongewenste/Kritieke gebeurtenis (Top Event). Deze bedreigingen beschikken over eigenschappen die het bedoelde proces kunnen verstoren, waardoor de controle over het proces (Risicobron/Hazard) wordt verloren en de Kritieke gebeurtenis (TopEvent) plaatsvindt.* *In de DPIA kunnen de bedreigingen hun oorzaak vinden in:* • *Interne menselijke bronnen (bijvoorbeeld uitvoerende medewerkers, managers, IT-medewerkers);* • *Externe menselijke bronnen (bijvoorbeeld ontvangers van de gegevens inclusief verwerkers; bevoegde overheidsorganisaties; bezoekers; onderhoudspersoneel; hackers; criminele organisaties);*

	• *Niet-menselijke bronnen (bijvoorbeeld fouten hardware, software en/of kanalen; schadelijke code van onbekende bronnen zoals virussen, wormen, et cetera; brand, water),* *De Bedreigingen moeten zo concreet mogelijk worden beschreven.*
Consequenties (Consequences)	*Als een Kritieke gebeurtenis (TopEvent) zich voordoet kan dit leiden tot bepaalde Consequenties. Het zijn de negatieve gevolgen van de procesverstoring; de onbedoelde schade van de Kritieke gebeurtenis.* *In de DPIA zijn dit primair de negatieve gevolgen voor de betrokkenen en secundair de negatieve gevolgen voor de organisatie.* *Net als de Bedreigingen dienen de Consequenties zo concreet mogelijk te worden beschreven.*
Barrières (Barriers)	*Risicomanagement gaat over het beheersen van risico's. Dit wordt gedaan door maatregelen (barrières) te plaatsen om te voorkomen dat bepaalde gebeurtenissen plaatsvinden. In de BowTie techniek zijn er:* • *Preventieve barrières (Proactive Barriers/Controls) die voorkomen dat een Kritieke gebeurtenis ontstaat (staan in het BowTie-dagram aan de linkerkant van de Kritieke gebeurtenis).* • *Herstel barrières (Reactive Barriers/Controls) die voorkomen dat de kritieke gebeurtenis leidt tot de negatieve Consequenties (staan in het BowTie-dagram aan de rechterkant van de Kritieke gebeurtenis).*
Escalatie factor / Escalatie factor barrière (Escalation factor / Escalation factor barrier)	*In een ideale situatie zal een barrière (maatregel) voorkomen dat een bedreiging de kritieke gebeurtenis veroorzaakt of de kritieke gebeurtenis leidt tot de consequentie. Veel maatregelen zijn echter niet 100% effectief. Er zijn bepaalde voorwaarden/condities waardoor een barrière kan falen. In de BowTie methodologie worden dit Escalatie factoren genoemd. Escalatie factoren kunnen op hun beurt worden beheerst door Escalatie factor barrières.* *In de DPIA wordt geadviseerd voorzichtig te zijn met het opnemen van Escalatie factoren in een BowTie-diagram.*

tabel 1: Begrippen BowTie

Uit te voeren stappen risico-identificatie DPIA met behulp van BowTie:

Stap 1. Stel de Risicobron/het Gevaar vast.

*In BowTie is de **Risicobron (Hazard)**, ook wel Gevaar genoemd, het proces dat onderdeel uitmaakt van de normale gang van zake maar dat schade kan veroorzaken.*

In de DPIA is de Risicobron het onderwerp van de DPIA; de in scope zijnde gegevensverwerking. Als de gegevensverwerking meerdere zeer uiteenlopende verwerkingsdoelen heeft en gebaseerd op meer dan één rechtmatigheidsgrondslag (zie vraag 2.2), wordt geadviseerd om per verwerkingsdoel/soortgelijke verwerkingsdoelen/grondslag een aparte Risicobron (Hazard) vast te stellen.

Stap 2. Stel de Kritieke gebeurtenis(sen) per Risicobron vast

*In BowTie is de **Kritieke gebeurtenis (Top Event)** de eerste gebeurtenis in een keten van ongewenste gebeurtenissen. Per Risicobron/Gevaar kunnen er meerdere verschillende Kritieke gebeurtenissen worden onderkend. In tabel 1 zijn voor DPIA's een aantal mogelijke Kritische Gebeurtenissen in algemene termen beschreven. Deze kunnen voor de in scope zijnde gegevensverwerking (Risicobron) nader worden geconcretiseerd.*

Stap 3. Stel een initiële BowTie op

Per Risicobron/Kritieke gebeurtenis-combinatie wordt een aparte BowTie-diagram opgesteld. De Kritieke gebeurtenis is het middelpunt van de BowTie. Voeg daar achtereenvolgens de Bedreigingen, Consequenties, Barrières en zo nodig Escalatie factoren aan toe.

a. ***Bedreigingen (Threats)**: De Kritieke gebeurtenis wordt veroorzaakt door Bedreigingen. Beschrijf de Bedreigingen zo concreet mogelijk en neem deze aan de linkerkant van de BowTie op. De Bedreigingen in de DPIA kunnen hun oorzaak bijvoorbeeld vinden in interne menselijke bron (binnen de organisatie); externe menselijke bron (buiten de organisatie) of niet-menselijke bron.*

b. ***Consequenties (Consequences)**: De Kritieke gebeurtenis kan leiden tot ongewenste/nadelige gevolgen, Consequenties. Beschrijf de Consequenties zo concreet mogelijk en neem deze aan de rechterkant van de BowTie op. In de DPIA zijn de Consequenties primair de negatieve gevolgen voor de betrokkenen. Deze kunnen betrekking hebben op fysieke, materiële en immateriële schade voor de betrokkenen. Secundair zijn het de negatieve gevolgen voor de organisatie (gevolg van een gevolg).*

c. ***Barrières (Barriers/Controls)**: de maatregelen die worden genomen om te voorkomen dat gebeurtenissen plaatsvinden. Hierbij wordt onderscheid gemaakt tussen Preventieve barrières (ter voorkoming van de Kritieke gebeurtenis) en Herstel barrières (ter voorkoming van de nadelige Consequenties).:*

   De in het NOREA Privacy Control Framework (PCF) opgenomen controls kunnen als bron dienen bij het bepalen van te nemen maatregelen (barrières).

   In geval de DPIA betrekking heeft op een bestaande gegevensverwerking dan worden in deze fase alleen de geïmplementeerde maatregelen opgenomen. Naar aanleiding van de risico-evaluatie kunnen eventueel aanvullende maatregelen worden toegevoegd waarbij dan weer geput kan worden uit de beschreven controls in PCF.

d. ***Escalatie factor (Escalation factor)**: Veel maatregelen zijn niet 100% effectief. Er zijn bepaalde voorwaarden waardoor een barrière kan falen. Zo'n voorwaarde/conditie wordt Escalatie factor genoemd. De Escalatie factor barrière voorkomt de Escalatie factor.*

8.2. Voer de risicoanalyse uit

Het tweede onderdeel van de risicobeoordeling is de *risicoanalyse*. De risicoanalyse is met name bedoeld om inzicht te krijgen in de aard van het risico en de kenmerken ervan, waaronder het risiconiveau. Wat zijn de inherente en restrisico's van de mogelijke negatieve gevolgen voor de betrokkene?

Nog eventuele openstaande vragen voor wat betreft risico's en maatregelen kunnen mogelijk worden beantwoord op basis van de goedgekeurde gedragscode (zie vraag 3.8), voor zover van toepassing.

Ter illustratie: Uitwerking risicoanalyse met behulp van BowTie

Vul de initiële BowTie-diagram(men) aan door (resultaat vraag 8.1):

a. ***Bijdrage Bedreiging bepalen**: Bepaal per Bedreiging de verwachte bijdrage (bijvoorbeeld Hoge Bijdrage, Middelmatige Bijdrage, Lage Bijdrage) die de Bedreiging heeft op het laten plaatsvinden van de Kritieke gebeurtenis. In het BowTie-diagram is dit als Bedreigings-categorie opgenomen.*

b. ***Inherente risico's bepalen**: Bepaal per Consequentie het inherente risico. Het inherente risico is het risico dat inherent is aan het proces voordat er rekening wordt gehouden met de eventuele daarop betrekking hebbende interne maatregelen.*

   *De verwachte waarde van het inherente risico kan worden ingeschat op basis van 'kans van optreden' * 'ernst van gevolgen (impact)'. De inschatting kan zowel gekwantificeerd als gekwalificeerd plaatsvinden en in verschillende mate van gedetailleerdheid (bijvoorbeeld een 3x3 schaal vs. een 5x5 schaal). Het team/degene die de DPIA uitvoert is hier vrij in. In is een voorbeeld opgenomen.*

Ernst van gevolgen / Kans van optreden	Klein	Middelgroot	Groot
Laag	Risico Zeer Laag	Risico Laag	Risico Middel
Middel	Risico Laag	Risico Middel	Risico Hoog
Hoog	Risico Middel	Risico Hoog	Risico Zeer Hoog

figuur 9: Voorbeeld kwalitatieve risico inschatting (3x3-schaal)

   Aan het BowTie-diagram kunnen zo nodig nog een Consequentie-categorie (bijvoorbeeld Groot Probleem, Middelgroot Probleem en Klein Probleem) worden toegevoegd.

c. ***Effectiviteit Barrières bepalen:***

   - *Bepaal de effectiviteit van de aan een Bedreiging gekoppelde Preventieve barrière op het voorkomen dat die Bedreiging leidt tot de Kritieke Gebeurtenis.*
   - *Bepaal de effectiviteit van de aan een Consequentie gekoppelde Herstel barrière op het voorkomen dat de Kritieke Gebeurtenis leidt tot die Consequentie.*

   Aan het BowTie-diagram kunnen zo nodig een Barrière-type (bijvoorbeeld gedrag, software, hardware, infra) worden toegevoegd.

d. ***Restrisico bepalen**: Bepaal per Consequentie het restrisico. Het restrisico is het risico van een ongewenste gebeurtenis dat resteert na het nemen van alle maatregelen om de ongewenste gebeurtenis te voorkomen. Gebruik hiervoor dezelfde matrix als bij het bepalen van het inherente risico. Houd bij het bepalen van het restrisico van een specifieke Consequent rekening met de vastgestelde:*

- *Bijdrage voor de relevante Bedreigingen;*
- *Effectiviteit van de aan die Bedreigingen gekoppelde Preventieve barrières;*
- *Effectiviteit van de aan de Consequentie gekoppelde Herstel barrières.*

8.3. Voer de Risico-evaluatie uit

Het derde en laatste onderdeel van de risicobeoordeling is de *risico-evaluatie*.

Zoals eerder is aangeven betekent het naleven van de AVG niet dat er helemaal geen risico's voor de rechten en vrijheden van de betrokkene mogen zijn. Elke gegevensverwerking houdt immers een risico in voor de betrokkene. De restrisico's voor de betrokkenen mogen alleen niet "hoog" zijn. Als dat het geval is, dient de organisatie voorafgaand aan de verwerking de AP te raadplegen..

De organisatie mag dus tot op zekere hoogte zelf bepalen wat haar risicobereidheid (risk appetite) is voor de risico's van de betrokkenen. Ten aanzien van de risico's die uitsluitend betrekking op de organisatie (meestal het gevolg zijn van een risico voor de betrokkene) is de AVG niet van toepassing en zijn er ook geen eisen aan de maximaal te accepteren restrisico's. De risicobereidheid hangt van veel factoren af. Tussen verschillende branches zal de risicobereidheid anders zijn (bijvoorbeeld social media versus financiële instellingen) maar ook tussen organisaties binnen dezelfde branche zal de risicobereid verschillen.

Bij de risico-evaluatie worden de resultaten van de risicoanalyse vergeleken om te bepalen waar aanvullende actie is vereist. Dit kan leiden tot een besluit om:

a. **verder niets te doen (accepteren risico):** Het accepteren van het restrisico van de betrokkenen, zolang deze lager is dan "hoog", en voor de organisatie is afhankelijk van de risicobereidheid (risk appetite) van de organisatie.

b. **na te denken over opties voor risicobehandeling (beheersen risico)**: Als de bestaande/voorgenomen maatregelen voor een negatief gevolg niet effectief zijn en de organisatie het restrisico niet wil/kan accepteren dan is een optie deze maatregelen te vervangen en/of nieuwe maatregelen toe te voegen (zie ook vraag 9.1);

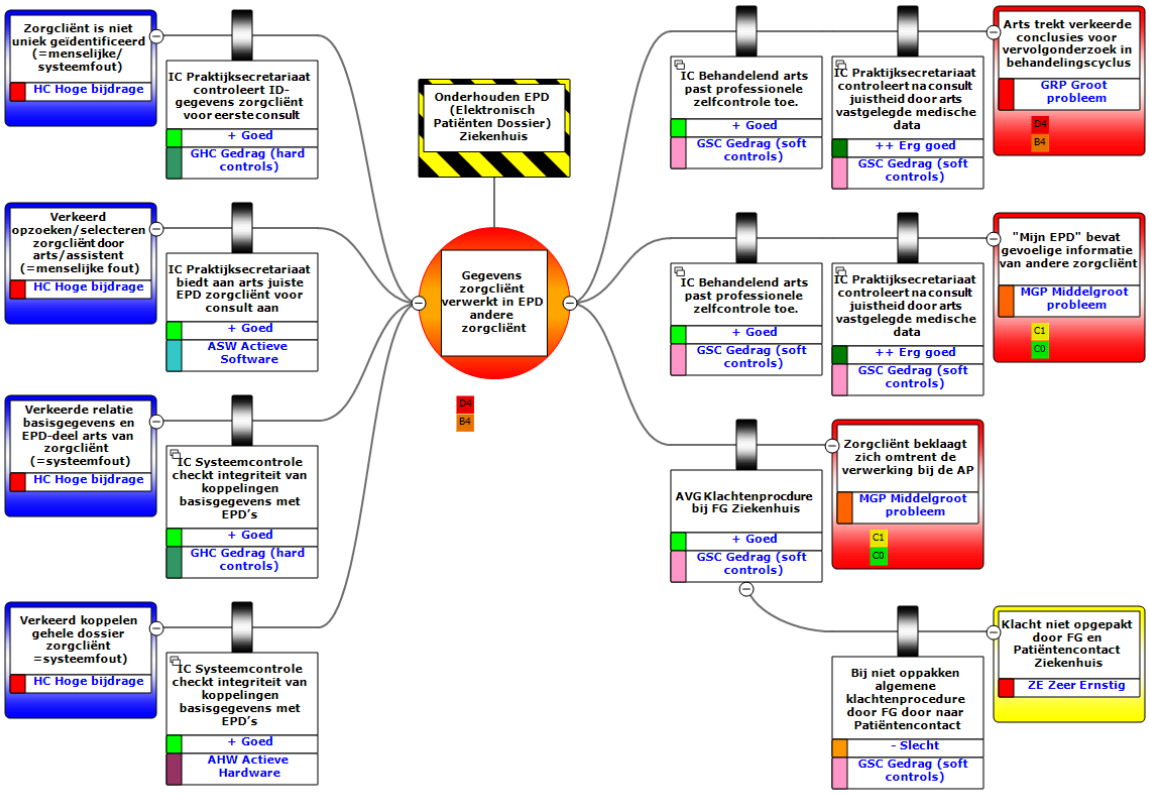
c. **doeleinden te herzien (elimineren risico)**: Als de organisatie het restrisico niet wil/kan accepteren en geen gewijzigde/nieuwe maatregelen kan nemen, kan de organisatie ook de doeleinden van de gegevensverwerking herzien; een of meer doeleinden wijzigen dan wel laten vervallen waardoor negatieve gevolgen worden voorkomen of beperkt.

Ter illustratie: Uitwerking risico-evaluatie met behulp van BowTie

Wijzigingen als gevolg van onderdeel b) en c) worden in het BowTie-diagram doorgevoerd waarna de risicoanalyse (vraag 8.2) en risico-evaluatie (vraag 8.3) voor het betreffende deel opnieuw wordt doorlopen. Dit is een iteratief proces.

Neem vervolgens per Risicobron/Kritieke gebeurtenis-combinatie het definitieve BowTie-diagram op.

In figuur 10 en figuur 11 zijn de risicobeoordelingen (risk assessments) opgenomen voor twee verschillende verwerkingsactiviteiten. Het eerste voorbeeld gaat over het onderhouden van een EPD (elektronisch patiënten dossier) en het tweede voorbeeld over het stimuleren van de vergroening van het rijgedrag van leaserijders binnen een bepaalde organisatie. De voorbeelden zijn uitsluitend bedoeld ter illustratie voor het gebruik van de begrippen binnen BowTie en hebben niet de intentie juist en volledig te zijn. In bijlage 0 worden deze twee voorbeelden nader toegelicht en zijn de BowTie-diagrammen uitgebreider.

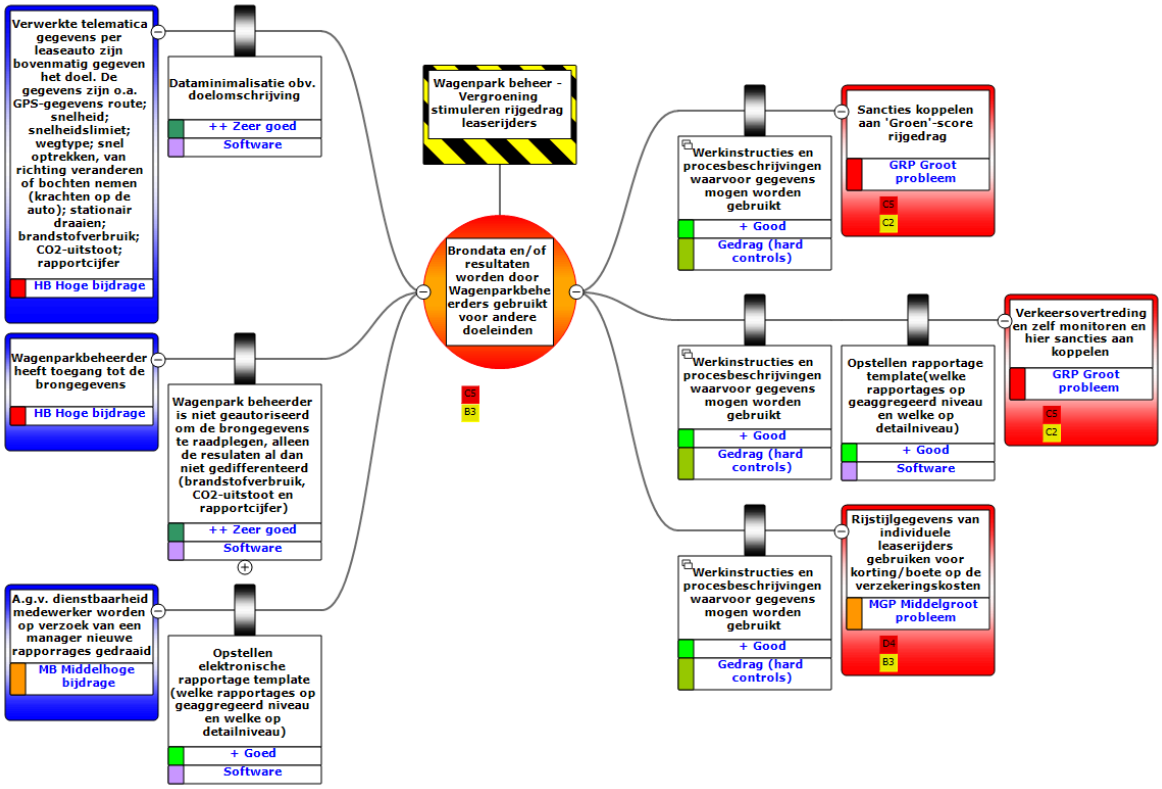


figuur 10: Voorbeeld BowTie-diagram voor Onderhouden EPD-dossier/ Gegevens zorgcliënt verwerkt in EPD andere zorgcliënt (gemaakt met BowTie XP).

Korte toelichting figuur 10: Voor de DPIA 'Onderhouden van een EPD (Elektronisch Patiënten Dossier)' is de Risicobron/het Gevaar 'Onderhouden EPD'. Een Kritieke gebeurtenissen voor het proces 'Onderhouden EPD' is 'Gegevens zorgcliënt verwerkt in EPD andere zorgcliënt'. Dit is een concretisering van de in tabel 1 genoemde Kritieke gebeurtenis '2. Persoonsgegevens zijn niet juist en/of volledig'. Bedreigingen zijn onder andere 'Verkeerd opzoeken/ selecteren zorgcliënt door arts/assistent' en

'Verkeerd koppelen gehele dossier zorgcliënt', respectievelijk interne menselijke fout en niet-menselijke fout (systeem-fout). Consequenties zijn onder meer 'Arts voert verkeerde behandeling op de zorgcliënt' (negatief gevolg betrokkene; primaire consequentie) en 'Ziekenhuis moet schadevergoeding betalen aan zorgcliënt' (negatief gevolg organisatie; secundaire consequentie). Een Preventieve barrière is bijvoorbeeld 'Secretariaat biedt aan arts juiste EPD zorgcliënt voor consult aan' en een voorbeeld van een Herstel barrière is 'Behandelend arts past professionele zelfcontrole toe'.

Voor de Consequentie "Zorgclient klaagt bij de AP" is Herstel barrière 'Een klacht kan worden ingediend bij de FG van het Ziekenhuis opgenomen'. Nu kan het voorkomen dat de FG de klacht om welke reden dan ook niet (tijdig) oppakt. De Escalatie factor zou dan zijn 'FG pakt klacht zorgcliënt niet op' en een mogelijke Escalatie factor beheersmaatregel 'Bij niet oppakken algemene klachtenprocedure FG door naar Patiëntencontact'.



figuur 11: Voorbeeld BowTie-diagram voor Wagenparkbeheer – Vergroening stimuleren/ Brondata en resultaten worden door Wagenparkbeheerders gebruikt voor andere doeleinden (gemaakt met BowTie XP)

Korte toelichting figuur 11: Voor een DPIA op het 'Wagenparkbeheer' is een van de doeleinden het stimuleren dat de leaserijders 'groener' zouden gaan rijden. Het voorstel was om hiervoor het rijgedrag van de berijder continue te monitoren middels 'car telematics'. De Risicobron/het Gevaar is 'Wagenparkbeheer – Vergroening stimuleren rijgedrag leaserijder. Een van de Kritieke gebeurtenis voor het proces 'Wagenparkbeheer – Vergroening rijgedrag' is bijvoorbeeld 'Brondata en resultaten worden door wagenparkbeheerder gebruikt voor andere doeleinden' ('function creep'). Dit is een concretisering van de in tabel 1 genoemde Kritieke gebeurtenis '3. Persoonsgegevens worden verwerkt voor andere doeleinden dan wel verstrekt/beschikbaar gesteld of anderszins aan andere derden dan die zijn geformuleerd'.

Bedreigingen zijn onder andere 'Verwerkte persoonsgegevens zijn bovenmatig gegeven het doel' en 'Als gevolg van dienstbaarheid medewerkers worden op verzoek van een manager nieuwe rapportages gedraaid', respectievelijk een niet-menselijke fout (systeemfout) en interne menselijke fout. Consequenties zijn onder meer 'Sancties koppelen aan 'groen'-score rijgedrag' (negatief gevolg betrokkene; primaire consequentie) en 'Rijstijlgegevens van individuele leaserijders gebruiken voor korting/boete op de verzekeringskosten'. Een Preventieve barrière kan bijvoorbeeld zijn 'Dataminimalisatie toepassen' en een Herstel barrière kan zijn 'Werkinstructies en procesbeschrijvingen waarvoor gegevens mogen worden gebruikt.

8.4. Bepaal of voorafgaande raadpleging bij de AP noodzakelijk is.

Als het restrisico voor een of meer van de negatieve gevolgen voor de betrokkene 'Hoog' is en de organisatie kan/wil geen aanvullende maatregelen nemen om het risico te verkleinen dan dient de organisatie de AP te raadplegen voorafgaand aan de verwerking.

Indien dit het geval is dient te worden aangetoond dat de voorafgaande raadpleging heeft plaatsgevonden en wat de reactie van de AP was.

9. Risicobehandeling

Het doel van risicobehandeling (risk treatment) is het selecteren en implementeren van opties voor het aanpakken van risico's.

Risicobehandeling omvat een iteratief proces van:

- het formuleren en selecteren van opties voor risicobehandeling;
- het plannen en implementeren van risicobehandeling;
- het beoordelen of de behandeling doeltreffend is;
- het beslissen of het resterende risico aanvaardbaar is;
- het overgaan tot verdere behandeling indien dit niet aanvaardbaar is.

Op basis van de uitgevoerde risicobeoordeling (vragen 8.1- 8.3) zijn zowel de risico's als een set aan maatregelen om deze risico's te voorkomen/te mitigeren tot een acceptabel niveau in kaart gebracht. De maatregelen kunnen worden geprioriteerd, tijdlijnen voor implementatie worden vastgesteld, te nemen acties en verantwoordelijke afdelingen/functionarissen kunnen worden benoemd, et cetera. Beoordeeld dient te worden of de geïmplementeerde maatregelen doeltreffend zijn, of het resterende risico aanvaardbaar is en of nog dient te worden overgegaan tot het nemen van aanvullende maatregelen. Hierbij dient te worden opgemerkt dat het proces van "geadviseerde maatregelen" tot "te nemen acties" in de regel in fases plaatsvindt; voor een effectieve implementatie hiervan moeten goede afspraken worden gemaakt.

9.1. Benoem de te nemen acties (onder andere verantwoordelijkheid, prioriteit en doorlooptijd) voor de geselecteerde maatregelen opnemen in een tabel of toevoegen aan het BowTie-diagram.

Op basis hiervan kan een concreet actieplan worden opgesteld voor de te nemen acties naar aanleiding van de DPIA. Wie is verantwoordelijk, betreft het een bestaande/nieuwe maatregel, wat is de prioriteit, de doorlooptijd, et cetera

Bij voorkeur zijn alle maatregelen geïmplementeerd voordat wordt aangevangen met de nieuwe verwerking zodat de verwerking in overeenstemming is met de risicobereidheid van de organisatie. In ieder geval dienen die maatregelen te zijn geïmplementeerd die ervoor zorgen dat het restrisico onder het niveau 'Hoog' zit. Indien dat niet gerealiseerd kan worden is afstemming met de AP nodig.

Deel IV: Ondertekening DPIA-rapportage

Voor het borgen van de beheersing van de risico's wordt geadviseerd de DPIA-rapportage te laten ondertekenen door bijvoorbeeld de proceseigenaar, de FG (indien aanwezig)/Privacy officer, CISO en de algemeen directeur/Raad van Bestuur.

C. Bijlagen

I. Criteria EDPB voor een aanvaardbare DPIA

In bijlage 2 van WP248.rev01 "Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking 'waarschijnlijk hoog risico inhoudt' in de zin van Verordening 2016/79" stelt de EDPB de onderstaande criteria voor die verwerkingsverantwoordelijken kunnen gebruiken om te beoordelen of een DPIA, of een methode voor het uitvoeren van een DPIA, volledig genoeg is om aan de AVG te voldoen:

- er wordt een systematische beschrijving van de verwerking verstrekt (artikel 35, lid 7, onder a)):
  - er wordt rekening gehouden met de aard, omvang, context en doelen van de verwerking (overweging 90);
  - de persoonsgegevens, de ontvangers en de periode gedurende welke de persoonsgegevens worden bewaard worden geregistreerd;
    - er wordt een functionele beschrijving van de verwerking verstrekt;
    - de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen) worden geïdentificeerd;
    - er wordt rekening gehouden met de naleving van de goedgekeurde gedragscodes (artikel 35, lid 8);
- de noodzaak en evenredigheid worden beoordeeld (artikel 35, lid 7, onder b)):
  - de beoogde maatregelen om aan de verordening te voldoen worden bepaald (artikel 35, lid 7, onder d), en overweging 90), waarbij rekening wordt gehouden met:
    - maatregelen die bijdragen aan de evenredigheid en noodzaak van de verwerking op basis van:
      - een of meer gespecificeerde, expliciete en legitieme doeleinden (artikel 5, lid 1, onder b));
      - rechtmatigheid van de verwerking (artikel 6);
      - toereikend, ter zake dienend en beperkt tot wat noodzakelijke gegevens zijn (artikel 5, lid 1, onder c));
      - beperkte bewaartermijn (artikel 5, lid 1, onder e));
    - maatregelen die bijdragen aan de rechten van de betrokkenen:
      - informatie verstrekt aan de betrokkene (artikelen 12, 13 en 14);
      - recht van inzage en recht op overdraagbaarheid van gegevens (artikelen 15 en 20);

- recht op rectificatie en recht op gegevenswissing (artikelen 16, 17 en 19);
- recht van bezwaar en recht op beperking van de verwerking (artikelen 18, 19 en 21);
- relaties met verwerkers (artikel 28);
- waarborgen omtrent internationale doorgifte(n) (hoofdstuk V);
- voorafgaande raadpleging (artikel 36).

- de risico's voor de rechten en vrijheden van betrokkenen worden beheerd (artikel 35, lid 7, onder c)):
  - er wordt rekening gehouden met de oorsprong, de aard, het specifieke karakter en de ernst van de risico's (zie overweging 84) of, meer specifiek, voor elk risico (onrechtmatige toegang, ongewenste wijziging en verdwijning van gegevens) vanuit het perspectief van de betrokkenen:
    - er wordt rekening gehouden met de bronnen van de risico's (overweging 90);
    - de mogelijke gevolgen voor de rechten en vrijheden van de betrokkenen worden geïdentificeerd in geval van gebeurtenissen zoals onrechtmatige toegang, ongewenste wijziging en verdwijning van gegevens;
    - bedreigingen die kunnen leiden tot onrechtmatige toegang, ongewenste wijziging en de verdwijning van gegevens worden geïdentificeerd;
    - de waarschijnlijkheid en ernst worden ingeschat (overweging 90);
  - de beoogde maatregelen om de risico's aan te pakken worden bepaald (artikel 35, lid 7, onder d), en overweging 90);
  - de belanghebbenden worden betrokken
    - het advies van de functionaris voor gegevensbescherming wordt ingewonnen (artikel 35, lid 2)
    - indien nodig wordt de betrokkenen of hun vertegenwoordigers naar hun mening gevraagd (artikel 35, lid 9).

II. Referenties

De Handreiking DPIA en het Raamwerk DPIA zijn gebaseerd op onder meer de volgende documenten/bronnen (in alfabetische volgorde):

- Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679) en Uitvoeringswet Algemene Verordening Gegevensbescherming
- Handleiding AVG en UAVG van het Ministerie van Veiligheid en Justitie (jan. 2018)
- ISO 31000: 2018 – Risk management – Guidelines
- ISO 31010: 2019 – Risk management – Risk assessment techniques
- Lijst van Autoriteit Persoonsgegevens met soorten verwerkingen waarvoor een DPIA verplicht is
- NOREA Handreiking Privacy Control Framework (v2.0), augustus 2019
- Wet Politiegegevens
- WP248.rev01 Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking 'waarschijnlijk hoog risico inhoudt' in de zin van Verordening 2016/79" (okt. 2017)
- WP2451.rev01 Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening 2016/79" (feb. 2018)
- WP259.rev01 Richtsnoeren voor toestemming inzake Verordening 2016/79" (april 2018)

III. Begrippenlijst

Hieronder zijn in alfabetische volgorde de belangrijkste definities opgenomen zoals beschreven in art. 4, 9 en 26 AVG.

Betrokkene	een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Bijzondere persoonsgegevens	Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.
Inbreuk in verband met persoons-gegevens (datalek)	een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens
Persoonsgegevens	alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene").
Verwerking	een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
Verwerker	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
Verwerkingsverantwoordelijke	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

IV. Lijst van soorten verwerkingen waarvoor een DPIA verplicht is van de AP

De Autoriteit Persoonsgegevens heeft onderstaande lijst[12] opgesteld van soorten verwerkingen waarvoor het uitvoeren van een DPIA altijd verplicht is vóórdat begonnen wordt met verwerken. Deze lijst is aan verandering onderhevig. Geadviseerd wordt de actualiteit te verifiëren voordat begonnen wordt met het DPIA-proces.

1. Heimelijk onderzoek

Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens waarbij informatie wordt verzameld met onderzoek, zonder de betrokkene daarvan vooraf op de hoogte te stellen.

Bijvoorbeeld heimelijk onderzoek door particuliere recherchebureaus, onderzoek voor fraudebestrijding en onderzoek op internet voor bijvoorbeeld online handhaving van auteursrechten.

Een DPIA is ook verplicht bij heimelijk cameratoezicht door werkgevers om diefstal of fraude door werknemers te bestrijden. Hierbij moet soms ook een DPIA worden uitgevoerd vanwege de ongelijkwaardige machtsverhouding tussen werknemer en werkgever.

2. Zwarte lijsten

Verwerkingen waarbij persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door organisaties of particulieren worden verwerkt en gedeeld met derden.

Bijvoorbeeld zwarte lijsten of waarschuwingslijsten, zoals verzekeraars, horecabedrijven, winkelbedrijven en telecomproviders die gebruiken. En ook zwarte lijsten die gaan over onrechtmatig gedrag van werknemers, bijvoorbeeld in de zorg of door uitzendbureaus.

3. Fraudebestrijding

Grootschalige verwerkingen en/of stelselmatige monitoring van (bijzondere) persoonsgegevens voor fraudebestrijding. Bijvoorbeeld fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars.

[12] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia?qa=dpia (geraadpleegd op 30 juni 2020)

4. Creditscores

Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen, bijvoorbeeld tot uitdrukking gebracht in een creditscore.

5. Financiële situatie

Grootschalige verwerkingen en/of stelselmatige monitoring van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden. Bijvoorbeeld overzichten van bankoverschrijvingen, overzichten van de saldi van iemands bankrekeningen of overzichten van mobiele- of pinbetalingen.

6. Genetische persoonsgegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van genetische persoonsgegevens. Bijvoorbeeld DNA-analyses om persoonlijke kenmerken in kaart te brengen, bio-databanken.

7. Gezondheidsgegevens

Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratiebedrijven, (speciaal)onderwijsinstellingen, verzekeraars en onderzoeksinstituten), waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid.

Let op: individuele artsen en individuele zorgprofessionals zijn op grond van overweging 91 van de AVG uitgezonderd van de verplichting een DPIA uit te voeren.

8. Samenwerkingsverbanden

Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard met elkaar uitwisselen, zoals gegevens over gezondheid, verslaving, armoede, problematische schulden, werkloosheid, sociale problematiek, strafrechtelijke gegevens, betrokkenheid van jeugdzorg of maatschappelijk werk. Bijvoorbeeld in wijkteams, veiligheidshuizen of informatieknooppunten.

9. Cameratoezicht

Grootschalige verwerkingen en/of stelselmatige monitoring van openbaar toegankelijke ruimten met camera's, webcams of drones.

10. Flexibel cameratoezicht

Grootschalig en/of systematisch gebruik van flexibel cameratoezicht. Bijvoorbeeld camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams gebruikt door hulpdiensten.

11. Controle werknemers

Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens om activiteiten van werknemers te monitoren. Bijvoorbeeld controle van e-mail en internetgebruik, GPS-systemen in (vracht)auto's van werknemers of cameratoezicht voor diefstal- en fraudebestrijding.

12. Locatiegegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van locatiegegevens van of herleidbaar tot natuurlijke personen. Bijvoorbeeld door (scan)auto's, navigatiesystemen, telefoons, of verwerking van locatiegegevens van reizigers in het openbaar vervoer.

13. Communicatiegegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder of het randapparaat van de eindgebruiker.

14. Internet of things

Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen. Bijvoorbeeld 'internet of things'- toepassingen, zoals slimme televisies, slimme huishoudelijke apparaten, connected toys, smart cities, slimme energiemeters, medische hulpmiddelen, et cetera

15. Profilering

Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering). Bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.

16. Observatie en beïnvloeding van gedrag

Grootschalige verwerkingen van persoonsgegevens waarbij op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen wordt geobserveerd of beïnvloed, dan wel gegevens die daarover worden verzameld en/of vastgelegd, inclusief gegevens die voor het doel online behavioural advertising worden verzameld.

17. Biometrische gegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren.

NB: Op grond van de AVG is de verwerking van biometrische gegevens met als doel de unieke identificatie van een natuurlijk persoon in beginsel verboden. In Nederland zijn aanvullende voorwaarden gesteld in de Uitvoeringswet AVG. De verwerking van biometrische gegevens is alleen toegestaan als de verwerking strikt noodzakelijk is voor authenticatie of beveiligings-doeleinden.

V. Criteria European Data Protection Board (EDPB)

De EDPB heeft negen criteria[13] opgesteld om te beoordelen of een voorgenomen verwerking van persoonsgegevens een 'hoog' privacyrisico oplevert voor de betrokken personen. Als vuistregel geldt dat een DPIA uitgevoerd moet worden uitvoeren als de verwerking aan twee of meer van de onderstaande negen criteria voldoet.

1. Beoordelen van mensen op basis van persoonskenmerken

Het gaat hierbij onder meer om profilering en het maken van prognoses, met name op basis van kenmerken als iemands beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen.

Voorbeelden hiervan zijn een bank die de kredietwaardigheid van klanten bepaalt (creditscoring), een bedrijf dat DNA-testen aan consumenten levert om gezondheidsrisico's te testen en een bedrijf dat bezoekers van zijn website volgt en op basis daarvan profielen van deze mensen opstelt.

2. Geautomatiseerde beslissingen

Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Zo'n gegevensverwerking kan er bijvoorbeeld toe leiden dat mensen worden uitgesloten of gediscrimineerd. Gegevensverwerkingen met geringe of geen gevolgen voor mensen vallen niet onder dit criterium.

Voor meer informatie, zie de handreiking over geautomatiseerde besluitvorming en profilering[14] (Engelstalig) van de EDPB.

3. Stelselmatige en grootschalige monitoring

Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht. Hierbij kunnen persoonsgegevens worden verzameld zonder dat betrokkenen weten wie hun gegevens verzamelt en wat daar vervolgens mee gebeurt. Bovendien kan het onmogelijk zijn voor mensen om zich in openbare ruimten aan deze gegevensverwerking te onttrekken.

---

[13] WP248.rev01 "Richtsnoeren voor gegevenseffectbeoordelingen en bepaling of een verwerking 'waarschijnlijk hoog risico inhoudt' in de zin van Verordening 2016/79" (okt. 2017);

[14] WP251.rev01"Richtsnoeren inzake geautomatiseerde individueel besluitvorming en profilering voor toepassing van Verordening 2016/79 " (feb. 2018); https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf

4. Gevoelige gegevens

Het gaat hierbij om bijzondere categorieën van persoonsgegevens (zie artikel 9 van de AVG), zoals informatie over iemands politieke voorkeuren. Ook strafrechtelijke gegevens vallen hieronder. Tot slot gaat het hier ook om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens.

5. Grootschalige gegevensverwerkingen

De AVG geeft geen definitie van 'grootschalige gegevensverwerkingen'. De EDPB adviseert om met de volgende criteria te bepalen of hiervan sprake is:

- de hoeveelheid mensen van wie gegevens worden verwerkt;
- de hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt;
- de tijdsduur van de gegevensverwerking;
- de geografische reikwijdte van de gegevensverwerking.

Zie ook: wat ziet de AVG als een grootschalige verwerking van persoonsgegevens?

6. Gekoppelde databases

Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn. Bijvoorbeeld databases die voortkomen uit twee of meer verschillende gegevensverwerkingen met verschillende doelen en/of uitgevoerd door verschillende verantwoordelijken, op een manier die betrokkenen niet redelijkerwijs kunnen verwachten.

7. Gegevens over kwetsbare personen

Bij het verwerken van dit type gegevens kan een DPIA nodig zijn omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens. Het kan hierbij om bijvoorbeeld werknemers, kinderen en patiënten gaan.

8. Gebruik van nieuwe technologieën

De AVG is er duidelijk over dat een DPIA nodig kan zijn bij het gebruik van een nieuwe technologie. De reden hiervoor is dat dit gebruik gepaard kan gaan met nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacyrisico's.

De persoonlijke en maatschappelijke gevolgen van het gebruik van een nieuwe technologie kunnen zelfs nog onbekend zijn. Een DPIA helpt de verantwoordelijke dan om de risico's te begrijpen en te verhelpen.

Sommige 'Internet of Things'-toepassingen bijvoorbeeld kunnen een grote impact hebben op het dagelijks leven en de privacy van mensen, waardoor hierbij een DPIA nodig is.

9. Blokkering van een recht, dienst of contract

Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen:

- een recht niet kunnen uitoefenen of;
- een dienst niet kunnen gebruiken of;
- een contract niet kunnen afsluiten.

Bijvoorbeeld een bank die persoonsgegevens verwerkt om te bepalen of zij een lening aan iemand willen verstrekken.

VI. Mogelijke rollen/deelnemers bij het uitvoeren van een DPIA

Indien de DPIA door een team wordt uitgevoerd kan sprake zijn van verschillende rollen, al dan niet verdeeld over verschillende deelnemers. Hierna is een aantal rollen opgenomen. De rollen illustreren welke partijen betrokken kunnen zijn bij het uitvoeren van de DPIA en welke type vragen zij met de uitvoering van de DPIA wensen te beantwoorden. De IT-auditor kan afhankelijk van zijn kennis en ervaring als adviseur een of meerdere rollen vervullen bij het uitvoeren van een DPIA.

- Opdrachtgevers/initiatiefnemers en investeerders van het project: Is het initiatief/project haalbaar vanuit de optiek van privacybescherming en de daarmee samenhangende risico's? Doen we – gegeven de risico's – een verantwoorde investering? Dit zijn bijvoorbeeld aandeelhouders, producteigenaren, proceseigenaren, systeemeigenaren en data-eigenaren.

- Opdrachtnemer/verantwoordelijke uitvoering van het project: Houden we ook voldoende rekening met de niet-functionele eisen en wensen, in dit geval het onderwerp privacybescherming en hieraan gerelateerde onderwerpen (beveiliging, document- en archiefbeheer en dergelijke)? Kennen we de risico's en beheersen we deze afdoende? Verantwoordelijk voor de uitvoering van het initiatief zijn veelal de directie/management en indien aangesteld de projectleiding.

- Opdrachtnemer/verantwoordelijke uitvoering van de DPIA: Wordt de DPIA op een gedegen wijze uitgevoerd? Worden de juiste experts ingezet? Wordt rekening gehouden met alle belanghebbenden?

- Meedenkers/Experts: Krijgt het onderwerp privacy en hieraan gerelateerde onderwerpen (beveiliging, document- en archiefbeheer en dergelijke) juiste/voldoende aandacht? Is helder wat een en ander concreet betekent voor de praktijk van de uitvoering? Meedenkers zijn te splitsen in drie 'competentiegroepen':

  1. Personen die de organisatie en/of het project goed kennen.

  2. Experts die deskundig zijn op het onderwerp:
     - Techniek;
     - Informatiebeveiliging;
     - Privacy;
     - Juridische aspecten;
     - Organisatorische aspecten;
     - Risicomanagement;
     - Data analytics;
     - Andere aandachtsgebieden die voor het project van belang zijn.

3. Uitvoerders: De resultaten van de DPIA moeten leiden tot concrete instructies c.q. randvoorwaarden voor de uitvoerders. Deze uitvoerders zijn bijvoorbeeld de systeemontwikkelaars (waaronder ICT-dienstverleners), architecten, product-ontwikkelaars en beleidsmakers. Zij moeten precies weten binnen welke kaders zij hun werk kunnen doen. Om dit te kunnen weten, is het gewenst dat zij meedenken.

- Meekijkers/beoordelaars (DPIA assessor): Wordt op adequate wijze rekening gehouden met de impact van het project op betrokkenen en met de risico's voor de betrokkenen, voor de eigen organisatie en de belanghebbenden? Meekijkers vervullen met name een Quality Assurance rol tijdens het traject en beoordelaars vervullen meer een controlerende rol aan het einde van (bepaalde fases in) het project. Deze rollen kunnen worden vervuld door professionele privacy assessors (privacy adviseurs en privacy auditors), maar mogelijk ook de Compliance Officer, de Privacy Officer en de Functionaris voor de Gegevensbescherming.

Overigens zullen niet alle personen continu bij de DPIA-activiteiten betrokken zijn. De samenstelling van het DPIA-team en de betrokken expertises kunnen gedurende de verschillende fasen van het project wijzigen. Zo zullen aanvankelijk de juridische experts meer betrokken zijn en pas later bijvoorbeeld informatieanalisten, beveiligingsspecialisten en uitvoerders (waaronder architecten).

De personen kunnen uit de eigen organisatie komen, dan wel van daarbuiten.

VII. Uitgewerkte BowTie-diagrammen

Disclaimer:
De uitwerkingen van het primaire proces EPD en van het Wagenparkbeheer zijn slechts voorbeelden voor een risico situatie die in kaart is gebracht op basis van de BowTie methodiek. Er mogen geen conclusie worden getrokken dat deze voorbeelden juist, volledig of betrouwbaar is. In iedere ziekenhuis omgeving zal, hangende de keuze welk EPD-systeem is gekozen, andere uitkomsten denkbaar zijn. Dit geldt ook voor de leasemaatschappijen gebruikte telematica oplossingen en de aangeboden applicatie voor de wagenparkbeheerder van de leasende organisatie.

VII.1 DPIA: Onderhouden Elektronisch Patiënten Dossier

Het primaire proces EPD (Elektronisch Patiënten Dossier) is in een ziekenhuis het hart van de informatievoorziening rondom de gezondheidszorg. Het doet meer dan de naam sec zou doen geloven. Binnen het primaire proces EPD is er sprake van meerdere verwerkingen met elk hun eigen kenmerken in relatie tot de AVG en sectorale wetgeving:

Verwerking	Wet en regelgeving	Wie mag toegang hebben	Wie verantwoordelijk
Aanmelding zorgcliënt	Avg: voornamelijk algemene persoonsgegevens	Algemene balie Balies polikliniek	Ziekenhuis beschikbaar-stelling EPD
	Gebruik BSN verplicht: Artikel 4 Wabvpz *(Wet Aanvullende Bepalingen Verwerking Persoonsgegevens in de Zorg)*	Algemene balie Balies polikliniek	College van Bestuur Ziekenhuis
		Facilitaire dienst voor diverse diensten	College van Bestuur Ziekenhuis
Elektronisch Patiënten dossier	Avg + Wgbo (Afd 5 BW7): artikel 454 Wgbo *(Wet Geneeskundige Behandelings Overeenkomst)*	AGB-gecertificeerde zorgverlener (arts) en BIG-gecertificeerde verpleegkundige	College van Bestuur Ziekenhuis voor beschikbaar-stelling EPD. AGB-gecertificeerde voor het medisch dossier
	Procestoestemming: Artikel 15a tm 15c Wabvpz	AGB-gecertificeerde zorgverlener (arts)	AGB-gecertificeerde zorgverlener (arts)
	Wkkgz *(Wet Kwaliteit, Klachten en Geschillen Zorg)*	Klachtencommissie bestaande uit aangewezen AGB-zorgverleners	College van Bestuur Ziekenhuis AGB-zorgverlener
	Bekostiging van ziekenhuis en medisch specilaisten *(Regeling declaratiebepalingen DBC-bedragen: Behandeling van DBC-codering voorzien)*	AGB-gecertificeerde zorgverlener (arts) BIG-gecertificeerde verpleegkundige	College van Bestuur ZiekenhuisAGB-gecertificeerde zorgverlener (arts)
Onderzoek en research	Avg + Wgbo (Afd 5 BW7): artikel 454 Wgbo	AGB-gecertificeerde zorgverlener (arts) BIG-gecertificeerde verpleegkundige	AGB-gecertificeerde zorgverlener (arts)
	Specifieke toestemming vereist voor toegespitst onderzoek met het oog op research op een zorgcliënt	AGB-gecertificeerde zorgverlener (arts)	AGB-gecertificeerde zorgverlener (arts)
Verwerking bekostiging	Wet marktordening gezondheidszorg en Regeling declaratiebepalingen DBC-bedragen	BI-afdeling specifiek benoemde functionarissen met toegang tot DBC-informatie t.b.v.: - Opstellen declaraties zorgverzekeraars en verdelen gelden naar medisch specialisten en ziekenhuis - Opstellen stuurinformatie	College van Bestuur Ziekenhuis
Authenticatie en Identificatie toegang EPD en monitoring toegang	Procestoestemming: Artikel 15a tm 15f Wabvpz	IT systeembeheer: Inregelen authorisaties	College van Bestuur Ziekenhuis
		HR, Functiehoofden waaronder AGB-gecertificeerden, BIG-gecertificeerde, CISO, FG	College van Bestuur Ziekenhuis
		FG en CISO: beoordeling breaking the glass procedure	College van Bestuur Ziekenhuis

tabel 2: Voorbeeld verwerkingen die onderdeel zijn van het primaire proces EPD

Uit bovenstaand niet-limitatieve overzicht blijkt dat uit de primaire bedrijfsactiviteit EPD meerdere verwerkingen zijn vast te stellen. De verwerking Elektronisch Patiënten Dossier is de kern waar het om gaat. Onder deze verwerking zijn tientallen operationele processen te herkennen, vaak toegespitst per specialisme of ondersteunende medische onderzoeks-

afdelingen zoals röntgen, laboratorium, e.d. Ieder individueel proces is relatief eenvoudig. Het gaat niet om complexe processtappen, maar om de aard van de verwerkte gegevens, met name veel bijzondere persoonsgegevens. Deze zijn uitsluitend voor de behandelend AGB-gecertificeerde arts. Deze arts bepaalt wat er in het dossier wordt vastgelegd en welke BIG-gecertificeerde verpleegkundige(n) toegang krijgen (poliklinische afdelings-verpleegkundigen, administratieve ondersteuning, verpleegafdeling, ziekenhuisapotheek, e.d.).

Kritieke gebeurtenissen EPD

De volgende Kritieke gebeurtenissen (Top Events) werden onder meer herkend in een uitgevoerde DPIA met betrekking tot het EPD (niet limitatief):

- Primair: Medische gegevens van een zorgcliënt worden verwerkt in EPD waar deze zorgcliënt geen uitdrukkelijke toestemming heeft gegeven voor verwerking van diens gegevens in een EPD. Verwerking in een EPD houdt feitelijk direct in dat de gegevens worden doorgegeven aan andere zorgverleners zoals huisarts en apotheek;
- **Primair: Medische gegevens worden door de arts of verpleegkundige in een EPD verwerkt van een andere zorgcliënt dan de betrokken zorgcliënt. Interne controle processen dienen daarvoor in de plaats te zijn;**
- Primair: Zorgcliënt heeft toegang tot een EPD van een andere zorgcliënt;
- Ondersteunend: Ongeautoriseerde toegang in het medisch deel en BI-deel van een EPD van een zorgcliënt of tot het EPD in het algemeen;
- Et cetera.

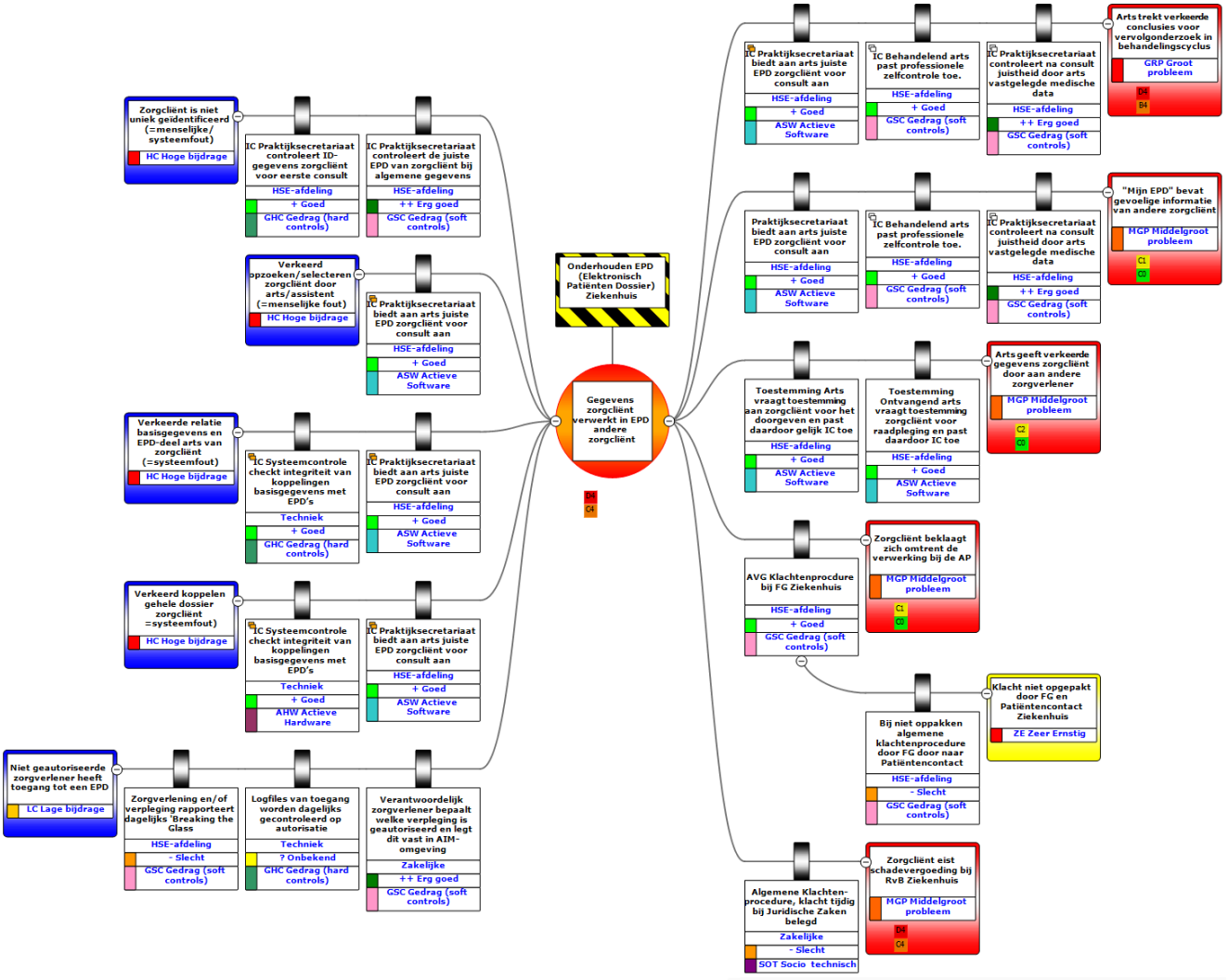
Als voorbeeld voor deze handreiking werken wij het tweede top-event op deze lijst verder uit, waarbij de Risicobron/het Gevaar (Hazard) betreft het 'Onderhouden EPD ziekenhuis' en de Kritieke Gebeurtenis 'Gegevens zorgcliënt verwerkt in EPD andere zorgcliënt.

De Kritieke gebeurtenis/Risicobron is vanzelfsprekend, inherent. Een ziekenhuis is feitelijk een bedrijf met als hoofddoelstelling het genezen van zieke mensen die zich tot het ziekenhuis wenden. Daarbij voldoet het ziekenhuis als instelling aan bepaalde kwalificaties. Meer belangrijk is dat het ziekenhuis medisch specialisten aan zich weet te binden, in loondienst of vanuit een maatschap. In beide gevallen onderhouden deze medisch specialisten een medisch dossier per zorgcliënt op basis van een wettelijke plicht aan hun opgelegd en voor redenen van organisatorische efficiëntie wordt dat gedaan op een elektronische wijze waardoor heel veel met name logistieke efficiëntie kan worden bereikt. Het Risicobron/het Gevaar is daarom inherent aan het primaire proces.

Bedreigingen en Preventieve barrières

De Kritieke gebeurtenis kent een aantal Bedreigingen (Threats), welke niet limitatief zijn uitgewerkt aan de linkerhelft van het BowTie diagram in figuur 12:

- De zorgcliënt is niet uniek geïdentificeerd. Identificatie van de zorgcliënt bij diens eerste bezoek aan een medisch specialist is wettelijk verplicht. Identificatie geschiedt dan op basis van het BSN en dat BSN dient te worden vastgelegd in de basisgegevens van het EPD omdat deze gegevens bij iedere verwerking binnen het primaire proces Onderhouden EPD terugkomt. Daarbij zijn belangrijke controles (Barrières) om dit te voorkomen:
    - Het praktijksecretariaat controleert de gegevens van de zorgcliënt door deze te identificeren op basis van diens paspoort of ID. Dit moet wettelijk verplicht gebeuren voorafgaand aan het eerste consult bij de betreffende medisch specialist en kan zo nodig bij vervolgafspraken opnieuw gevraagd worden;
    - Het praktijksecretariaat controleert of het juiste medisch dossier van de zorgcliënt gekoppeld is aan de juiste set aan algemene gegevens omtrent de zorgcliënt. De koppeling is een verantwoordelijkheid van de systeembeheerders, de controle natuurlijk door het secretariaat;
- Direct voorafgaand aan een consult selecteert de arts of diens assistent het verkeerde EPD bij de zorgcliënt die hem bezoekt. Deze Bedreiging kan tot verstrekkende gevolgen leiden. Daarbij is de belangrijkste controle (Barrière) om dit te voorkomen:
    - Dat de praktijkassistente het juiste EPD opzoekt bij de zorgcliënt van de afspraak (BSN-nummer check algemene gegevens versus EPD), en dit dossier aanbiedt op het beeldscherm van de arts. De arts controleert vervolgens of hij inderdaad het juiste EPD voor zich heeft, bijvoorbeeld door herkenning van de zorgcliënt of door het stellen van enkele controlevragen;



figuur 12: BowTie diagram van Kritieke gebeurtenis 'Gegevens zorgcliënt verwerkt in EPD andere zorgcliënt' (gemaakt met BowTieXP)

- De relatie tussen de basisgegevens en het zorgdeel (EPD-deel) van de van de zorgcliënt in niet juist gekoppeld. Men kan beschouwen dat de algemene gegevens van zorgcliënten is één algemene zorgcliënten database zijn opgenomen. Ieder EPD (zorgdeel) van een zorgcliënt is echter een kleine database. Dit is van belang om aan wettelijke vereiste te voldoen van beveiliging maar ook vanuit gegevensbescherming. De NEN-7510, 7512 en 7513 stellen daartoe de vereisten. Daarbij zijn belangrijke controles (Barrières) om dit te voorkomen:

    - De koppeling tussen de algemene gegevens en de individuele EPD's van zorgcliënten is de verantwoordelijkheid van systeembeheer. Daarom zal dagelijks een integriteitscheck op die koppelingen moeten worden uitgevoerd door systeembeheer door het uitvoeren van een systeemcontrole;

- Het praktijksecretariaat controleert of het juiste medisch dossier van de zorgcliënt gekoppeld is aan de juiste set aan algemene gegevens omtrent de zorgcliënt;

- Verkeerd koppelen gehele dossier zorgcliënt. Dit betreft het geval als bepaalde deeldossiers in het EPD niet juist gekoppeld zijn. Bijvoorbeeld EPD-delen betreffende meerder specialisten en onderzoeksafdelingen. Daarbij zijn belangrijke controles (Barrières) om dit te voorkomen gelijk aan de controles beschreven in de vorige bedreiging;

- Een niet geautoriseerde zorgverlener heeft toegang tot een EPD. Andere zorgverleners dan de direct verantwoordelijke zorgverlener en verpleegkundigen hebben geen toegang tot het EPD van een zorgcliënt. Gebeurt dit wel, dan is er sprake van een datalek[15]. Echter, er zijn situaties denkbaar dat een andere zorgverlener of verpleegkundige direct inzage moet hebben in een EPD van een zorgcliënt, bijvoorbeeld op het moment dat die zorgverlener dienst heeft als Eerste Hulp en een zorgcliënt die wordt binnengebracht die niet in staat is toestemming voor die inzage te geven. Dan maakt die zorgverlener of verpleegkundige gebruik van de 'Breaking the Glass' procedure. Daarbij zijn belangrijke controles (Barrières) om dit te voorkomen:

  - De zorgverlener en verpleegkundige rapporteren dagelijks en met redenen omkleed waarom inzage is genomen in een EPD van een zorgcliënt. Deze Breaking the Glass rapportage wordt regulier beoordeeld door de FG;

  - De logfiles van wie toegang heeft gehad tot de EPD's worden geautomatiseerd gecontroleerd, waarbij ongeautoriseerde toegang direct wordt herkend. De controlerapportage wordt beheerd door controleurs van systeemcontrole die zo nodig escaleren omtrent de overtreding;

  - De verantwoordelijk zorgverlener krijgt rapport omtrent andere zorgverleners en verpleegkundigen die ongeautoriseerd toegang hebben gehad per EPD.

Consequenties en Herstel barrières

De Kritieke gebeurtenis kent een aantal negatieve gevolgen (Consequenties) welke kunnen voortvloeien uit de bedreigingen, welke niet limitatief zijn uitgewerkt aan de rechterhelft van het BowTie diagram in figuur 12:

- Arts trekt vereerde conclusies voor het vervolgtraject in de behandelingscyclus of geneeskundige behandelingsovereenkomst. Dit kan leiden tot het inzetten van verkeerde diagnostische behandelingen, voorschrijven van verkeerde medicijnen tot en met

15 https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-patiëntendossiers

operatieve verrichtingen uitvoeren die niet voor de betreffende zorgcliënt gelden. Dit kan daarom zelfs leiden tot levensbedreigende situaties. Daarbij zijn belangrijke controles (Barrières) om dit te voorkomen:

  - Dat de praktijkassistente het juiste EPD opzoekt bij de zorgcliënt van de afspraak (BSN-nummer check algemene gegevens versus EPD), en dit dossier aanbiedt op het beeldscherm van de arts;

  - De arts controleert vervolgens of hij inderdaad het juiste EPD voor zich heeft Professionele zelfcontrole), bijvoorbeeld door herkenning van de zorgcliënt of door het stellen van enkele controlevragen;

  - Het praktijksecretariaat controleert na het consult dat de door de arts vastgelegde gegevens en vervolgafspraken plausibel zijn in de context van de geneeskundige behandelingsovereenkomst. In de medische wereld is dit een essentiële controlestap;

- Iedere zorgcliënt beschikt over een "Mijn EPD". Daar zouden gevoelige persoonsgegevens in kunnen staan van een andere zorgcliënt. Dit zou een datalek betekenen. Daarbij zijn belangrijke controles (Barrières) om dit te voorkomen gelijk aan die uit het vorige beschreven gevolg;

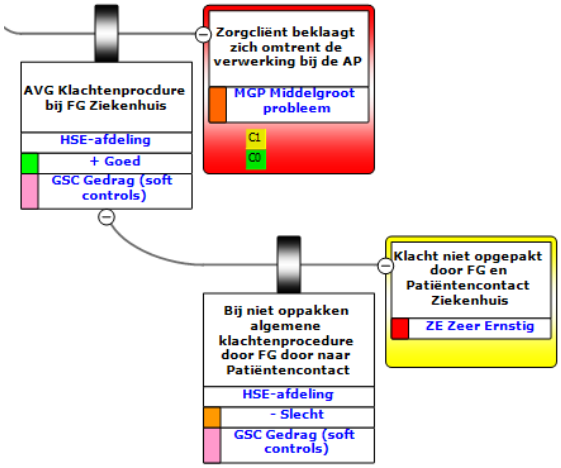
- Arts geeft de verkeerde medisch (bijzondere) persoonsgegevens door aan een andere zorgverlener voor bijvoorbeeld een diagnostisch onderzoek, second opinion of deelbehandeling. Dit kan tot ernstige problemen leiden. Daarbij zijn belangrijke controles (Barrières) om dit te voorkomen:

  - In geval van een doorverwijzing voorziet de wet (art 15a lid 3 Wabvpz[16]) dient de verwijzende arts daartoe toestemming te ontvangen van de zorgcliënt en te bespreken om welke reden hij die doorverwijzing wil doen. Daarbij houdt deze stap gelijk een professionele zelfcontrole in, mits zo uitgevoerd;

  - De ontvangende arts dient eveneens in geval van doorverwijzing toestemming van zijn (nieuwe) zorgcliënt te vragen of hij de ontvangen gegevens mag raadplegen (art 15b lid 1 Wabvpz). Ook voor deze arts geldt professionele zelfcontrole, door het stellen van enkele controlevragen, dat hij vaststelt de juiste gegevens van de juiste zorgcliënt voor zich te hebben;

[16] Wet Aanvullende Bepalingen Verwerking Persoonsgegevens in de Zorg

- De zorgcliënt heeft vastgesteld dat er in zijn “Mijn dossier” medische gegevens van een andere zorgcliënt zijn vastgelegd of dat de verkeerde medische gegevens aan een andere zorgverlener zijn doorgegeven. Dan is er sprake van een datalek. Als zijn zorgverlener of ziekenhuis hem daar niet over informeert, kan hij zich beklagen bij de AP. Daarbij zijn belangrijke controles (Barrières) om dit te voorkomen en hier tonen we gelijk een tweetraps controle barrière in:



  - Het ziekenhuis heeft een FG aangesteld. Zorgcliënt meldt zich met zijn klacht bij de FG. Mocht de FG nu niet ingaan op deze klacht, bestaat er een tweede vangnet,

  - Dat de klacht automatisch binnen enkele dagen wordt doorgezet naar Patiëntencontact. Patiëntencontact zou de klacht moeten opnemen, met de FG afstemmen en rapporteren naar het College van Bestuur. Immers een klacht kan naast schade aan het individu ook leiden tot (ernstige) schade aan het ziekenhuis;

  - Mocht ook Patiëntencontact de klacht niet oppakken, dan heeft de zorgcliënt inderdaad een escalatiemogelijkheid zijn klacht voor te leggen aan de AP. Het ziekenhuis kan dan een bezoek van de AP verwachten, met alle gevolgen van dien;

- Een zorgverlener heeft een ernstige fout gemaakt in een medische ingreep als gevolg van het verwisselen van medische gegevens van twee zorgcliënten. De zorgcliënt waarop de ernstige fout is begaan houdt hier blijvend letsel en klachten aan over. Deze zorgcliënt dient een formele klacht in bij het College van Bestuur van het ziekenhuis. Daarbij zijn belangrijke controles (Barrières) om dit te voorkomen:

  - Vanzelfsprekend alle drie de controle barrières genoemd in het eerste en tweede gevolg op de hiervoor:

    - Dat de praktijkassistente het juiste EPD opzoekt bij de zorgcliënt van de afspraak;

    - De arts controleert vervolgens of hij inderdaad het juiste EPD voor zich heeft;

    - Het praktijksecretariaat controleert na het consult dat de door de arts vastgelegde gegevens plausibel zijn;

- Daarnaast dient de postkamer, of welke afdeling ook maar berichtgeving ontvangt, bijvoorbeeld Patiëntencontact, geïnstrueerd zijn een dergelijke brief/bericht direct naar de afdeling Juridische Zaken te sturen voor een correcte afhandeling.

VII.2 DPIA: Wagenparkbeheer

Veel leasemaatschappijen bieden op telematica gebaseerde diensten aan de leasende organisatie. Met car telematics worden auto's verbonden met het internet. Hierdoor krijgt de wagenparkbeheerder van de leasende organisatie meer inzicht in brandstof-/energiekosten, rijgedrag, gereden routes en onderhoudsbehoefte van de auto. De leaserijders kunnen meestal makkelijk een logboek bijhouden van al hun autoritten (vaak benaderbaar via een app) wat handig is voor de belastingaangifte.

In de DPIA staat de gegevensverwerking van het wagenparkbeheer centraal en worden de volgende doeleinden onderkend:

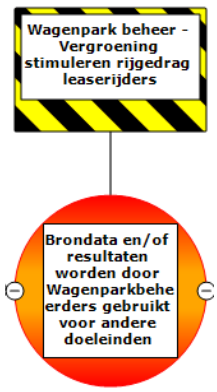
- Fiscaal sluitende ritregistratie (personenauto's)
- Real-time track en trace (bestelauto's ten behoeve bezorgdienst)
- Vergroening (stimuleren rijgedrag leaserijders)
- Vloot en wagenparkbeheer
- Managementinformatie

Risicobron/Gevaar

Omdat de doeleinden (en ook de grondslagen voor de gegevensverwerking) uit elkaar liggen wordt per combinatie gegevensverwerking/doeleinde een aparte Risicobron/Gevaar (Hazard) uitgewerkt. In dit voorbeeld is de Risicobron 'Wagenpark beheer – Vergroening stimuleren rijgedrag leaserijders'.

Kritieke gebeurtenis

Binnen de Risicobron 'Wagenpark beheer – Vergroening stimuleren rijgedrag leaserijders' kunnen meerdere Kritieke gebeurtenissen (Top Events) worden onderkend, te weten (niet limitatief):



- De brondata is niet juist en/of de resultaten worden verkeerd vastgesteld
- De brondata en/of resultaten worden door de wagenparkbeheerder voor andere doeleinden gebruikt
- Er vindt ongeautoriseerde toegang tot de brondata en/of de resultaten (hacking, datalek, et cetera)
- De brondata en/of resultaten worden gewijzigd (onopzettelijk of ongeautoriseerd)

- De brondata en/of resultaten worden verwijder (onopzettelijk of ongeautoriseerd

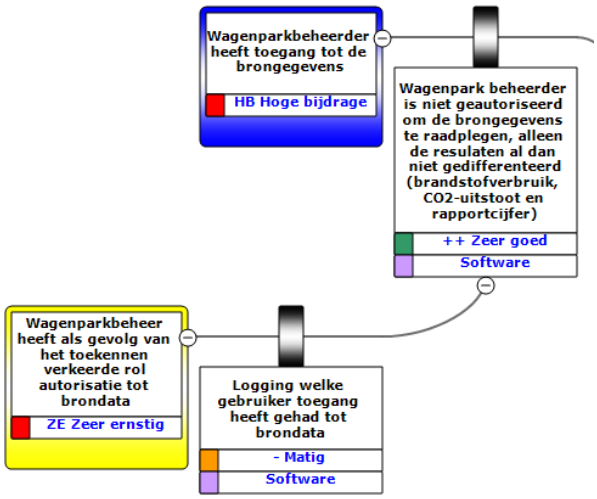
In dit voorbeeld is de Kritieke gebeurtenis 'De brondata en/of resultaten worden door de wagenparkbeheerder voor andere doeleinden gebruikt'. In BowTie staat de Kritieke gebeurtenis centraal.

Bedreigingen (Threats) en Preventieve barrières

De Kritieke gebeurtenis kent een aantal oorzaken (Bedreigingen) die niet limitatief zijn uitgewerkt aan de linkerhelft van het BowTie-diagram in figuur 13:

- 'Verwerkte persoonsgegevens zijn bovenmatig gegeven het doel'. Hoewel in het kader van de beoordeling van het proportionaliteits- en subsidiariteitsbeginsel al is vastgesteld of het doel niet met minder gegevens kan worden bereikt, kan de situatie zich voordoen dat er toch meer persoonsgegevens worden verwerkt dan noodzakelijk is voor het specifieke doel van de organisatie. Bijvoorbeeld, zoals in dit geval, er wordt gewerkt met een 'standaard' softwareoplossing. Bij de Bedreiging is de 'Bijdrage van de Bedreiging aan de Kritieke gebeurtenis' toegevoegd. In dit geval "Hoge bijdrage" Bij de Preventieve barrière 'Dataminimalisatie toepassen' zou dan bijvoorbeeld vastgesteld kunnen worden in hoeverre de te verzamelde gegevenssoorten flexibel is in te richten. Aan de Barrière is de verwachte Effectiviteit van de Barrière ('Zeer goed') de Barrière-type (Software) toegevoegd

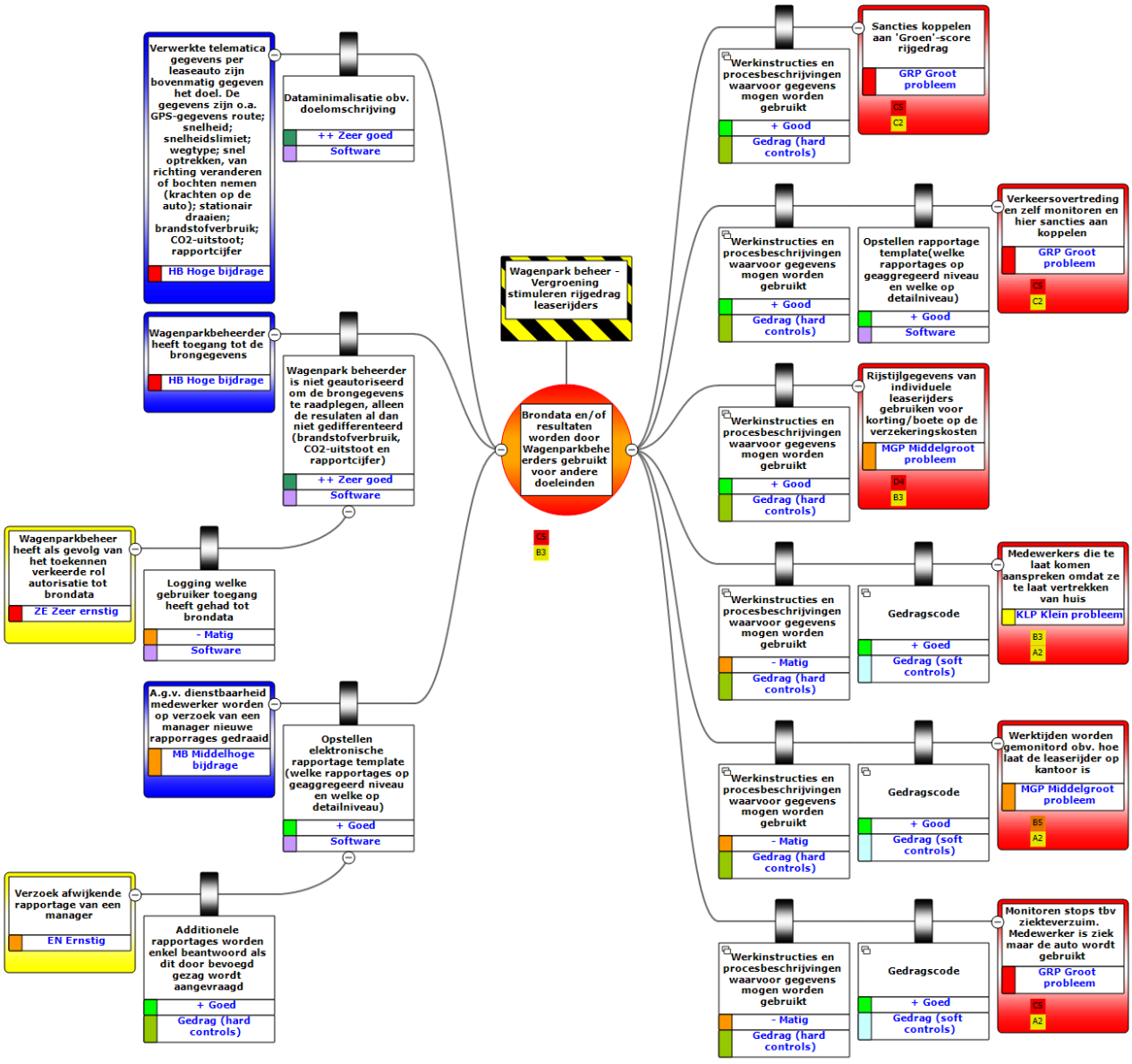
- Als de wagenpark beheerder toegang heeft tot de brondata. Door geen autorisatie toe te kennen tot de brondata (preventieve barrière) wordt voorkomen dat hij de brondata raadpleegt/queries er op gaat draaien die voor andere doeleinden kunnen worden gebruikt dan is beschreven.



- Nu kan het voorkomen dat de Wagenparkbeheerder per ongeluk de verkeerde rechten gekregen. De Escalatie factor zou dan zijn 'Wagenparkbeheerder heeft als gevolg van het toekennen verkeerde rol autorisatie brondata' en een mogelijke Escalatie factor beheersmaatregel zou kunnen zijn 'Logging welke gebruiker toegang heeft gehad tot de brondata'.

- 'Als gevolg van dienstbaarheid medewerkers worden op verzoek van een manager nieuwe rapportages gedraaid'. Indien de wagenparkbeheerders zich dienstbaar opstellen ten opzichte van de verschillende lijnmanagers die graag managementinformatie willen ontvangen over hun medewerkers bestaat het risico dat de telematica data voor andere doeleinden worden gebruikt dan is bedoeld. Een preventieve maatregel zou kunnen zijn

het bouwen van een set van elektronische rapportagetemplates die de lijnmanagers kunnen draaien/laten draaien door de wagenparkbeheerder.



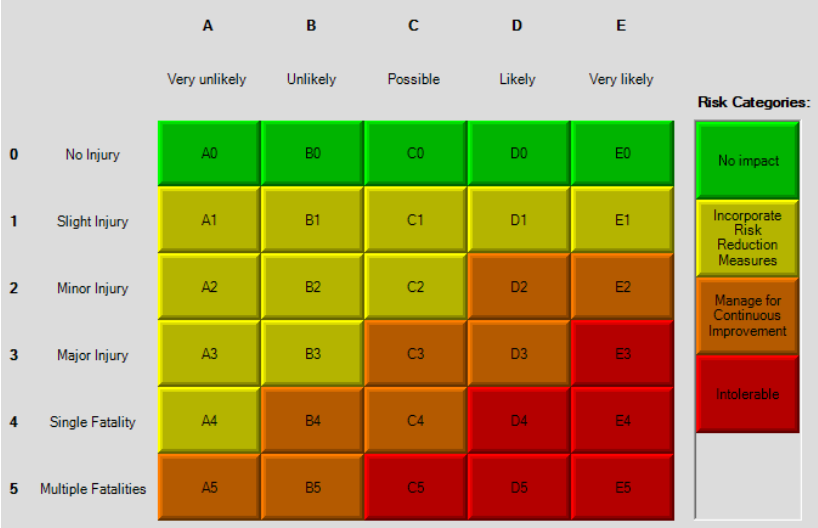
figuur 13 BowTie diagram van Rechtsbron/Kritieke gebeurtenis 'Wagenparkbeheer – Vergroening rijgedrag/Brondata en resultaten worden gebruikt voor andere doeleinden' (gemaakt met BowTieXP)

Consequenties (Consequences) en Herstel barrières

De Kritieke gebeurtenis kent een aantal negatieve gevolgen (Consequenties) die niet limitatief zijn uitgewerkt aan de rechterhelft van het BowTie diagram in figuur 13:

- 'Sancties koppelen aan 'groen'-score rijgedrag'. De gegevensverwerking is bedoeld om de vergroening van het rijgedrag van de leaserijders te stimuleren en niet te sanctioneren. Dit

negatieve gevolg wordt als een Groot probleem gezien (Consequentie-categorie). Het inherente risico van deze consequentie is ingeschat op C5 (op basis van een 5x5 risicomatrix, zie figuur 14)



figuur 14: Risicomatrix (bron BowTieXP)

- Als Herstel Barrière voor deze consequentie is opgenomen 'Werkinstructies en procesbeschrijvingen waarvoor gegevens mogen worden gebruikt'. De Effectiviteit van deze maatregel voor deze Consequentie wordt als 'Goed' ingeschat. De Barrière-type 'Gedrag (hard control). Het Restrisico wordt voor de Consequentie 'Sancties koppelen aan 'Groen'-score rijgedrag is ingeschat op C2.

- 'Verkeersovertredingen zelf monitoren en hier sancties aan koppelen' Op grond van de GPS-data is het mogelijk te zien hoe hard de berijder reed en hoe hard hij mocht rijden. Naast de eerdergenoemde Herstel barrière 'Werkinstructies…' is hier aanvullend een maatregel opgenomen om te werken met alleen rapportage templates die alleen op geaggregeerd niveau de resultaten weergeeft.

- 'Rijstijlgegevens van individuele leaserijders gebruiken voor korting/boete op de verzekeringskosten'. De Herstel barrière 'Werkinstructies…' wordt hier als voldoende geacht.

- Voor de Consequenties 'Medewerkers die te laat komen aanspreken omdat ze te laat vertrekken van thuis', 'Werktijden worden gemonitord o.b.v. hoe laat de leaserijder op kantoor is' en 'Monitoren stops t.b.v. ziekteverzuim. Medewerker is ziek maar auto wordt gebruikt' wordt minder heil gezien in de Herstel barrière 'Werkinstructie…' maar meer 'Gedragscodes (integriteit)'.