DPIA toelichting

Citeertitel	DPIA toelichting Westerwolde
Auteur(s)	5.1.2e
Datum	22-05-2025
Versie	1.0

Inhoudsopgave

1 Inleiding

Organisaties die persoonsgegevens verwerken, moeten voldoen aan de eisen van de Algemene Verordening Gegevensbescherming (AVG). De European Data Protection Board (EDPB) geeft richtlijnen uit over de interpretatie van kernbegrippen van de AVG. Volgens de EDPB is een Data Protection Impact Assessment (DPIA) een belangrijk instrument voor verantwoording. Het helpt niet alleen om aan de AVG-eisen te voldoen, maar ook om aan te tonen dat passende maatregelen zijn genomen om de naleving van de verordening te waarborgen. In het Nederlands wordt dit aangeduid als gegevensbeschermingseffectbeoordeling (GEB), maar in deze toelichting wordt de term DPIA gebruikt. Het uitvoeren van een DPIA is een proces om naleving te realiseren en aan te tonen.

1.1 Wat is een DPIA?

Een DPIA is een hulpmiddel om de gegevensverwerking te beschrijven, de rechtmatigheid te beoordelen, risico's vast te stellen en maatregelen te bepalen om mogelijke negatieve gevolgen tot een aanvaardbaar niveau te verminderen. Artikel 35 van de AVG richt zich op "risico's voor de rechten en vrijheden van natuurlijke personen" (de betrokkenen). Hoewel de nadruk in de praktijk vaak op organisatierisico's ligt, vloeien de negatieve gevolgen voor de organisatie voort uit inbreuken op de rechten van betrokkenen.

1.2 Waarom dient een DPIA uitgevoerd te worden?

Een DPIA stelt een organisatie in staat om privacyrisico's van projecten, beleid, programma's, diensten, producten, of andere manieren van gegevensverwerking op een gestructureerde en transparante manier vroegtijdig te identificeren. Door deze risico's in een vroeg stadium te begrijpen en erop te anticiperen, kunnen kostbare aanpassingen en juridische kosten worden vermeden. De DPIA-resultaten dienen als basis voor Privacy by Design & by Default. Het geeft inzicht in de negatieve gevolgen van privacyrisico's, helpt bij het bepalen van de risicobereidheid van de organisatie, vergroot het privacybewustzijn, verbetert de gegevensverwerking, en draagt bij aan het anticiperen op maatschappelijke privacyzorgen. Bovendien toont een DPIA de naleving aan van de AVG. De voorgestelde maatregelen in de DPIA worden gebruikt om een plan van aanpak op te stellen voordat gegevensverwerking begint. Bij uitbesteding kunnen deze maatregelen dienen als inkoopvereisten voor serviceproviders.

1.3 Wanneer is het verplicht om een DPIA uit te voeren?

De Algemene Verordening Gegevensbescherming (AVG) geeft aan wanneer het verplicht is om een DPIA uit te voeren, namelijk wanneer een gegevensverwerking waarschijnlijk een 'hoog' privacyrisico oplevert voor de betrokkenen.

Criteria zoals geautomatiseerde evaluatie van persoonlijke aspecten, grootschalige verwerking van bijzondere persoonsgegevens of strafrechtelijke gegevens, en grootschalige systematische monitoring in publiek toegankelijke gebieden vereisen een DPIA volgens artikel 35 lid 3 AVG.

De Autoriteit Persoonsgegevens heeft aanvullend op haar website een lijst van 17 verwerkingen, gebaseerd op de 9 criteria van de European Data Protection Board (hierna: EDPB), opgesteld waarvoor een DPIA verplicht is. Als een verwerking niet op de lijst staat, moet de organisatie zelf beoordelen of er een 'hoog' privacy risico is, met behulp van de 9 criteria van de EDPB.

Hoewel de AVG de DPIA-verplichtingen specificeert, is privacy risicomanagement belangrijk, ongeacht de wettelijke verplichtingen. Als een organisatie besluit geen DPIA uit te voeren, moet dit onderbouwd worden vastgelegd als onderdeel van de verantwoordingsplicht, mogelijk in het register van verwerkingsactiviteiten. Details over wie beslist over een DPIA, waar dit wordt vastgelegd, en of

de Functionaris Gegevensbescherming moet worden geraadpleegd, kunnen worden opgenomen in het privacy beleid of een apart DPIA-beleid.

1.4 Wanneer moet een DPIA uitgevoerd worden?

1.4.1 Nieuwe verwerkingen

Volgens de AVG is het verplicht om een DPIA uit te voeren voordat een organisatie start met een gegevensverwerking die mogelijk een hoog risico voor betrokkenen kan opleveren. Dit is niet alleen in overeenstemming met risicomanagementprincipes maar wordt ook aanbevolen door de Autoriteit Persoonsgegevens (AP), die adviseert om de DPIA zo vroeg mogelijk in de ontwerpfase te starten. Dit impliceert dat een organisatie al in de beginfase van het product- of dienstontwikkelingsproces met de DPIA begint. Tijdens de ontwikkeling van een dienst of product zijn meerdere risicoanalyses raadzaam, waar belangrijke privacy risico's worden besproken en strategische vragen worden beantwoord. De DPIA kan ook opgenomen worden als een 'deliverable' van de *businesscase*-fase en de resultaten ervan kunnen worden meegenomen in de *ontwikkeling*, in lijn met de principes van Privacy by Design en Privacy by Default. Oftewel, de DPIA loopt mee met de gehele ontwikkeling en past daar waar nodig de ontwikkelfase aan. Het uiteindelijke doel is om het product of de dienst (die persoonsgegevens verwerkt) uiteindelijk rechtmatig en zorgvuldig op te leveren. Tijdens *test- en validatiefasen* wordt geadviseerd de DPIA opnieuw uit te voeren om te waarborgen dat gekozen oplossingsrichtingen de geïdentificeerde privacy risico's hebben aangepakt. Het uitvoeren van een DPIA gedurende verschillende projectfasen moet een vast onderdeel zijn van het product- of projectontwikkelingsproces en wordt aanbevolen om op te nemen in het DPIA-beleid van de organisatie.

1.4.2 Bestaande verwerkingen

Volgens de AVG is het ook verplicht om voor bestaande gegevensverwerkingen, indien nog niet eerder gedaan, een DPIA uit te voeren. De organisatie dient de meest risicovolle gegevensverwerkingen als eerste te analyseren door een DPIA uit te voeren. Om dit te stroomlijnen, kan de organisatie het ingeschatte privacy risico van de bestaande verwerkingen (hoog/midden/laag) vastleggen in het Register van verwerkingsactiviteiten. Voor bestaande gegevensverwerkingen wordt geadviseerd, in lijn met het advies voor product-/projectontwikkeling, de DPIA als een vast onderdeel te integreren in het changemanagementproces.

1.4.3 Evaluatie van uitgevoerde DPIA's

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.

1.5 Wie voert de DPIA uit?

Een multidisciplinair team is bij voorkeur verantwoordelijk voor de uitvoering van een DPIA, gezien de diverse invalshoeken die privacy vereist. De betrokkenheid van verschillende teamleden, waaronder opdrachtgever, opdrachtnemer, experts op het gebied van projectmanagement, privacy, technologie, informatiebeveiliging, juridische zaken, organisatie, risicomanagement en data-analyse, verbetert de kwaliteit van de DPIA-resultaten. De IT-auditor kan als adviseur diverse rollen vervullen. Bij complexe gegevensverwerkingen is het raadzaam verwerkers of ketenpartners te betrekken. Conform de AVG is het wenselijk dat betrokkenen of hun vertegenwoordigers worden geraadpleegd tijdens het DPIA-proces, aangezien zij mogelijk andere privacy risico's identificeren of de impact ervan anders beoordelen.

Het is aan te raden dat de organisatie haar standpunt over het raadplegen van betrokkenen of hun vertegenwoordigers onderbouwt in het DPIA-beleid.

Als er een FG is aangesteld, wordt diens advies ook ingewonnen als onderdeel van het DPIA-proces, wat extra zekerheid biedt dat de DPIA de risico's adequaat in kaart brengt en er passende maatregelen worden genomen.

Als de DPIA aangeeft dat de te verwerken persoonsgegevens een hoog risico inhouden en er onvoldoende maatregelen zijn om dit risico te beperken, moet de organisatie de Autoriteit Persoonsgegevens vooraf raadplegen.

2 Toelichting concrete uitvoering

2.1 Beschrijven kenmerken gegevensverwerkingen

2.1.1 Voorstel/scope

Een Data Protection Impact Assessment (DPIA) is vereist vanwege potentiële risico's voor de rechten en vrijheden van betrokkenen bij de verwerking van persoonsgegevens. Het uitvoeren van een DPIA is ook noodzakelijk bij beleid en regelgeving die verband houden met persoonsgegevensverwerkingen. Het doel van de DPIA is het identificeren en verminderen van risico's, en het is essentieel om duidelijkheid te hebben over de specifieke gegevensverwerkingen die worden beoordeeld.

De scope van het DPIA-rapport moet beknopt en helder de gegevensverwerkingen beschrijven om misinterpretaties te voorkomen. Het is ook nuttig om expliciet aan te geven wat niet binnen de scope valt. Controlepunten voor de volledigheid van het voorstel omvatten de aanleiding, vervanging of vernieuwing van bestaande situaties, betrokken departementen en organisaties, Privacy by Design en Default, en de redenen achter de voorgestelde aanpak.

Privacy by Design impliceert dat privacy- en gegevensbescherming worden geïntegreerd in de ontwikkeling van nieuw beleid of gegevensverwerking, met minimale inbreuk op de privacy. Praktische maatregelen omvatten technologische status, uitvoeringskosten, de aard van de verwerking, en risico's voor betrokkenen.

Privacy by Default betekent dat alle instellingen en functies van nieuwe beleidsmaatregelen of verwerkingsprocessen standaard zijn ingesteld op de meest privacy vriendelijke opties. Voorbeelden zijn het beperken van cookies en het minimaliseren van vereiste gegevens bij e-mailadressen. Beide beginselen moeten worden overwogen bij openbare aanbestedingen volgens de AVG.

Bij conceptregelgeving kan aansluiting worden gezocht bij de inleidende paragraaf van de memorie of nota van toelichting die betrekking heeft op persoonsgegevensverwerking. Bij overheidsverwerking kan een beschrijving van de gegevensverwerkingen worden gebaseerd op het projectvoorstel of de architectuurbeschrijving.

2.1.2 Soorten persoonsgegevens

Betrokkenen zijn personen waarop de gegevens betrekking hebben binnen de gegevensverwerkingen. Dit omvat alle geïdentificeerde of identificeerbare natuurlijke personen over wie persoonsgegevens worden verwerkt. Dit kunnen onder andere medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers, en ingezetenen van een gemeente zijn.

Het voorstel kan verschillende effecten hebben op betrokkenen, afhankelijk van de categorie waartoe zij behoren. Sommige betrokkenen zijn kwetsbaarder dan anderen, waarbij kwetsbaarheid wordt gedefinieerd als een situatie waarin negatieve effecten van gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen. Voorbeelden van kwetsbare groepen zijn minderjarigen, ouderen, verstandelijk gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, medewerkers van inlichtingen- en veiligheidsdiensten, klokkenluiders of informanten van politie of justitie, asielzoekers, en etnische minderheden.

De Algemene Verordening Gegevensbescherming (AVG) biedt specifieke bescherming aan kinderen, met name bij het gebruik van persoonsgegevens voor marketingdoeleinden, het opstellen van persoonlijkheids- of gebruikersprofielen, en het verzamelen van persoonsgegevens bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. Voor kinderen jonger dan 16 jaar is de verwerking slechts rechtmatig als toestemming wordt verleend door de wettelijke vertegenwoordiger (ouder of voogd).

De **definitie van persoonsgegevens** omvat alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Voor identificatie wordt rekening gehouden met alle middelen die redelijkerwijs kunnen worden gebruikt om de persoon direct of indirect te identificeren, zoals naam, contactgegevens, demografische gegevens, apparaat- en internetgegevens, financiële gegevens, werk gerelateerde gegevens, en andere persoonsgegevens.

Pseudonimisering is het verwerken van persoonsgegevens op een manier dat ze niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder het gebruik van aanvullende gegevens (sleutels). Gepseudonimiseerde gegevens worden nog steeds beschouwd als persoonsgegevens, omdat ze met behulp van sleutels kunnen worden herleid tot een identificeerbare persoon.

Anonieme en geanonimiseerde gegevens worden niet beschouwd als persoonsgegevens. Anonimiseren als handeling valt echter wel onder privacywetgeving.

Gevoelige persoonsgegevens omvatten onder andere financiële gegevens, gegevens die tot stigmatisering of uitsluiting kunnen leiden, gegevens over kwetsbare groepen, gebruikersnamen, wachtwoorden, communicatie- en locatiegegevens.

Bijzondere persoonsgegevens, verboden om te verwerken zonder een uitzonderingsgrond, omvatten onder andere ras, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens, gezondheidsgegevens, gegevens over seksueel gedrag of seksuele gerichtheid. Beeldmateriaal kan bijzondere persoonsgegevens bevatten, maar het wordt als zodanig beschouwd wanneer het doel van de verwerking is om onderscheid te maken op basis van die bijzondere persoonsgegevens.

Strafrechtelijke persoonsgegevens omvatten informatie over strafrechtelijke veroordelingen en strafbare feiten, waarbij drie criteria relevant zijn: juridische kwalificatie van het strafbare feit, aard van het strafbare feit, en de zwaarte van de sanctie. Nationale identificatienummers mogen alleen worden verwerkt voor wettelijk bepaalde doeleinden.

De **herkomst** van persoonsgegevens moet worden vermeld, inclusief de organisatie, tool/platform, doeleinde van oorspronkelijke verzameling, en de grondslag voor verstrekking.

2.1.3 Gegevensverwerkingen

Om de rechtmatigheid van de gegevensverwerkingen te kunnen beoordelen, is het essentieel om een volledig overzicht te hebben van alle gegevensverwerkingen die vallen binnen de scope zoals uiteengezet in het voorstel. Het begrip 'verwerking van persoonsgegevens' omvat elke handeling of reeks handelingen met betrekking tot persoonsgegevens, waarbij elke handeling gerelateerd is aan het beheer van een persoonsgegeven.

Deze handelingen variëren van het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden, ter beschikking stellen, aligneren, combineren, afschermen, tot het wissen of vernietigen van gegevens. Met andere woorden, het omvat het gehele proces vanaf het moment van gegevensverzameling tot aan het moment van vernietiging.

Het wordt sterk aanbevolen om bij het beschrijven van gegevensverwerkingen een abstractieniveau te kiezen dat nauw aansluit bij de beschrijvingen in het register van verwerkingsactiviteiten. Dit bevordert een helder overzicht van de gegevensverwerkingen binnen de organisatie in relatie tot de beoordelingen in de Data Protection Impact Assessment (DPIA). Dit vergemakkelijkt ook de koppeling van het DPIA-rapport aan specifieke gegevensverwerkingen in het register van verwerkingsactiviteiten.

Gezien de complexiteit van de gegevensverwerkingen in het voorstel en de uitdaging om deze volledig in woorden uit te drukken, is het raadzaam om de gegevensverwerkingen te visualiseren met behulp van een stroomschema, input-proces-output model, of workflow. Zo'n stroomschema biedt in één oogopslag inzicht in het verloop van de gegevensverwerkingen, waardoor het gemakkelijker wordt het overzicht te behouden tijdens de DPIA. Het gebruikte stroomschema kan ook in de rest van de DPIA worden gerefereerd.

Voor een helder stroomschema is het van belang om:

- Alle betrokken partijen te benoemen, zodat duidelijk is welke partij verantwoordelijk is of deelneemt aan de betreffende gegevensverwerkingen, inclusief diens AVG-rol.
- Aan te geven over welke gegevensverwerkingen de DPIA specifiek gaat wanneer het stroomschema groter is dan de reikwijdte van de DPIA.
- Per gegevensverwerking te vermelden of specifieke applicaties, software, online platformen, of cloudopslag worden gebruikt, ter verhoging van de transparantie.

2.1.4 Technieken en methoden van de gegevensverwerkingen

Bepaalde technieken en methoden van gegevensverwerking, zoals (semi-)geautomatiseerde besluitvorming, profilering, en big data-verwerkingen, kunnen extra risico's met zich meebrengen en moeten daarom voldoen aan strengere regels en aanvullende maatregelen. Hierbij is het van belang informatie in te winnen bij diverse data-experts, waaronder de Chief Information Security Officer (CISO), de Information Security Officer (ISO), een data-analist, en een ICT-architect, om de technische complexiteit van gegevensverwerkingen beter te begrijpen.

Geautomatiseerde besluitvorming, met name besluiten die uitsluitend op geautomatiseerde verwerking zijn gebaseerd en significante gevolgen hebben voor betrokkenen, is in beginsel verboden. Er zijn echter uitzonderingen, zoals wanneer het besluit noodzakelijk is voor contractuele doeleinden, wettelijk is toegestaan, gebaseerd is op de uitdrukkelijke toestemming van de betrokkene, of passende waarborgen biedt.

Kunstmatige intelligentie (AI) en **algoritmen**, hoewel vaak door elkaar gebruikt, verschillen in wezen. AI omvat software die doelen kan bereiken door het genereren van resultaten op basis van menselijk gedefinieerde doelstellingen, terwijl algoritmen een reeks instructies zijn. AI, vooral machine learning-algoritmen, kan leren via verschillende methoden zoals supervised, unsupervised, en reinforcement learning. Bij gebruik van AI of algoritmen is het essentieel om zorgvuldig te testen en onbevooroordeelde trainingsdata te gebruiken om discriminatie te voorkomen.

Bij **cloudoplossingen**, het inzetten van servers via een groot netwerk voor gegevensopslag en -beheer, moeten specifieke aandachtspunten worden overwogen, waaronder dataclassificatie, anonimisering, verantwoordelijkheid van de cloudaanbieder, doelbinding, afhankelijkheid, en beoordeling van nieuwe gegevensverwerkingen.

Profilering, geautomatiseerde evaluatie van persoonsgegevens voor het analyseren of voorspellen van persoonlijke aspecten, en big data-analyses brengen specifieke risico's met zich mee. Profilering die leidt tot discriminatie op basis van bijzondere persoonsgegevens is verboden volgens de Richtlijn.

Big data-analyses zoeken naar correlaties tussen grote hoeveelheden gestructureerde en ongestructureerde data en vereisen specifieke maatregelen.

Nieuwe technologieën, waaronder intelligente volgsystemen, biometrie, gezondheidsmonitoring via wearables, zelfrijdende voertuigen, en internet of things-toepassingen, kunnen aanzienlijke gevolgen hebben voor privacy en moeten worden beoordeeld als nieuwe technologieën in het kader van gegevensbescherming.

2.1.5 Verwerkingsdoeleinden

De privacyregelgeving legt als basisprincipe vast dat persoonsgegevens uitsluitend mogen worden verzameld voor welbepaalde, duidelijk omschreven en gerechtvaardigde doeleinden. Het vaststellen van deze verwerkingsdoeleinden is een cruciale voorwaarde om de rechtmatigheid van de gegevensverwerkingen te beoordelen en om passende maatregelen te identificeren ter preventie of vermindering van risico's.

Het wordt sterk aanbevolen om per gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk te beschrijven, bij voorkeur met behulp van de voorgestelde voorbeeldtabel. Deze tabel maakt het mogelijk om voor elke categorie persoonsgegevens aan te geven wat het beoogde verwerkingsdoel is.

In gevallen waarin persoonsgegevens oorspronkelijk zijn verzameld voor een ander doeleinde, biedt de mogelijkheid om zowel het oorspronkelijke als het huidige (nieuwe) doel van de verwerking aan te geven belangrijke transparantie. Hierbij moet worden onderbouwd waarom de persoonsgegevens voor het nieuwe doeleinde mogen worden verwerkt.

Verwerkingsdoeleinden kunnen diverse aspecten omvatten, zoals het beveiligen van gebouwen en objecten, personeelszaken behandelen, strafbare feiten opsporen, direct marketing, vorderingen innen, leveringen en bestellingen doen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Neem ook eventuele nevendoelen in overweging, zoals wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratie- en rapportagedoeleinden, verbetering van dienstverlening, of beleidsontwikkeling.

Om de verwerkingsdoeleinden nauwkeurig af te stemmen op de geïdentificeerde gegevensverwerkingen, is het raadzaam om het algemene overkoepelende doel te gebruiken als basis, waaraan verschillende specifieke subdoelen kunnen worden opgehangen. Bijvoorbeeld:

- E-mailadres: noodzakelijk voor communicatie met de betrokkene.
- IP-adres: noodzakelijk ter verificatie van de locatie van waaruit het systeem wordt benaderd.
- Adresgegevens: noodzakelijk om een beschikking naar de betrokkene te kunnen sturen.
- Financiële gegevens: noodzakelijk om vast te stellen of de betrokken partij in aanmerking komt voor een toeslag.
- Strafrechtelijke gegevens: noodzakelijk voor het uitvoeren van een screening.

In het geval van conceptregelgeving is het wenselijk het doel van de gegevensverwerking bij voorkeur in de regeling zelf vast te leggen of op zijn minst te benoemen in de memorie of nota van toelichting. Dit bevordert de rechtszekerheid door een nadere invulling te geven aan het beoordelingskader.

Bij overheidsverwerkingen ter uitvoering van regelgeving is het cruciaal om binnen de publieke taak te blijven die in de regelgeving is vastgesteld. Het koppelen van de verwerkingsdoeleinden aan de gegevensverwerkingen (punt 3) draagt bij aan een heldere weergave van de verwerkingsdoeleinden.

2.1.6 Betrokken partijen

Om de rechtmatigheid van gegevensverwerkingen te beoordelen, is het essentieel inzicht te hebben in welke organisaties (functioneel) betrokken zijn bij welke gegevensverwerking en in welke rol: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub-verwerker, verstrekker of ontvanger. Het is belangrijk op te merken dat een organisatie of partij meerdere AVG-rollen tegelijk kan vervullen, zoals een verwerkingsverantwoordelijke die tegelijkertijd een verstrekker kan zijn.

Verwerkingsverantwoordelijke: De verwerkingsverantwoordelijke is de entiteit die het doel en de middelen van de gegevensverwerking bepaalt. Dit kan een natuurlijke persoon, rechtspersoon of overheidsorgaan zijn, en deze rol kan ook worden vastgesteld in Unie- of lidstatelijk recht. In wezen is het de persoon of organisatie die formeel bevoegd is om te beslissen of, waarom, en hoe persoonsgegevens worden verwerkt.

Gezamenlijke verwerkingsverantwoordelijke: Als twee of meer verwerkingsverantwoordelijken samen de doelen en middelen van de verwerking bepalen, worden ze beschouwd als gezamenlijke verwerkingsverantwoordelijken. Het is van belang dat ze onderling vastleggen wie verantwoordelijk is voor welk aspect en aansprakelijkheid dragen. Een cruciaal criterium hierbij is of het proces kan doorgaan zonder de samenwerking tussen de betrokken organisaties.

Verwerker: De verwerker is de entiteit die persoonsgegevens verwerkt voor de verwerkingsverantwoordelijke, handelend volgens diens instructies. Dit kan een natuurlijke persoon, rechtspersoon of overheidsorgaan zijn, maar het is altijd een entiteit buiten de organisatie van de verwerkingsverantwoordelijke. Schriftelijke afspraken tussen de verwerkingsverantwoordelijke en de verwerker zijn essentieel, en naast formele taakverdeling moet ook worden gekeken naar de feitelijke omstandigheden.

Sub-verwerker: De sub-verwerker voert specifieke taken uit voor de verwerker in het kader van samenwerking tussen de verwerker en de verwerkingsverantwoordelijke. Er moeten schriftelijke afspraken zijn tussen de verwerker en de sub-verwerker, waarbij de privacyverplichtingen op zijn minst hetzelfde strenge niveau moeten hebben als tussen de verwerkingsverantwoordelijke en de verwerker.

Ontvanger: De ontvanger is de entiteit aan wie de persoonsgegevens worden verstrekt.

Verstrekker: De verstrekker is de entiteit die de persoonsgegevens verstrekt aan een andere partij.

Derde: Een derde is een entiteit die geen betrokkene, verwerkingsverantwoordelijke, verwerker, of een persoon onder gezag van de verwerkingsverantwoordelijke of verwerker is, maar wel betrokken is bij de gegevensverwerking. Bijvoorbeeld, op basis van het gerechtvaardigd belang van een derde kan een verwerkingsverantwoordelijke gegevens verwerken met betrekking tot de belangen van deze derde.

Betrokkene: De natuurlijke persoon wiens gegevens worden verwerkt.

In gevallen waarin wettelijk niet is voorgeschreven wie de verwerkingsverantwoordelijke is of welke criteria hiervoor gelden, moeten betrokken organisaties onderling bepalen wie welke rol vervult en wie toegang heeft tot welke persoonsgegevens, rekening houdend met autorisatiematrix en de doeleinden van de gegevensverwerking.

2.1.7 Toepasselijke normen

Voor gemeenten en organisaties die persoonsgegevens verwerken zijn er specifieke normen die van toepassing zijn op informatiebeveiliging en gegevensbescherming, hieronder een paar voorbeelden:

De BIO biedt richtlijnen, maatregelen en beveiligingsstandaarden die overheidsorganisaties kunnen implementeren om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen. Het stelt een set van minimale eisen en maatregelen op die overheidsinstanties dienen te implementeren om hun informatiebeveiligingsniveau te verhogen.

De norm behandelt verschillende aspecten van informatiebeveiliging, zoals toegangscontrole, risicomanagement, incidentrespons, beveiligingsbeleid, bewustwordingstraining en continuïteitsplanning. Het doel is om een solide basis te bieden voor de bescherming van gevoelige informatie en om de weerbaarheid van overheidsinstanties tegen cyberdreigingen te versterken.

De BIO is niet alleen gericht op centrale overheidsorganisaties, maar is ook van toepassing op decentrale overheden en andere publieke instellingen in Nederland. Het naleven van de BIO-normen helpt bij het creëren van een consistente en robuuste benadering van informatiebeveiliging binnen de gehele Nederlandse overheid.

2.1.8 Juridisch en beleidsmatig kader

Voor een gestructureerd overzicht van de wet- en regelgeving die van toepassing is op het verwerkingsproces, wordt geadviseerd om hiërarchisch te werk te gaan. Dit kan bijvoorbeeld in de volgende volgorde:

- Internationale verdragen
- Europese verdragen, verordeningen, richtlijnen en besluiten
- Nationale wetgeving
- AMvB's, gemeentelijke verordeningen, algemeen verbindende voorschriften
- Intern beleid

Naast de Algemene Verordening Gegevensbescherming (AVG) en de Richtlijn kunnen (sectorale) wetten en regels de mogelijkheden voor gegevensverwerking creëren, conditioneren of beperken. Enkele voorbeelden hiervan zijn:

- Wet algemene bepalingen burgerservicenummer
- Wet gebruik burgerservicenummer in de zorg
- Wet basisregistratie personen
- Algemene wet inzake rijksbelastingen
- Archiefwet
- Telecommunicatiewet
- Kadasterwet
- Handelsregisterwet 2007
- Kieswet
- Wet bijzondere maatregelen grootstedelijke problematiek
- Wet op de geneeskundige behandelingsovereenkomst
- Omgevingswet
- Jeugdwet
- Wet maatschappelijke ondersteuning 2015
- Participatiewet

Daarnaast kan departementaal of Rijksbreed beleid specifieke beperkingen of voorwaarden opleggen aan gegevensverwerkingen, met name met betrekking tot opslag en beveiliging van persoonsgegevens. Deze inventarisatie vormt de basis voor de beoordeling van de rechtmatigheid van gegevensverwerkingen en de voorschrijving van specifieke maatregelen.

2.1.9 Bewaartermijnen

De privacyregelgeving stelt als principe dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk voor het verwezenlijken van de verwerkingsdoeleinden. Als persoonsgegevens niet meer nodig zijn voor deze doeleinden, dienen ze te worden vernietigd of geanonimiseerd. Een uitzondering op dit opslagbeperkingsbeginsel geldt wanneer persoonsgegevens uitsluitend worden verwerkt voor archiveringsdoeleinden in het algemeen belang, wetenschappelijk of historisch onderzoek, of statistische doeleinden. In dit geval moeten passende maatregelen worden genomen ter bescherming van de betrokkenen.

De Archiefwet speelt een belangrijke rol in dit kader, waarbij niet alle persoonsgegevens in alle documenten van gegevensverwerkingen vernietigd of geanonimiseerd hoeven te worden. Sommige gegevens moeten worden gearchiveerd volgens de Archiefwet, wat essentieel is voor publieke verantwoording, rechtsvinding en culturele en historische overwegingen. Specifieke regels zijn vastgelegd in de Archiefwet, het Archiefbesluit, en de Archiefregeling.

De relatie tussen de bewaartermijn volgens de AVG en archivering is cruciaal. Als een document geen persoonsgegevens bevat of als deze geanonimiseerd zijn, valt het buiten het bewaartermijnregime van de AVG. Wanneer documenten wel persoonsgegevens bevatten, moet een bewaartermijn worden bepaald op basis van het oorspronkelijke doel van de gegevensverzameling en -verwerking. Na afloop van de bewaartermijn wordt archivering het nieuwe doel van de gegevensverwerking.

Het vaststellen van bewaartermijnen vereist aandacht voor specifieke persoonsgegevens en gegevensverwerkingen. Na de bewaartermijn kunnen documenten ofwel worden vernietigd/geanonimiseerd, ofwel worden gearchiveerd, afhankelijk van de toepasselijkheid van de Archiefwet, het Archiefbesluit, en/of de Archiefregeling.

Concrete stappen omvatten het nagaan van bestaande wettelijke of beleidsmatige bewaartermijnen, het bepalen van de duur van de bewaartermijn, het identificeren van handelingen na de bewaartermijn, en het controleren van de toepasselijkheid van archiveringsregelgeving.

Voorbeelden van specifieke bewaartermijnen zijn onder meer:

- Twee jaar na het einde van een arbeidsovereenkomst worden sollicitatiegegevens vernietigd.
- Vier weken na het beëindigen van een sollicitatieprocedure worden sollicitatiegegevens van afgewezen kandidaten vernietigd.
- Een jaar na de afronding van een evenement worden persoonsgegevens vernietigd.
- Een jaar na het laatste inlogmoment worden inloggegevens geanonimiseerd.
- Een jaar na de publicatie van een onderzoeksrapport worden ruwe onderzoeksgegevens gepseudonimiseerd en gearchiveerd voor 10 jaar, waarna ze geanonimiseerd en gepubliceerd worden via een open science platform.
- Twintig jaar na het verlenen van een bouwvergunning worden persoonsgegevens en bijbehorende documenten naar de regionale archiefdienst gebracht voor archivering.

Door de gemeente Westerwolde zijn de bewaartermijnen vastgelegd in de gemeentelijke selectielijst van de VNG. De bewaartermijnen zijn afhankelijk van de wet op grond waarvan de gegevens worden verwerkt.

2.1.10 Verwerkingslocaties

De fysieke locaties waar gegevensverwerkingen plaatsvinden, kunnen extra risico's met zich meebrengen en vereisen mogelijk strengere regels en aanvullende maatregelen. Deze locaties hebben ook invloed op de bevoegdheid van de (leidende) privacytoezichthouder.

Alle locaties waar persoonsgegevens worden verwerkt binnen de beoordeelde gegevensverwerkingen in deze DPIA, inclusief niet alleen de opslag maar ook waar gegevens worden geopend, gestreamd of tijdelijk opgeslagen, worden hierbij betrokken.

Om te voorkomen dat regels voor gegevensbescherming worden omzeild door gegevens in een ander land te verwerken, schrijven de AVG en de Richtlijn voor dat gegevensverwerkingen buiten de Europese Economische Ruimte (EER) alleen onder bepaalde voorwaarden zijn toegestaan. Dit geldt bijvoorbeeld wanneer er gebruik wordt gemaakt van een specifiek doorgiftemechanisme, zoals een adequaatheidsbesluit van de Europese Commissie, modelcontractbepalingen (SCC's), gedragscodes, of bindende bedrijfsvoorschriften (BCR's).

Naast deze algemene regels zijn er specifieke situaties waarin gegevensverwerking in een derde land toch kan plaatsvinden zonder passend beschermingsniveau en waarborgen. Dit kan bijvoorbeeld gelden bij uitdrukkelijke toestemming van de betrokkene, noodzaak vanwege gewichtige redenen van algemeen belang, of noodzaak voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Het is belangrijk op te merken dat naast de AVG en de Richtlijn ook andere wettelijke regels of beleidsmaatregelen de locaties waar persoonsgegevens worden verwerkt kunnen beïnvloeden, zoals het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) met betrekking tot gerubriceerde overheidsinformatie en situaties waarin opslag in een overheidsdatacenter passend is.

2.2 Beoordeling rechtmatigheid gegevensverwerkingen

2.2.1 Rechtsgrond

De Algemene Verordening Gegevensbescherming (AVG) stelt als beginsel dat persoonsgegevens rechtmatig, behoorlijk en transparant moeten worden verwerkt. Om dit te waarborgen, moeten gegevensverwerkingen gebaseerd zijn op een van de zes rechtsgronden:

a. Toestemming van de betrokkene.
b. Noodzakelijkheid voor de uitvoering van een overeenkomst met de betrokkene of precontractuele maatregelen op verzoek van de betrokkene.
c. Noodzakelijkheid om te voldoen aan een wettelijke verplichting.
d. Noodzakelijkheid voor de bescherming van vitale belangen van de betrokkene of anderen.
e. Noodzakelijkheid voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
f. Noodzakelijkheid voor de behartiging van gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde, behalve wanneer belangen of grondrechten van de betrokkene zwaarder wegen.

De beoordeling van de noodzaak van gegevensverwerkingen wordt gedaan in de DPIA. Binnen de DPIA kunnen verschillende verwerkingen verschillende juridische of uitzonderingsgronden hebben. Bijvoorbeeld, de verwerking van persoonsgegevens in een sollicitatieprocedure kan oorspronkelijk gebaseerd zijn op 'toestemming' of 'noodzakelijk voor de uitvoering van een overeenkomst'. Als een arbeidsovereenkomst wordt aangeboden, wordt de verwerking van persoonsgegevens gerechtvaardigd door 'wettelijke verplichting'.

Ondanks overlappende persoonsgegevens wordt aangeraden om verschillende gegevensverwerkingen te onderscheiden, zodat duidelijk is welke rechtsgrond van toepassing is. Bij wettelijke plicht (c) en taak van algemeen belang (e) moet de basis in Unie- of lidstaatrecht worden vastgesteld. Een wettelijke plicht kan breder zijn dan expliciete verplichting, en de taak van algemeen belang moet blijken uit geldende regelgeving voor de verwerkingsverantwoordelijke.

De rechtsgrond 'gerechtvaardigde belangen' (f) is niet van toepassing op overheidsorganen voor gegevensverwerkingen in hun publieke taak. Overheidsorganen kunnen deze grond alleen gebruiken voor taken die niet wezenlijk verschillen van private organisaties. Belangenafweging is verplicht bij deze grond en wordt aanbevolen om op te nemen in de DPIA.

Bij conceptregelgeving kan de keuze van de rechtsgrond gevolgen hebben. Overheidsorganen moeten zich baseren op een van de zes rechtsgronden, en 'gerechtvaardigd belang' is niet geldig voor

publieke taken. Toestemming is vaak niet geschikt vanwege hiërarchische verhoudingen bij overheidsorganen.

2.2.2 Doelbinding

De privacyregelgeving stelt als principe dat persoonsgegevens alleen mogen worden verzameld voor welbepaalde, duidelijk omschreven en gerechtvaardigde doeleinden, en dat verdere verwerking niet mag plaatsvinden op een manier die onverenigbaar is met die oorspronkelijke doeleinden.

Volgens de AVG is verdere verwerking voor een ander, niet-verenigbaar doel alleen toegestaan onder specifieke voorwaarden. Dit omvat toestemming van de betrokkene, Unierechtelijke of lidstaatrechtelijke bepalingen, noodzakelijke en evenredige maatregelen in een democratische samenleving ter waarborging van een belangrijke doelstelling van algemeen belang, en verwerking ten behoeve van archivering, wetenschappelijk of historisch onderzoek, of statistische doeleinden, met passende beschermingsmaatregelen voor de betrokkenen.

Bij de beoordeling van de verenigbaarheid van verdere verwerking moeten verschillende aspecten worden overwogen, zoals het verband tussen het oorspronkelijke en nieuwe doel, de context van gegevensverzameling, het type persoonsgegevens, de mogelijke gevolgen van de verdere verwerking en het bestaan van passende waarborgen.

Bij overheidsverwerkingen moet de verwerkingsverantwoordelijke dezelfde beoordeling uitvoeren en tevens controleren of sectorwetgeving geheimhoudingsplichten of verboden op verdere verwerking bevat.

Bij conceptregelgeving moet worden beoordeeld of het noodzakelijk is wettelijk te regelen dat verdere verwerking is toegestaan, vooral in verband met het doorbreken van geheimhoudingsplichten.

Binnen dit kader is er ruimte voor een wettelijke regeling waarmee persoonsgegevenssets van verschillende partijen en domeinen worden gecombineerd voor big data-analyses, zolang het doel van deze analyse in de wet is vastgesteld. Het benadrukt echter dat de verwerkingsverantwoordelijke die beslissingen neemt op basis van deze analyses moet voldoen aan alle eisen voor rechtmatige gegevensverwerking en een eigen rechtsgrond moet hebben.

2.2.3 Bijzondere persoonsgegevens

De Algemene Verordening Gegevensbescherming (AVG) verbiedt over het algemeen de verwerking van bijzondere persoonsgegevens, behalve in bepaalde uitzonderlijke situaties. De relevante uitzonderingen zijn als volgt:

a. Toestemming van de betrokkene.
b. Noodzakelijk voor de uitvoering van verplichtingen en uitoefening van specifieke rechten op het gebied van arbeids- en socialezekerheidsrecht, volgens Unie- of lidstatelijke wetgeving.
c. Noodzakelijk ter bescherming van vitale belangen van de betrokkenen of anderen.
d. Uitgevoerd door een instantie op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied.
e. Betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt.
f. Noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

g. Noodzakelijk om redenen van zwaarwegend algemeen belang, volgens Unie- of lidstatelijke wetgeving.
h. Noodzakelijk voor preventieve en arbeidsgeneeskunde, beoordeling van arbeidsgeschiktheid, medische diagnosen, gezondheidszorg of sociale diensten, op basis van Unie- of lidstatelijke wetgeving.
i. Noodzakelijk voor redenen van algemeen belang op het gebied van volksgezondheid, volgens Unie- of lidstatelijke wetgeving.
j. Noodzakelijk voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, volgens Unie- of lidstatelijke wetgeving.

Het is essentieel om artikel 9, lid 2 van de AVG te raadplegen voor de volledige tekst van deze uitzonderingen, en aanvullende uitzonderingen kunnen tevens in nationale wetgeving worden gevonden. De AVG staat de verwerking van strafrechtelijke gegevens alleen toe onder overheidstoezicht of bij wettelijke regeling. Verwerking van nationale identificatienummers is alleen toegestaan voor wettelijk bepaalde doeleinden.

De Richtlijn schrijft voor dat verwerking van bijzondere persoonsgegevens alleen is toegestaan als deze strikt noodzakelijk is en geschiedt met passende waarborgen voor de rechten en vrijheden van de betrokkene, en onder de voorwaarden dat het wettelijk is toegestaan, noodzakelijk is voor vitale belangen, of betrekking heeft op openbaar gemaakte gegevens.

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

2.2.4 Noodzaak en evenredigheid

De privacyregelgeving stelt als beginsel dat gegevensverwerking beperkt moet blijven tot wat noodzakelijk is voor de verwerkingsdoeleinden, zoals aangegeven in de AVG en Richtlijn. Dit principe van minimale gegevensverwerking (dataminimalisatie) vereist dat de verwerking noodzakelijk is voor het bereiken van de doelen en dat deze voldoet aan de principes van proportionaliteit en subsidiariteit.

Proportionaliteit betekent dat moet worden beoordeeld of de indringendheid van de gegevensverwerking in een redelijke verhouding staat tot het doel. Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen (zijn de beperkingen van het grondrecht en het doel dat met de verwerking wordt beoogd met elkaar in balans?). Daarbij zal onder meer moeten worden gekeken of de gegevensverwerking effectief is om het beoogde doel te bereiken en of de aangevoerde redenen relevant en toereikend zijn om het beoogde doel te bereiken. Daarbij kunnen empirische onderzoeksresultaten helpen.

Ter beoordeling van de proportionaliteit kunnen de volgende vragen worden gesteld:

- Staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
- Is de gegevensverwerking van persoonsgegevens te verwachten en voorzienbaar voor de betrokkenen?
- Hoe groot is het belang om de verwerkingsdoeleinden te bewerkstelligen?

- Is de gegevensverwerking het meest effectieve middel om het doeleinde te bereiken?

Bij **subsidiariteit** wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt (bijvoorbeeld: kan bij het gebruik van bijzondere of strafrechtelijke persoonsgegevens hetzelfde resultaat behaald worden met gebruikmaking van een combinatie van gewone persoonsgegevens?). Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht in onderdeel A betrokken.

Ter beoordeling van de subsidiariteit kunnen de volgende vragen worden gesteld:

1. Kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?
    1. Kunnen minder persoonsgegevens worden verwerkt en hetzelfde doeleinde worden bereikt?
    2. Zijn er wellicht manieren om minder gevoelige persoonsgegevens te verwerken?
    3. Kunnen de persoonsgegevens in het proces gepseudonimiseerd of geanonimiseerd worden?
    4. Kunnen de persoonsgegevens met minder partijen worden gedeeld of minder lang worden bewaard?
2. Zijn er alternatieve minder privacy invasieve verwerkingsprocessen onderzocht en gedocumenteerd?
    1. Welke alternatieven zijn overwogen en waarom zijn deze alternatieven niet gekozen?
    2. Zijn alternatieven overwogen die hetzelfde doeleinde kunnen bereiken met minder persoonsgegevens?
    3. Zijn alternatieven overwogen waarbij de gehele dienst binnen Nederland of de EU uitgevoerd kan worden?
    4. Zijn alternatieven overwogen waarbij de verwerker geen gebruikmaakt van sub-verwerkers buiten de EU?

Bij conceptregelgeving is het belangrijk de uitkomsten van deze afwegingen mee te nemen in de grondrechtentoets van het Integraal Afwegingskader voor beleid en regelgeving (IAK).

2.2.5 Rechten van betrokkenen

De AVG verleent betrokkenen verschillende rechten met betrekking tot de verwerking van hun persoonsgegevens. Het is essentieel om de naleving van deze privacy rechten bij gegevensverwerkingen vast te stellen en de procedure voor betrokkenen om hun rechten uit te oefenen te beschrijven. De privacy rechten zijn:

1. **Recht op informatie:** Betrokkenen hebben recht op duidelijke en transparante informatie over de verwerking van hun persoonsgegevens.
2. **Recht van inzage:** Betrokkenen hebben het recht om te weten of hun persoonsgegevens worden verwerkt en, indien dit het geval is, toegang tot die gegevens te krijgen.
3. **Recht op rectificatie:** Betrokkenen hebben het recht om onjuiste persoonsgegevens te laten corrigeren en om eventuele onvolledige gegevens aan te vullen.
4. **Recht op gegevenswissing:** Ook bekend als het 'recht om vergeten te worden', betrokkenen hebben het recht om persoonsgegevens te laten wissen onder bepaalde omstandigheden.
5. **Recht op beperking van de verwerking:** Betrokkenen kunnen onder bepaalde omstandigheden vragen om de verwerking van hun persoonsgegevens te beperken.

6. **Kennisgevingsplicht bij rectificatie of wissing:** Als persoonsgegevens zijn gecorrigeerd of gewist, moet de verwerkingsverantwoordelijke de betrokkene hiervan op de hoogte stellen.
7. **Recht op overdraagbaarheid van gegevens:** Betrokkenen hebben het recht om hun persoonsgegevens te ontvangen in een gestructureerd, veelgebruikt en machineleesbaar formaat.
8. **Recht van bezwaar:** Betrokkenen kunnen bezwaar maken tegen de verwerking van hun persoonsgegevens, met name als deze wordt uitgevoerd op basis van gerechtvaardigde belangen.
9. **Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming:** Betrokkenen hebben het recht om niet onderworpen te worden aan besluiten die uitsluitend gebaseerd zijn op geautomatiseerde verwerking.

Uitzonderingen op deze rechten zijn mogelijk, maar moeten voldoen aan specifieke voorwaarden zoals beschreven in de privacyregelgeving. In gevallen van gezamenlijke verwerkingsverantwoordelijkheid moeten duidelijke afspraken worden gemaakt over wie verantwoordelijk is voor het faciliteren van de uitoefening van deze rechten.

Wanneer conceptregelgeving uitzonderingen op deze rechten introduceert, moeten specifieke bepalingen worden opgenomen, zoals de doeleinden van de verwerking, de categorieën van persoonsgegevens, waarborgen tegen misbruik, opslagperiodes en risico's voor de rechten van betrokkenen.

Het recht op informatie vereist dat betrokkenen op een transparante manier worden geïnformeerd over de verwerking van hun persoonsgegevens. De informatie moet onder andere de identiteit van de verwerkingsverantwoordelijke, verwerkingsdoeleinden, rechtsgrond, ontvangers, bewaartermijn, rechten van betrokkenen en geautomatiseerde besluitvorming bevatten. Hoe deze informatie aan betrokkenen wordt verstrekt, kan variëren, bijvoorbeeld via een privacyverklaring, brief, e-mail of telefonisch contact.

De DPIA moet aangeven hoe betrokkenen worden geïnformeerd over gegevensverwerkingen, bijvoorbeeld door middel van een openbaar gepubliceerde privacyverklaring, interne bekendmaking, fysieke of digitale brieven, of telefonisch contact.

In bepaalde gevallen kunnen decentrale overheden als verwerkingsverantwoordelijke de rechten van de betrokkene inperken, bijvoorbeeld om de nationale of openbare veiligheid te waarborgen of om de rechten en vrijheden van anderen te beschermen.

De beperking moet gebaseerd zijn op wettelijke bepalingen en de verwerkingsverantwoordelijke moet waarborgen dat de wezenlijke inhoud van grondrechten en fundamentele vrijheden ongeschonden blijft.

De beperking van rechten van betrokkenen door wettelijke bepalingen is toegestaan voor doeleinden zoals nationale veiligheid, landsverdediging, openbare veiligheid, preventie, onderzoek, opsporing en vervolging van strafbare feiten, uitvoering van straffen, bescherming tegen en preventie van gevaren voor de openbare veiligheid, andere belangrijke doelstellingen van algemeen belang van de Unie of een lidstaat, waaronder economische of financiële belangen, alsook monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid, sociale zekerheid, bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures, opsporing en vervolging van schendingen van beroepscodes

voor gereglementeerde beroepen, toezicht, inspectie of regelgeving gerelateerd aan de uitoefening van openbaar gezag in eerder genoemde situaties, bescherming van de betrokkene of van de rechten en vrijheden van anderen, en inning van civielrechtelijke vorderingen.

2.3 Risicobeoordeling (BowTie a.d.h.v. NOREA)

Op basis van de gegevensverwerking worden risico's voor de rechten en vrijheden van personen beoordeeld, met bijbehorende maatregelen in de risicobeoordeling en -behandeling. Het naleven van de AVG betekent niet dat er geen enkel risico mag zijn; elk proces brengt inherent risico's met zich mee. Het resterende risico na genomen maatregelen moet echter acceptabel zijn. Eerder is al beoordeeld of de gegevensverwerking rechtmatig is.

Vaak wordt in de praktijk de term 'privacy risico' gebruikt in plaats van 'risico's voor de rechten en vrijheden van personen'. Hierbij ligt de focus meer op de organisatorische risico's dan op die voor de betrokkenen. Hoewel de impact op de organisatie belangrijk is, komt deze vaak voort uit inbreuken op de rechten van betrokkenen. 'Privacy risico' is hier een containerbegrip geworden, waardoor de juiste maatregelen mogelijk niet worden genomen. In dit document wordt met 'privacy risico' primair het risico voor de rechten van betrokkenen bedoeld en secundair het risico voor de organisatie. Een gestructureerde risicobeoordeling met focus op concrete negatieve gevolgen voor betrokkenen is essentieel voor een effectieve DPIA.

Voor risicobeoordelingen kunnen allerlei technieken worden gebruikt. 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. In deze toelichting wordt, in het geval van grote gegevensverwerkingen, gebruik gemaakt van de BowTie-methode.

2.3.1 Risico-identificatie

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. 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 (o.a. BowTie XP) worden uitgevoerd.

1. Stel de **Risicobron**/het **Gevaar** vast.
2. Stel de **Kritieke Gebeurtenissen** per **Risicobron** vast.
3. Stel per **Risicobron/Kritieke gebeurtenis-combinatie** een apart BowTie-diagram op. De **Kritieke gebeurtenis** is het middelpunt van de BowTie. Voeg daar achtereenvolgens de **Bedreigingen**, de **Consequenties**, de **Barrières** en zo nodig de **Escalatie factoren** aan toe.

2.3.2 Risicoanalyse

Het tweede onderdeel van de risicobeoordeling is de *risico-analyse*. De analyse 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, voor zover van toepassing. Bepaal achtereenvolgend:

5. De **bijdrage van de Bedreiging** op het laten plaatsvinden van de Kritieke Gebeurtenis (bijvoorbeeld Hoog, Middelmatig, Laag).
6. De **inherente risico's** per Consequentie. Dit 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' x 'impact'.
7. De **effectiviteit** van de aan een Bedreiging gekoppelde Preventieve barrière op het voorkomen dat die Bedreiging leidt tot de Kritieke Gebeurtenis én de effectiviteit van de aan een Consequentie gekoppelde Herstel barrière op het voorkomen dat de Kritieke Gebeurtenis leidt tot die Consequentie.
8. 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:
    i. Bijdrage voor de relevante Bedreigingen;
    ii. Effectiviteit van de aan die Bedreigingen gekoppelde Preventieve barrières;
    iii. Effectiviteit van de aan de Consequentie gekoppelde Herstel barrières.

2.3.3 Risico-evaluatie

In het laatste onderdeel van de risicobeoordeling, de risico-evaluatie, wordt erkend dat het naleven van de AVG niet betekent dat er geen enkel risico mag zijn voor de rechten en vrijheden van de betrokkenen. Elke gegevensverwerking brengt inherent risico's met zich mee, maar deze mogen niet "hoog" zijn.

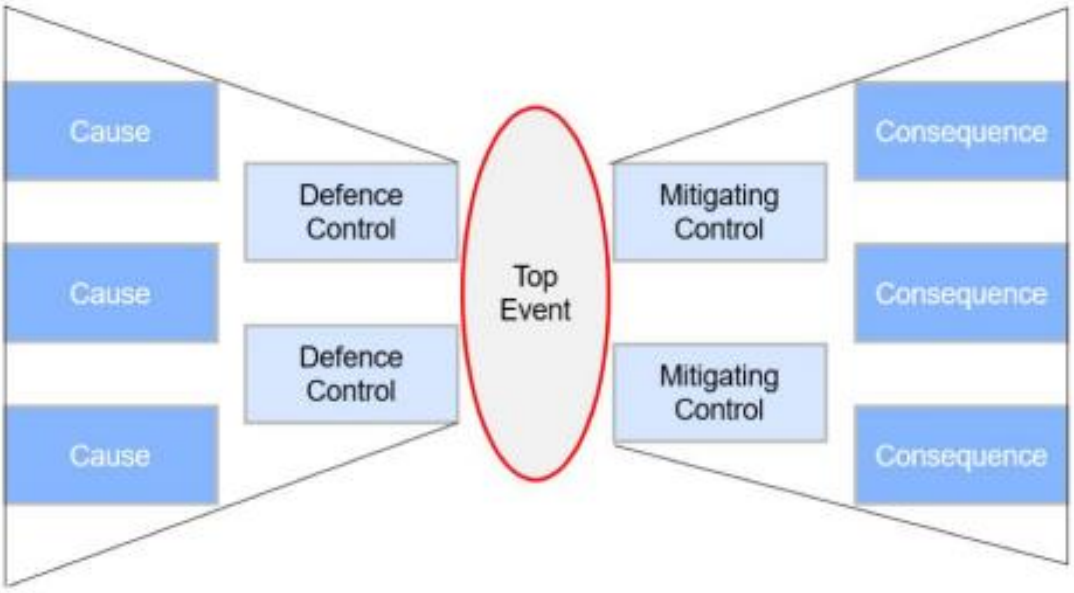
Als het restrisico hoog is, moet de organisatie de Autoriteit Persoonsgegevens (AP) raadplegen voordat de verwerking plaatsvindt.

De organisatie heeft enige vrijheid om haar risicobereidheid te bepalen met betrekking tot de risico's voor de betrokkenen. Voor risico's die alleen de organisatie betreffen (vaak het gevolg van risico's voor de betrokkene), is de AVG niet van toepassing en zijn er geen specifieke eisen aan de maximaal acceptabele restrisico's. De risicobereidheid varieert tussen verschillende branches en zelfs tussen organisaties binnen dezelfde branche.

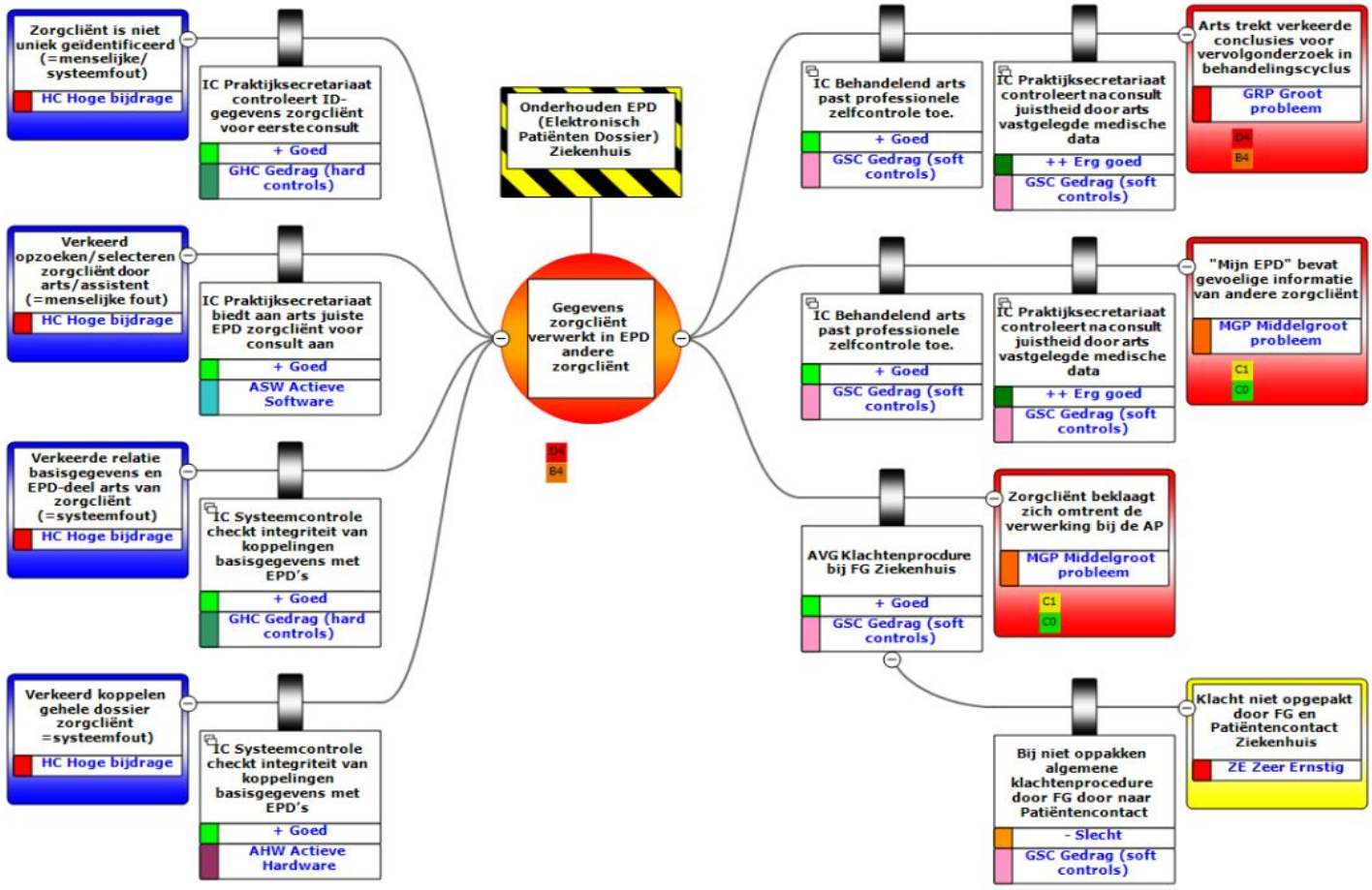
Bij de risico-evaluatie worden de resultaten van de risicoanalyse vergeleken om te bepalen of aanvullende actie vereist is. Dit kan leiden tot de volgende besluiten:

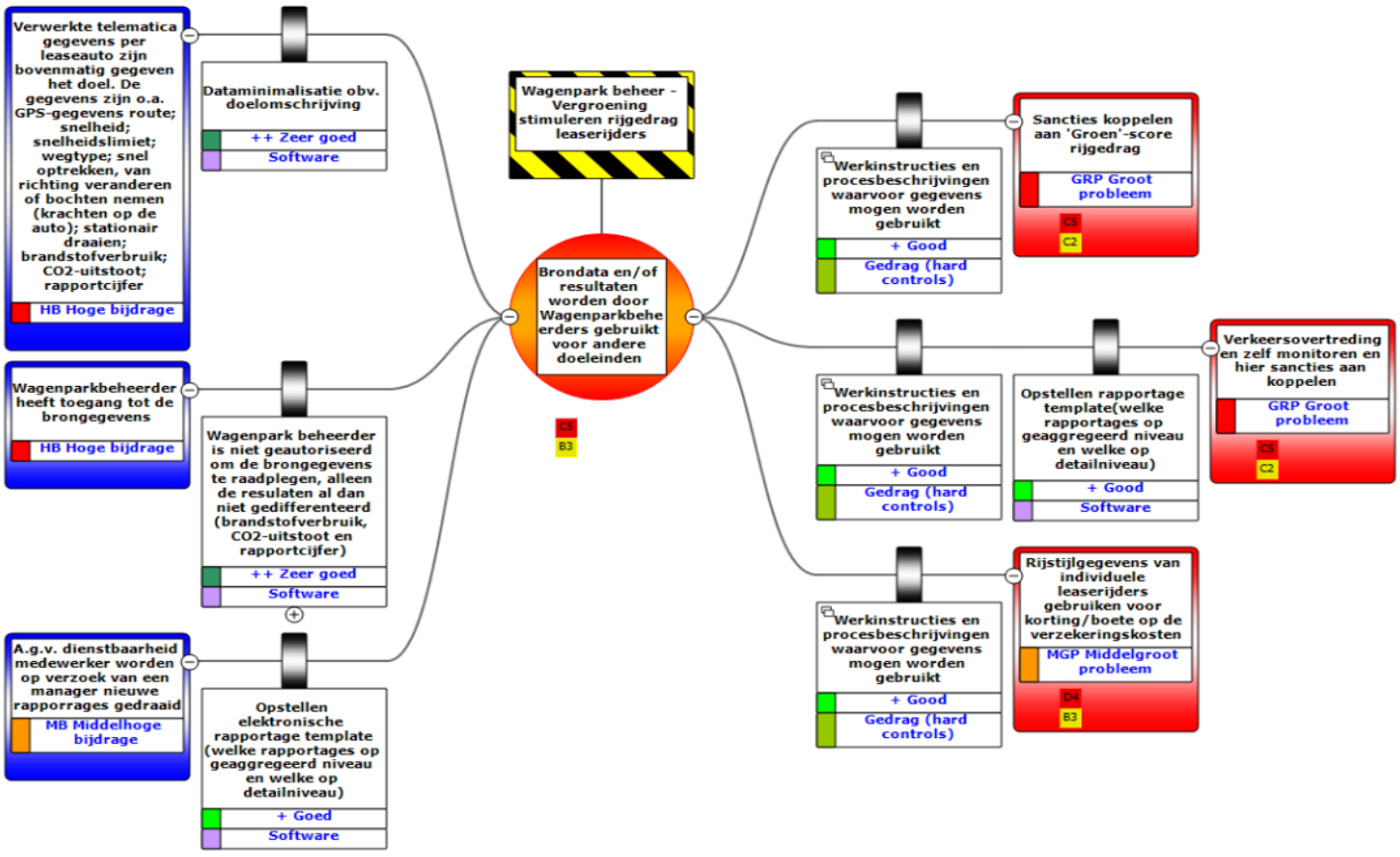
1. **Niets doen (accepteren van risico):** De organisatie accepteert het restrisico voor de betrokkenen zolang dit lager is dan "hoog". Deze beslissing is afhankelijk van de risicobereidheid van de organisatie.
2. **Nadenken over opties voor risicobehandeling (beheersen van risico):** Als de bestaande of voorgenomen maatregelen niet effectief zijn tegen negatieve gevolgen en de organisatie het restrisico niet wil of kan accepteren, overweegt de organisatie alternatieve maatregelen of aanvullende maatregelen.
3. **Doeleinden herzien (elimineren risico):** Als de organisatie het restrisico niet wil of kan accepteren en er geen nieuwe maatregelen mogelijk zijn, kan de organisatie overwegen de doeleinden van de gegevensverwerking te herzien. Dit kan betekenen dat een of meer doeleinden worden gewijzigd of geëlimineerd om negatieve gevolgen te voorkomen of te beperken.

Voorbeeld BowTie’s



GEMEENTE WESTERWOLDE





2.4 Risicobeoordeling

Volgens de privacyregelgeving moet een Data Protection Impact Assessment (DPIA) een evaluatie van risico's voor de rechten en vrijheden van betrokkenen bevatten. Bij het identificeren van risico's ligt de focus niet op de belangen van de organisaties die verantwoordelijk zijn voor gegevensverwerking, maar op de impact die de verwerking op de betrokkene kan hebben.

Door de aard, het toepassingsgebied, de context en de doeleinden van gegevensverwerking te analyseren, moet de waarschijnlijkheid en ernst van risico's voor de betrokkenen worden bepaald. Een objectieve beoordeling bepaalt of gegevensverwerking gepaard gaat met (hoog) risico, waarbij de oorsprong, aard, specifieke kenmerken en ernst van het risico worden geëvalueerd.

De risicogerichte benadering omvat het identificeren, analyseren en evalueren van risico's, vergelijkbaar met een informatiebeveiligingsrisicoafweging. In tegenstelling tot informatiebeveiliging, die gericht is op betrouwbaarheidseisen voor systemen, richt DPIA zich op de mogelijke impact voor betrokkenen.

2.4.1 Impact-identificatie

Het identificeren van de impact begint met het vaststellen van potentiële risico's, gebaseerd op de huidige situatie en bestaande maatregelen. Privacyrechten, waaronder het recht op privacy en andere fundamentele rechten, kunnen worden geschonden, resulterend in materiële of immateriële schade. Hierbij kan gedacht worden aan de volgende situaties waar de gegevensverwerking kan leiden tot:

- Discriminatie, stigmatisering en uitsluiting;
- (Blootstelling aan) identiteitsdiefstal of -fraude;
- Financiële verliezen;
- Reputatie- of anderszins relationele schade;
- Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
- Ongeoorloofde ongedaanmaking van pseudonimisering;
- Of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;
- Wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;
- Wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;
- Wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- Wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt; of
- Wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.[1]

Bij de (onrechtmatige) verwerking van persoonsgegevens wordt overwogen of er sprake is van al dan niet opzettelijke handelingen zoals de vernietiging en het verlies van persoonsgegevens, wat de beschikbaarheid ervan aantast. Ook de wijziging van gegevens, wat de integriteit beïnvloedt, en ongeoorloofde toegang en verstrekking, wat de vertrouwelijkheid schendt, behoren tot deze

[1] Overwegingen 75 en 85 AVG en overweging 51 Richtlijn.

handelingen. Dit omvat tevens elk ander gedrag dat in strijd is met de geldende wet- en regelgeving met betrekking tot persoonsgegevens.

2.4.1.1 Discriminatie

Het maken van ongerechtvaardigd onderscheid tussen gelijke gevallen is wettelijk verboden volgens artikel 1 van de Nederlandse Grondwet. Deze wet richt zich niet alleen op een beperkt aantal gronden waarop in principe geen besluiten mogen worden genomen, zoals godsdienst, levensovertuiging, ras of geslacht, maar verbiedt discriminatie op welke grond dan ook. Dit verbod omvat niet alleen directe discriminatie, waarbij een persoon anders wordt behandeld dan een ander in een vergelijkbare situatie, maar strekt zich ook uit tot indirecte discriminatie.

Indirecte discriminatie doet zich voor wanneer een ogenschijnlijk neutrale bepaling, maatstaf of handelwijze een bepaalde groep personen bijzonder treft in vergelijking met andere groepen personen. Een voorbeeld hiervan is te vinden in beveiligingssystemen op basis van gezichtsherkenning, waar strenge kledingvoorschriften kunnen resulteren in indirecte discriminatie. In dit geval kunnen personen met hoofd- of gezichtsbedekking vanwege religieuze redenen onevenredig worden beïnvloed.

2.4.1.2 Big Data

Big data-verwerkingen brengen specifieke risico's met zich mee voor de betrokkenen. Een algoritme kan bijvoorbeeld een statistisch logische correlatie ontdekken, maar dit kan leiden tot vooroordelen, stereotypering, discriminatie, en sociale uitsluiting. Deze gevolgen kunnen zich manifesteren in diverse situaties, zoals sollicitaties, het verkrijgen van leningen, en het afsluiten van verzekeringen. Daarnaast bestaat het risico dat de betrokkene wordt onderworpen aan besluitvorming op basis van big data waar hij geen begrip van heeft en geen invloed op kan uitoefenen.

2.4.2 Risicoanalyse

Na het identificeren van risico's is het essentieel om ze te beoordelen door de waarschijnlijkheid van dreigingen en de mogelijke gevolgen voor de betrokkenen in te schatten. Men moet zich richten op de verwachte impact op individuen en de manier waarop deze risico's zich manifesteren, en de waarschijnlijkheid hiervan. Deze evaluatie is geen zoektocht naar zwart-wit-antwoorden maar vereist een zorgvuldige afweging. Het vaststellen van een risiconiveau is gebaseerd op deze analyse.

De ernst van de risico's wordt beïnvloed door de context van de gegevensverwerking, waaronder de aard van de persoonsgegevens, de verwerkingsprocessen en de doeleinden van de gegevensverwerking. De waarschijnlijkheid van risico's die zich voordoen hangt samen met de gebruikte middelen door de verwerkingsverantwoordelijke en de aard van de persoonsgegevens. Bijvoorbeeld, persoonsgegevens die dienen als toegangssleutel tot financiële middelen of die de betrokkene blootstellen aan reputatieschade brengen inherente risico's met zich mee, zoals inloggegevens voor DigiD of informatie over de psychologische situatie van de betrokkene.

Het wordt aanbevolen om de risico-inschatting te structureren door zowel de kans als de impact van het risico te classificeren als laag, gemiddeld of hoog. Vervolgens wordt de classificatie voor het risico zelf bepaald door de kans te vermenigvuldigen met de impact. Het template maakt gebruik van deze berekening om de algehele ernst van het risico in te schatten.

Voor een meer diepgaande beoordeling van de risico's kan het raadzaam zijn om de betrokkenen of hun vertegenwoordigers te raadplegen. Dit zorgt voor een breder begrip van mogelijke gevolgen en draagt bij aan een zorgvuldige inschatting van de risico's die gepaard gaan met gegevensverwerking.

2.4.3 Risico-evaluatie

Stel aanvaardbare waarden voor risico's vast en beoordeel of deze binnen acceptabele grenzen liggen. Het is van belang om een toelichting toe te voegen aan de inschatting van de impact, zodat gedocumenteerd wordt op welke overwegingen deze inschatting is gebaseerd. Hierdoor ontstaat een helder inzicht in de afwegingen die hebben geleid tot de beoordeling van de aanvaardbaarheid van de risico's.

2.5 Maatregelen

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

Voorbeelden van maatregelen zijn:

AVG:

- Pseudonimiseren en versleutelen van persoonsgegevens;
- Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Maatregelen die afkomstig zijn uit de hoek van informatiebeveiliging zijn:

- Fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- Opslag van gegevens in een kluis;
- Project-, risico- en incidentenmanagement;
- Data opsplitsen;
- Dataminimalisatie;
- Back-ups;
- Integriteitscontroles;
- Meerfactor-authenticatie;
- Monitoring en logging;
- Controle van toegekende bevoegdheden;
- Privacybewustzijn- en beveiligingstrainingen;
- Managementrapportages over risicobeheer;
- Beperken inzageniveau;
- Periodiek een audit of hack- of penetratietest uitvoeren;
- Richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- Responsible-disclosurebeleid;
- Geheimhoudingsverklaringen;
- Service level agreements (met boeteclausules);
- Verwerkersovereenkomsten.

- Screening personeel en VOG-verklaring.
- Controle op de toegang tot de apparatuur;
- Controle op de gegevensdragers;
- Opslagcontrole;
- Gebruikscontrole
- Controle op de toegang tot gegevens;
- Transmissiecontrole;
- Invoercontrole;
- Transportcontrole;
- Herstelmogelijkheid.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1