NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

DPIA Raamwerk

Rapportage voor

<naam gegevensverwerking>

<Datum>
<Versie>
<Status>

Inleiding

Met het uitvoeren van een Data Protection Impact Assessment (DPIA), in het Nederlands aangeduid met Gegevensbeschermingseffectbeoordeling (GEB; hierna wordt alleen de term DPIA gebruikt), 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 van een gegevensverwerking en hierop te anticiperen worden kostbare aanpassingen in processen, herontwerp van systemen of 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 risico's van een gegevens-verwerking kan het management helpen bij een betere onderbouwing van de risicobereidheid ('risk appetite') van de organisatie. Daarnaast helpt de DPIA bij het verhogen van privacy-bewustzijn 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 vertrouwen doordat de organisatie privacybescherming zichtbaar in het ontwerp van een project meeneemt. Een bijkomend voordeel van de DPIA is dat de organisatie de naleving aan de Algemene Verordening Gegevensbescherming (AVG) ermee kan aantonen.

Een DPIA is een proces dat bestaat uit:

- Het beschrijven van de gegevensverwerking (deel I);
- Het beoordelen van de rechtmatigheid van de gegevensverwerking (deel II);
- Het helpen beheren van de aan de gegevensverwerking verbonden risico's voor de rechten en vrijheden van natuurlijke personen door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken (deel III).

In dit document, het DPIA Raamwerk, zijn de vragen voor de bovengenoemde drie delen, opgenomen die na beantwoording ervan leiden tot de DPIA-rapportage. Voor het borgen van de beheersing van de risico's van de gegevensverwerking wordt deze DPIA-rapportage ondertekend (deel IV).

In het document 'NOREA Handreiking DPIA' is een toelichting opgenomen van de in dit raamwerk gestelde vragen en wordt nader ingegaan op de DPIA (onder andere wat is het en wanneer, hoe en wie voert de DPIA uit), risicobeoordeling en risicobehandeling, inbedding in de organisatie en de relatie tussen de DPIA en de informatiebeveiligingsrisicoanalyse. De NOREA Handreiking DPIA en het NOREA DPIA Raamwerk zijn in lijn met de door de European Data

Protection Board (EDPB; de Europese privacy toezichthouders) gestelde criteria voor een aanvaardbare DPIA.[1]

De vragen in het DPIA Raamwerk zijn gebaseerd op de AVG. Dat wil niet zeggen dat dit 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 de vragen met betrekking tot 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 voor gedefinieerde antwoorden in dit DPIA Raamwerk moeten vaststellen.

[1] WP248.rev01 "Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking 'waarschijnlijk hoog risico inhoudt' in de zin van Verordening 2016/79" (okt. 2017). In Bijlage 2 van deze Richtsnoer zijn de criteria opgenomen voor een aanvaardbare gegevensbeschermingseffectbeoordeling.

Deel I: Beschrijving gegevensverwerking

Een beschikbare systematische beschrijving van de (beoogde) gegevensverwerking en de verwerkingsdoeleinden 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? Hoe draagt het project/ systeem bij aan het realiseren van de organisatiedoelen?

Sluit, voor zover aanwezig, aan bij de projectbeschrijving, het bedrijfsvoorstel, het systeemvoorstel. Gebruikt het project nieuwe technologieën? Wat is de omvang van de gegevensverwerking?

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

Voeg procesplaten of diagrammen toe die de stroom van persoonsgegevens, inclusief rapportages, tonen (dataflow van persoonsgegevens); input en output van gegevensstromen (zowel elektronisch als op papier). Welke medewerkers/functionarissen spelen een rol in het proces. Wie ontvangen de persoonsgegevens buiten de eigen organisatie?

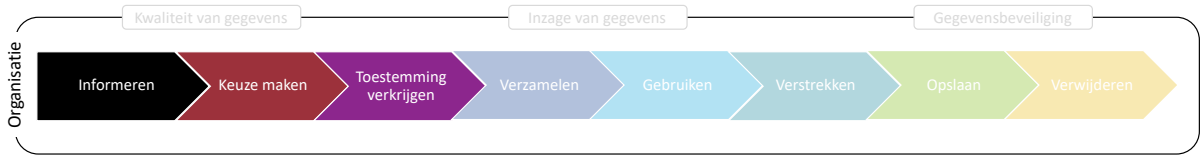
1.3. Geef een beschrijving van de 'geraakte' (persoonsgegevens bevattende) IT-systemen en/of interfaces naar andere platforms.

Geef inzicht in de samenhang van de IT-infrastructuur (applicaties, databases, operating systems en netwerken).

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

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.[2] Dit hoofdstuk gaat in op de fasen van de informatie-levenscyclus 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.



figuur 1: Informatielevenscyclus (fasen Informeren, Keuze maken en Toestemming verkrijgen)

2.1. Beschrijf de wijze waarop de betrokkenen worden geïnformeerd over de gegevens-verwerking.

2.2. Bepaal per verwerkingsdoel de grondslag van de gegevensverwerking en geef een toelichting.

Een gegevensverwerking is alleen rechtmatig als deze op ten minste een van de in de AVG genoemde grondslagen is gebaseerd.

<Voeg per verwerkingsdoel een rij toe aan onderstaande tabel>

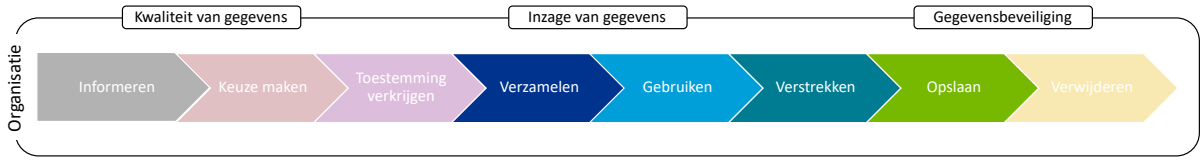
Verwerkingsdoel	Grondslag	Toelichting
	Maak per verwerkingsdoel de keuze op welke grondslag(en) de verwerking is gebaseerd: a. Toestemming; b. Uitvoering van een overeenkomst; c. Wettelijke verplichting; d. Bescherming van vitale belangen; e. Taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag; f. Behartiging van de gerechtvaardigde belangen van de verwerkings-verantwoordelijke of van een derde	Geef hier korte toelichting voor de gemaakte keuze. Bijvoorbeeld: • Voor de grondslagen 'c. Wettelijke verplichting' en 'e. Taak van algemeen belang' zijn aanvullende bepalingen opgenomen in de UAVG. Geef hier hoe daar mee wordt omgegaan. • Als de grondslag 'f. Behartiging 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] NOREA Handreiking Privacy Control Framework v2.0 (aug. 2019).

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.

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 2: 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[3] en/of gegevens van strafrechtelijke aard zijn, het verwerkingsdoel en de bewaartermijn.

Voor zover de PDIA 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 in na goedkeuring van de DPIA.

[3] Bijzondere categorieën van persoonsgegevens (art 9 AVG): 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.

<Voeg per categorie van betrokkenen een rij toe aan onderstaande tabel>

Categorie van betrokkenen	Categorie van persoonsgegevens	Bijzondere/ strafrechtelijke persoonsgegevens	Verwerkingsdoel	Bewaartermijn
Bijvoorbeeld medewerkers, klanten, patiënten, burgers, zakelijke contacten	Bijvoorbeeld identificerend, contact, demografisch, medisch en gezondheid, fysieke eigenschappen, voorkeur, opvatting en overtuiging, locatie, bancair, bezit, transactie, krediet, professie, strafrechtelijk, familie, social network	Ja / Nee[4]	Waarvoor worden de persoonsgegevens gebruikt (zie ook vraag 2.2)	Maak hierbij onderscheid tussen ingang van de bewaartermijn (event) en de bewaartermijn zelf. Neem ook de motivatie van bewaring op.

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.

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

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

Techniek	Onderbouwing
Profilering/(semi-)geautomatiseerde besluitvorming, monitoring, et cetera	Onderbouwing van waarom bijvoorbeeld profilering voor dit project noodzakelijk is

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.

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).

[4] Doorhalen wat niet van toepassing is.

Beschrijf of en hoe voor de in scope zijn gegevensverwerking aan de verschillende rechten kan worden voldaan. Hiermee wordt niet een algemene procedure bedoeld (al dan niet als onderdeel van het privacybeleid), maar specifiek de uitvoering ervan. In hoeverre is hier bij de ontwikkeling van het project/systeem rekening mee gehouden.

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

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, stel vast of de scope (geheel) overeenkomt en beschrijf hoe borging hiervan plaatsvindt. In geval van certificering benoem ook de externe instelling die het certificaat heeft uitgegeven.**

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 de 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').

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.**

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

<Voeg per 'Ontvangende bedrijfseenheid' een rij toe aan onderstaande tabel. Zie ook vraag 1.2 voor de beantwoording van de vraag 'Welke bedrijfseenheden, afdelingen zijn betrokken bij de gegevensverwerking?'>

Ontvangende bedrijfseenheid	Ontvangende afdeling

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

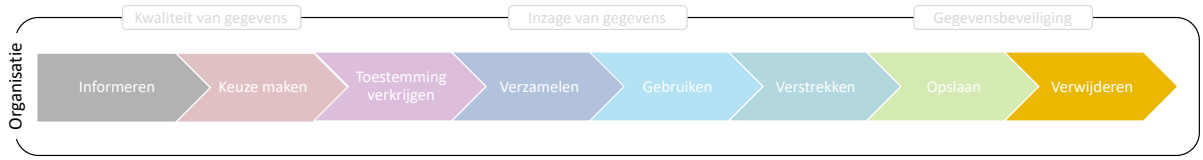
Geef aan of de ontvangende organisatie een onderdeel is van het concern waartoe de verstrekkende organisatie behoort en weke rol deze in de zin van de AVG vervult (verwerkingsverantwoordelijke of verwerker). Indien de ontvanger Verwerker is in de zin van de AVG, geef dan aan of een er een verwerkersovereenkomst is opgesteld. Indien de ontvanger buiten de EU/EER is gevestigd benoem dan op welke manier een passend beschermingsniveau wordt geborgd.

<Voeg per 'Ontvanger' een rij toe aan onderstaande tabel. Zie ook het antwoord op vraag 1.2 voor de beantwoording van de vraag "Welke organisaties zijn betrokken bij de gegevensverwerking?">

Ontvanger (Ontvangende organisatie)	Concern-onderdeel	Rol	Verwerkersovk. i.g.v. verwerker	Locatie	Buiten de EU/EER	Waarborgen internationale doorgifte
	Ja/ Nee	Verantwoordelijke/ Vewerker	Ja / Nee		Ja / Nee	

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 3: 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.

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.

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 risicobeoordeling en risicoafhandeling (deel III). Als uiteindelijk blijkt dat een bepaalde gegevensverwerking 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, gestopt moet worden met die gegevensverwerking.

5. Grondslag

5.1. **Beoordeel de grondslag/grondslagen waarop de gegevensverwerking is gebaseerd (zie 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 de aangehaalde uitzonderingsgrond op het verwerkingsverbod 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 het proportionaliteits- en subsidiariteitsvereiste wordt voldaan. Stel op grond van het proportionaliteitsbeginsel vast of de doeleinden van de verwerking in verhouding staan tot /in evenredigheid zijn met de inbreuk op de persoonlijke levenssfeer van de betrokkene?

Stel op grond van het subsidiariteitsbeginsel vast of de doeleinden ook op een andere wijze kunnen worden bereikt waarbij de inbreuk op de persoonlijke levenssfeer van de betrokkene minder is.

<Voeg per 'Verwerkingsdoel' een rij toe aan onderstaande tabel.>

Verwerkingsdoel	Proportionaliteit	Subsidiariteit
(zie vraag 2.2)	Worden de persoonsgegevens bijvoorbeeld niet langer bewaard dan noodzakelijk voor het doel en zijn de gegevens alleen toegankelijk voor degen die deze nodig hebben voor uitoefening van hun taak?	Kunnen de doeleinden bijvoorbeeld worden behaald met minder persoonsgegevens, of met persoonsgegevens die minder inbreuk maken op de privacy van de betrokkenen (met name gevoelige gegevens)?

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 vragen 2.1, 3.6 en 3.7).

Deel III: Risicobeoordeling en Risicobehandeling

Op basis van de beschrijving van de gegevensverwerking (deel I) worden in dit deel van het Raamwerk 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).[5]

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 0 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 en vrijheden van de betrokkenen (primair). Daarnaast is de term 'privacyrisico' ook een containerbegrip geworden waarbij oorzaken, gevolgen en soms zelfs maatregelen als 'risico' worden getypeerd. Dit alles kan tot gevolg hebben dat niet de 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 betrokkenen is essentieel voor de effectiviteit van de DPIA.

8. Risicobeoordeling (Risk assessment)

Voor risicobeoordelingen kunnen allerlei technieken worden gebruikt.[6] Het staat het team/degene die de DPIA uitvoert vrij om een bepaalde techniek te kiezen. Los van de gekozen

[5] Risicobeoordeling (risk assessment) en Risicobehandeling (risk treatment) zijn onderdelen uit het Proces Risicomanagement van NEN-ISO31000.

[6] 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.

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.

Neem hier de resultaten op van de uitgevoerde risico-identificatie op basis van de door het DPIA-team gekozen risicobeoordelingsmethodiek.

Ter illustratie: Uitwerking risico-identificatie met behulp van BowTie

In het NOREA DPIA Raamwerk is gekozen om de BowTie methodologie (vlinderdas-model) uit te werken voor de risicobeoordeling. De BowTie methodologie is bij uitstek een krachtig instrument om expliciet de negatieve gevolgen van risico's te analyseren en in kaart te brengen. In een BowTie-diagram worden in één figuur, concrete bedreigingen en consequenties alsmede bestaande/mogelijke preventieve- en herstelmaatregelen begrijpelijk in kaart gebracht. De BowTie methodologie kan zowel op 'papier' als met behulp van software worden uitgevoerd.

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 kunnen er meerdere verschillende Kritieke gebeurtenissen worden onderkend.

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.*

De van toepassing zijnde Kritieke gebeurtenis(sen) kan/kunnen voor de 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:*

   1 *De maatregelen die worden genomen om te voorkomen dat bedreigingen leiden tot de Kritieke gebeurtenis. Dit zijn de zogenaamde Preventieve barrières en worden aan de linkerkant van de BowTie opgenomen.*

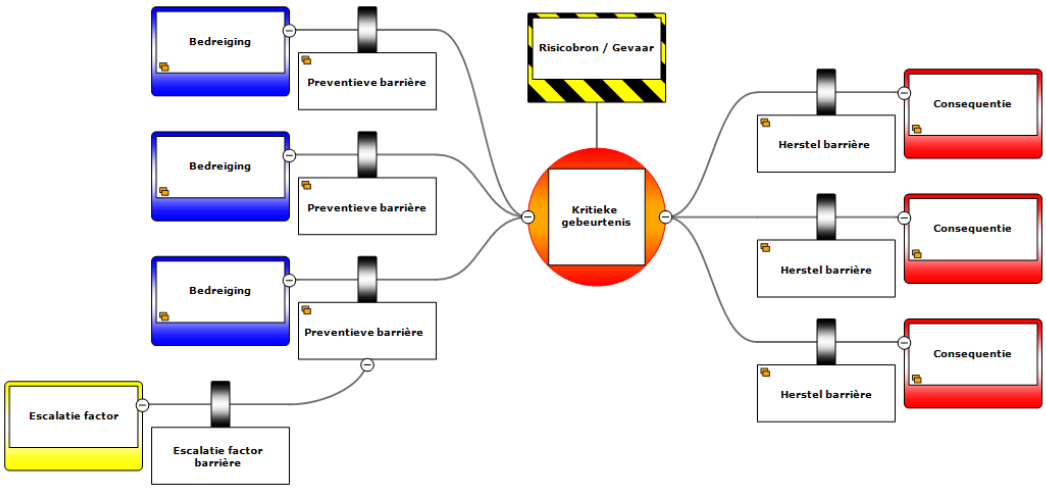
   2 *De maatregel die worden genomen om te voorkomen dat de Kritieke gebeurtenis resulteert in de nadelige Consequenties. Dit zijn de zogenaamde Herstel barrières en worden de rechterkant van de BowTie opgenomen.*

   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 het 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.*

In figuur 4 is als voorbeeld een BowTie opgenomen met de begrippen.



figuur 4: Voorbeeld begrippen BowTie (gemaakt met BowTieXP)[7]

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?

Neem hier de resultaten op van de uitgevoerde risicoanalyse op basis van de door het DPIA-team gekozen risicobeoordelingsmethodiek.

Ter illustratie: Uitwerking risicoanalyse met behulp van BowTie

*De initiële BowTie (resultaat van vraag **Error! Reference source not found.**) wordt aangevuld door:*

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' x 'ernst van gevolgen (impact)'*

Neem hier de risico-matrix op die de organisatie gebruikt voor het bepalen van het inherente en restrisico. 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 figuur 5 is een voorbeeld opgenomen.

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

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 5: 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 Consequente gekoppelde Herstelbarrière 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 en 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 Autoriteit Persoonsgegevens (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:

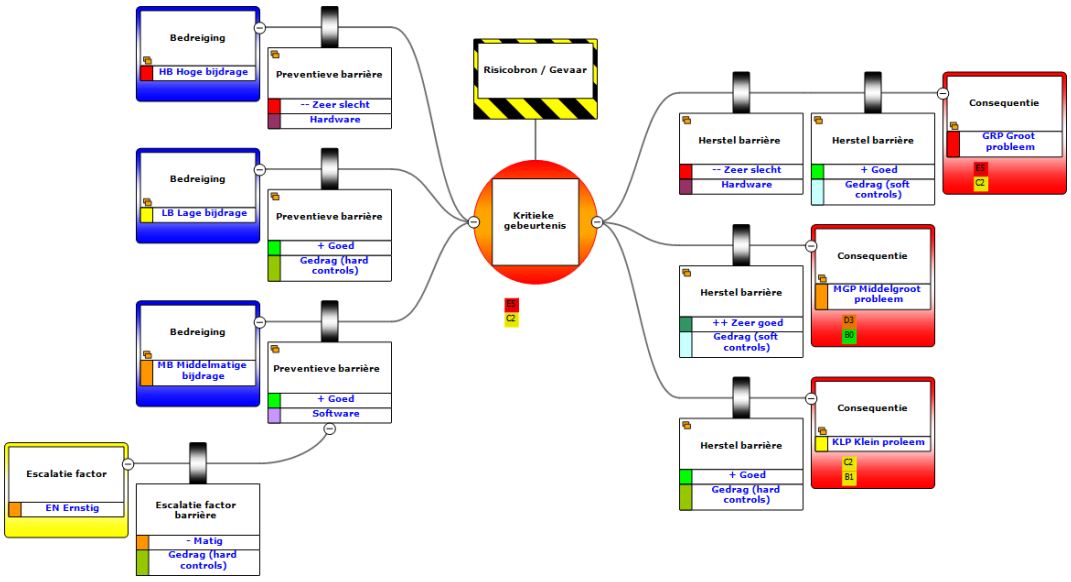
a. **Verder niets te doen (accepteren risico):** Het accepteren van het restrisico voor de betrokkenen, zolang deze lager is dan 'hoog', en voor de organisatie is afhankelijk van de risicobereidheid (risk appetite) van de organisatie.
b. **Na te denken over opties voor risicobehandeling (beheersen risico)**: 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.

Neem hier de resultaten op van de uitgevoerde risico-evaluatie op basis van de door het DPIA-team gekozen risicobeoordelingsmethodiek.

Ter illustratie: Uitwerking risico-evaluatie met behulp van BowTie

Wijzigingen als gevolg van onderdeel 'b) Na te denken over opties voor risicobehandeling' en 'c) Doeleinden te herzien' worden in het BowTie-diagram doorgevoerd waarna de risicoanalyse (0) en risico-evaluatie (8.3) voor het betreffende deel opnieuw wordt doorlopen. Dit is een iteratief proces.

Neem hier per Risicobron/Kritieke gebeurtenis-combinatie het definitieve BowTie-diagram op. Ter illustratie is hier de BowTie uit figuur 4 aangevuld naar aanleiding van de risicoanalyse en risico-evaluatie.



figuur 6: Voorbeeld begrippen BowTie, incl. Bijdrage Bedreiging, Effectiviteit Barrières en Inherente-/ Restrisico's (gemaakt met BowTieXP)

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

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

Zo ja, geef aan of raadpleging met de Autoriteit Persoonsgegevens heeft plaatsgevonden en wat hun reactie 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 gewenste maatregelen om deze risico's te voorkomen/te mitigeren tot een voor de stakeholders 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.

9.1. Benoem de te nemen acties (onder andere verantwoordelijkheid, prioriteit en doorlooptijd) voor de geselecteerde maatregelen.

<Voeg per 'Maatregel' een rij toe aan onderstaande tabel. Afhankelijk van de gekozen methodologie voor risicobeoordeling kan deze informatie ook (deels) worden toegevoegd aan het diagram>

Maatregel	Verantwoordelijke afdeling/ functionaris	Geïmplemen-teerd	Prioriteit	Te nemen acties	Oplever-datum
		Ja / Nee			

Bij voorkeur zijn alle voorgestelde 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

Proceseigenaar

Hierbij verklaar ik dat de beschrijving van de verwerking (deel I) juist en volledig is. Dat de belangrijkste organisatorische oorzaken in kaart zijn gebracht, de beschreven organisatorische maatregelen de risico's voldoende mitigeren.

Eventuele opmerking

Datum	Naam	Functie	Handtekening

Functionaris gegevensbescherming <voor zover aanwezig> / Privacy Officer

Hierbij verklaar ik dat de uitkomst van de rechtmatigheidscheck (deel II) afdoende is, dat de belangrijkste risico's die een inbreuk op de rechten en vrijheden van betrokkene kunnen hebben in kaart zijn gebracht. Dat ik als de FG om advies ben gevraagd voor deze DPIA en dat mijn adviezen zijn meegenomen in deze versie van de DPIA.

Eventuele opmerking + definitief advies aan directeur/Raad van Bestuur

Datum	Naam	Functie	Handtekening

Chief Information Security Officer (CISO)

Hierbij verklaar ik dat de beschreven informatiebeveiligingsmaatregelen de risico's voldoende kunnen mitigeren. Dat ik als de CISO om advies ben gevraagd voor deze DPIA en dat mijn adviezen zijn meegenomen in deze versie van de DPIA.

Eventuele opmerking + definitief advies aan directeur/Raad van Bestuur

Datum	Naam	Functie	Handtekening

Algemeen directeur/Raad van Bestuur

Hierbij verklaar ik/wij kennis te hebben genomen van de beschreven restrisico's, deze hebben geaccepteerd en budget vrij te stellen van de voorgestelde maatregelen.

Datum	Naam	Functie	Handtekening